УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ

Ненад Р. Путник

КИБЕР РАТОВАЊЕ – НОВИ ОБЛИК САВРЕМЕНИХ ДРУШТВЕНИХ КОНФЛИКАТА

докторска дисертација

Београд, 2012

UNIVERSITY OF BELGRADE
FACULTY OF SECURITY STUDIES

Nenad R. Putnik

CYBER WARFARE - A NEW FORM OF CONTEMPORARY SOCIAL CONFLICTS

Doctoral Dissertation

Belgrade, 2012

Ментор:

Др Радомир Милашиновић, редовни професор,
Универзитет у Београду − Факултет безбедности

Чланови комисије:

Др Озрен Цигурски, ванредни професор,
Универзитет у Београду − Факултет безбедности

Др Драган Симић, редовни професор,
Универзитет у Београду − Факултет политичких наука

Датум одбране:_____

КИБЕР РАТОВАЊЕ - НОВИ ОБЛИК САВРЕМЕНИХ ДРУШТВЕНИХ КОНФЛИКАТА

Настанак кибер простора представљао је својеврсну прекретницу у сфери војних активности али и поимања корпоративне, националне, регионалне и глобалне безбедности. Нови „простор“ пружио је велике могућности за спровођење специјалних пропагандних дејстава али и извођење напада посредством рачунарских мрежа на противничке информационе системе. За овај нови вид конфронтације у виртуелном простору се у англосаксонском говорном подручју користи појам *кибер ратовање* (*енгл*. cyber warfare). Напади у виртуелном простору, наоко неприметни, могу у реалном, физичком свету резултовати људским жртвама и материјалним разарањима. Због тога је кибер ратовање данас у жижи интересовања теоретичара и стручњака из области војних, информатичких, правних и безбедносних наука.

Проблем сукобљавања у виртуелном простору постаје, крајем прве деценије XXI века, једна од важних тема научне и стручне јавности у свим државама зависним од информационо-комуникационих технологија. Па ипак, досадашња истраживања су овом феномену приступала фрагментарно, што је за последицу имало немогућност формирања чврстог теоријског оквира и јасно дефинисаног појмовног апарата.

С обзиром на то да у научној литератури феномен кибер ратовања није обрађиван у довољној мери, и на кохерентан начин, научни циљ овог истраживања био је научно објашњење феномена кибер ратовања. Истраживање овако комплексног феномена нужно намеће мултиметодски приступ и захтева комплементарну анализу доступних и новостворених извора података. Реч је о доминантно квалитативном истраживачком приступу, а недовољна теоријска изграђеност условила је претежно експлораторну природу успостављених истраживачких захтева. Научно објашњење ове актуелне друштвене појаве подразумевало је, дакле, систематизацију досадашњих сазнања о кибер ратовању, што је претпостављало сагледавање, дескрипцију и исцрпну класификацију различитих облика сукобљавања у кибернетском простору.

Резултати истраживања указују на то да кибер ратовање јесте релативно нов и специфичан облик друштвеног конфликта који се води у специфичном окружењу,

специфичним средствима, са специфичним обележјима и принципима. Он може бити рат без жртава, али то не мора бити случај. Овај вид конфликта може се водити самостално или као подршка конвенционалном, кинетичком сукобу. Активност кибер ратовања не мора бити ограничена војним дискурсом. Принципи кибер ратовања присутни су у различитим друштвеним контекстима, мада распон мотивација и пракси може веома да варира. Протагонисти кибер ратовања користе добро промишљене тактике и стратегије како би тачно одредили мете напада и постигли своје циљеве на начин који наликује војним методама. Деструктивне акције различитих појединаца и група у кибер простору могу имати сличне пориве, показати слична схватања стратешких предности које омогућавају методе напада засноване на информационим технологијама, и бити одмазда према онима чији животи у великој мери зависе од употребе комплексних информационих и комуникационих система.

Кибер ратовање не само да преиспитује одређене конвенционалне претпоставке о природи друштвених конфликата, већ у исто време и илуструје неке од скривених могућности и парадоксалних потенцијала (социјална фузија и фисија) глобално умрежених технологија. Оно, такође, покреће мноштво питања везаних за етичност офанзивног кибер ратовања и адекватност постојећих мултилатералних прописа и конвенција у које би се ови нови модалитети морали уклопити.

Верујемо да ова, на холистичким основама спроведена анализа, доприноси и разјашњењу појмовног и терминолошког корпуса ове специфичне области. Раздвојени од својих војних корена, вокабулар и принципи кибер ратовања могу имати велику аналитичку применљивост. Различити аспекти кибер конфликата, који су у раду анализирани, могу се подвести под опште теоријске принципе и установљене карактеристике феномена који смо дефинисали појмом кибер ратовање.

На практичном нивоу, резултати истраживања могу допринети бољем разумевању ове проблематике, што је од великог значаја за развијање стратегија превенције, сузбијања и управљања безбедносним ризицима у кибер простору, како на корпоративном тако и на националном нивоу. Брз улазак „информационих конфликата“ унутар цивилних и корпоративних оквира, представља озбиљан проблем менаџерима који су одговорни за заштиту и безбедност информационе инфраструктуре. Управљачке структуре на корпоративно-економском нивоу морају бити свесне ширине спектра потенцијалних напада, укључујући савремену шпијунажу, организовани криминал, перцептивне битке, као и нападе хакера и група

спонзорисаних од стране држава или пословних конкурената. Концепт управљања безбедносним ризицима у кибер простору са аспекта националне безбедности, пак, захтева усаглашавање националног законодавства са постојећим међународним стандардима. Са аспекта регионалне и глобалне безбедности, посебно важан проблем представља непостојање опште сагласности о међународним споразумима који би разјаснили правни статус држава и недржавних актера у кибер конфликтима. Из наведених разлога, у раду је указано на потребу уједначавања нормативних приступа у циљу усвајања глобално прихватљивих правних дефиниција основних појмова у области кибер ратовања. Осим тога, представљени су предлози могућих праваца развоја међународног ратног права у циљу развијања адекватнијих механизама супротстављања и заштите од кибер конфликата.

Кључне речи: друштвени конфликти, ратни сукоби, савремено ратовање, кибер ратовање, аспекти кибер ратовања, критичне инфраструктуре, национална безбедност, заштита информационих система

Научна област: интердисциплинарне, мултидисциплинарне и трансдисциплинарне студије

Ужа научна област: студије безбедности

УДК број: 355.01:004

CYBER WARFARE - A NEW FORM OF CONTEMPORARY SOCIAL CONFLICTS

The creation of cyberspace represented a seminal turning point in the sphere of military activities, as well as in the understanding of corporate, national, regional and global security. The new "space" offered numerous possibilities for carrying out special propaganda operations and computer network based attacks on the enemy's information systems. In English-speaking countries a term "*cyber warfare*" (*kiber ratovanje)* has been coined to describe this new form of confrontation in the virtual space. Attacks in a virtual space though they seem to be insignificant, can cause numerous casualties and material devastations in real, physical world. That is why cyber warfare has a central place in the field of interest of military, information, legal and security theorists and experts.

At the end of the 21st century, the problem of conflicting in a virtual space has become one of the important topics of discussion in scientific and professional circles in all countries depending on information-communication technologies. Still, previous researches treated that phenomenon fragmentarily, and that resulted in the inability of creating a firm theoretical framework and clearly defined terminology.

Bearing in mind that scientific literature has not sufficiently and coherently explored the phenomenon of cyber warfare, a scientific aim of this research has been a scientific explanation of cyber warfare phenomenon. The research of a phenomenon this complex necessarily imposes a multi-methodical approach and requires a complementary analysis of available and newly acquired data sources. We are talking about dominantly qualitative research approach, and insufficient theoretical basis brought about mostly exploratory nature of established research requirements. A scientific explanation of this current social phenomenon meant, thus, systematization of previous knowledge about cyber warfare, which assumed recognition, description and a thorough classification of different forms of conflicts in cyberspace.

The results of the research show that cyber warfare is a comparatively new and unique form of social conflict which takes place in a specific environment, by using specific means, which has specific characteristics and principles. It can be a war without casualties, but it does not have to be like that. This form of conflict can be waged on its own, or can be a support to a conventional, kinetic conflict. The activity of cyber warfare does not have to be limited by a military discourse. Principles of cyber warfare are present

in various different contexts, though a range of motivations and practices can vary to a great extent. Protagonists of cyber warfare use very well thought-out tactics and strategies in order to precisely determine targets of the attack and achieve their aims in a way that is similar to military methods. Destructive actions of various individuals and groups in cyberspace can have similar impulses, show similar understanding of strategic advantages which enable attack methods based on information technologies, and be revenge to those whose lives depend to a great extent on the use of complex information and communication systems.

Cyber warfare not only questions certain conventional assumptions about the nature of social conflicts, but at the same time illustrates some of hidden possibilities and paradoxical potentials (social fusion and fission) of globally connected technologies. It, also, raises numerous questions related to the morality of offensive cyber warfare and adequacy of the existing multilateral regulations and conventions into which these new modalities should be adjusted.

We believe that this, holistically based, analysis helps clarifying conceptual and terminological corpus of this specific field. Devoid of its military roots, the vocabulary and principles of cyber warfare can have a great analytic applicability. Different aspects of cyber conflicts, which have been analyzed in this paper, can be assigned to general theoretical principles and established characteristics of the phenomenon we have defined by the concept “cyber warfare.”

On the practical level, the results of this research can contribute to a better understanding of this subject, which is of a great significance to developing strategies of prevention, suppression and controlling security risks in cyberspace, both on a corporate and national level. A fast entering of “information conflicts” into civil and corporate frameworks presents a serious problem to managers responsible for protection and security of information infrastructure. Managerial structures on a corporate-economy level have to be aware of how wide a spectrum of potential attacks is, including modern espionage, organized crime, perceptive battles, as well as hacker attacks, and attacks sponsored by states or business rivals. The concept of managing security risks in cyberspace from the aspect of national security, though, requires coordination of national legislation with the existing international standards. From the point of view of regional and global security, a particularly important problem is the lack of general accord on international agreements which would clarify a legal status of states and non-state actors in cyber conflicts. From the

said reasons, this paper has called attention to the need of equalization normative approaches with the aim of adopting acceptable legal definitions of basic concepts in the field of cyber warfare. Apart from that, propositions of possible directions of the development of international law of war have been proposed in order to develop more adequate mechanism of confronting and protection against cyber conflicts.

Key words: social conflicts, war conflicts, modern warfare, cyber warfare, aspects of cyber warfare, critical infrastructures, national security, protection of information systems

Scientific field: interdisciplinary, multidisciplinary and transdisciplinary studies

Specialized scientific field: security studies

UDC No. 355.01:004

С А Д Р Ж А Ј

УВОД

Убрзани развој науке и технологије, нарочито у другој половини двадесетог века, достигао је такав темпо да су се нови технолошки и културни обрасци смењивали не више на сваки век или пола века, већ сваке деценије, а пред крај те епохе и чешће. Тешко је пронаћи адекватан заједнички атрибут за претходно столеће. У различитој публицистичкој, али и научној литератури оно је називано атомским веком, веком светских ратова, веком глобалне културе и економије. Био је то и век медијâ, прва свемирска ера, епоха мултиполаризма, столеће пластике итд.

Двадесети век се сматра веком ратова јер су, у овој епохи, страдања достигла размере веће него икада раније. Процењује се да је број жртава у минулом веку био четири пута већи од броја жртава у претходна четири века. Оружане конфликте у XX веку обележило је проширење мета на цивилне објекте и, посебно, увећање броја цивилних жртава. Број цивилних жртава у односу на војне жртве потпуно је преокренут, што је навело поједине теоретичаре на закључак да је у савременим ратовима најбезбедније бити припадник војске.

На почетку двадесетог века постојало је оптимистичко веровање да су освојени поуздани темељи мира. Избијање Првог светског рата представљало је деманти таквих процена. У хладноратовском периоду, процес растуће милитаризације друштва изнедрио је идеју да се усавршавањем ратне технике феномен рата може укинути. Веровало се да се рат може учинити немогућим уколико се освоји технологија израде „оружја над оружјем“, оружја чији ће деструктивни потенцијал деловати превентивно против порива рата. Међутим, ниједно оружје – од барута, нуклеарне бомбе, до ракетног штита није оповргло логику рата. Оно је само подстицало трку за његовим ексклузивним поседовањем, или његовим ирационалним, квантитативним, увећавањем. Последица тога је и данашње улагање огромних финансијских средстава у наоружање, и бескрајно увећавање капацитета за уништење планете.

На крају двадесетог века, завршетак Хладног рата и јачање глобалних нити повезивања држава, изнова су изнедриле оптимистичке закључке да су ратни сукоби дефинитивно сишли са историјске сцене. Нажалост, и њих је потоњи ток историје у великој мери оспорио. Историја је показала да је сваки талас оптимизма био

поништаван савременијим и моћнијим средствима деструкције и њима узрокованим, новим формама насиља.

Последњу деценију XX века у међународним односима и светској политици обележили су нови видови насилних сукоба. Почетак XXI века наговестио је ескалацију недржавних асиметричних насилних сукоба. У низу локалних ратова крајем XX и почетком XXI века испољене су нове тенденције због којих их неки аутори сврставају у посебну категорију, тзв. трећу врсту сукоба, јер нису ни класични грађански ратови ни међудржавни, а тесно су повезани са фрагментацијом државе. Ову врсту сукоба одликује брисање разлике између државе и друштва, војника и цивила, рата и организованог криминала. У војне и паравојне формације регрутују се деца, спроводи се систематско уништавање културних споменика, али и социјалне инфраструктуре, као део стратегије поништавања културног идентитета и успостављања потпуне контроле над становништвом путем терора и страха. Такође су изражене тенденције развијања паралелне привреде посредством трговине ресурсима, дрогом, оружјем или пљачком. Данас, на почетку XXI века, палета сукоба обухвата низ локалних ратова уз посредно или непосредно учешће спољних актера, поновну ескалацију конфликата „замрзнутих“ пре више деценија, као и глобални рат против тероризма.

У свим досадашњим сукобима техничко-технолошки фактор је имао значајну улогу. Технолошка надмоћ значила је, у највећем броју случајева, и победу у рату. Ни данас није другачије. Тежње за освајањем нових технологија у циљу израде што деструктивнијег оружја не само да су опстале, већ су се и увећале. Може се рећи да је знање, као предуслов технолошког развоја, постало примарни и доминантни ресурс, неопходан за победу у сукобу. Технолошка креативност, дакле, није елиминисала опасности од конфликата већ их је, напротив, увећала.

Са социолошког аспекта посебно је значајан развој информационе и комуникационе технологије након Другог светског рата, јер је довео до важних промена у начину организовања и функционисања друштва. Настанак комуникационих инструмената, попут телевизије, првих генерација рачунара и сателита, не само да је повећао брзину и могућности за размену информација, већ је утицао и на промене у свим сферама друштвених активности. Настанак персоналних рачунара и стварање, прво, технолошки неусавршених локалних рачунарских мрежа, а затим и глобалне мреже – Интернета – утицали су на културну, економску и

политичку сферу друштвеног живота скоро свих технолошки напреднијих држава света. Ови информационо-комуникациони инструменти нашли су широку примену у друштву, постали су „технологија масе“, али и запослених у различитим делатностима и постепено су надмашили број радника. Рачунарске мреже су постале централни елемент друштва а, у апстрактном смислу, термин „мрежа“ је постао метафора многих аспеката модерног живота.

Ни са војног и безбедносног аспекта наведене промене нису од мањег значаја. Савремене оружане снаге се у својим активностима изузетно много ослањају на најновија технолошка достигнућа на пољу информационо-комуникационих технологија. Информациона револуција је значајно трансформисала начин на који се воде ратови у информационом добу. Она је изазвала промене, не само у начину на који оружане снаге воде оружани сукоб (у смислу борбене технике, средстава и тактике) већ и у начину на који друштва долазе у конфликт, у начину на који се „препарира јавно мњење“, задобија домаћа и међународна подршка за агресију итд.

Осим наведених улога, информационо-комуникациона технологија је почела да се злоупотребљава и на један специфичан начин. Интернет је промовисан у ново бојно поље, а рачунари и рачунарске мреже су попримили улоге средстава за извршење напада и мета напада. Информатичко ратовање је постало нови, све заступљенији облик друштвених сукоба, који се због специфичних карактеристика битно разликује од досадашњих врста ратовања. Оно се води истим средствима, методама и техникама као и кибер криминал, обавештајне активности и тероризам. У њему учествују оружане снаге, друштвене групе, корпорације али и индивидуални корисници рачунарских технологија. Из наведених разлога, научна и стручна јавност још увек није постигла сагласност по питању дефиниције овог вида ратовања.

1. ТЕОРИЈСКО-МЕТОДОЛОШКИ ОКВИР ИСТРАЖИВАЊА

1.1. Проблем истраживања

У оквиру међународних сукоба, од Другог светског рата до данас, испољена је тежња да се однос између технологије и исхода рата доведе у апсолутну корелацију, да технолошки супериорну моћ не може поразити инфериорна моћ. Када постоји асиметрија моћи, исход сукоба не може бити неизвестан. Надаље, испољена је тежња да се скрати време ратовања и да се на страни најмоћнијих сила света, уједно и најразвијених земаља, број жртава приближи нултој стопи. Назначене тежње водиле су, последњих деценија, ка постепеном премештању борбених дејстава са копна и мора у ваздух и свемир. Убрзани развој информационе и комуникационе технологије[1] у последњим декадама XX века довео је до споја машине, тј. рачунара[2] и војника, којим се физичка дистанца између супротстављених страна увећава а самим тим и равнодушност према жртвама.

Паралелно са активностима на развијању и усавршавању могућности и средстава за вођење конвенционалних сукоба кинетичким оружјем, високо развијене земље су користиле своју технолошку предност за унапређивање способности вођења специјалног рата. Распрострањена употреба телевизијске и сателитарне технологије је од шездесетих година XX века отворила нове могућности за вођење информационог рата.[3]

---

[1] Информациона и комуникациона технологија - ИКТ (*енгл*. Information & Communications Technologies – ICT) – комбинација рачунарских система и телекомуникацијских веза. ICT је скраћеница која се најчешће користи у Европи, док се у САД користи само IT (Information technologies – информационе технологије). У европском истраживачком контексту, ИКТ се понекад још дефинишу и као IST (информационо-социјална технологија). Према: *Regional Development Glossary*, http://www.emergence.nu/toolkit/glossary.php

[2] Рачунари, односно рачунарски системи, јесу електронске машине које обрађују улазне информације (податке или наредбе) и од њих производе излазне информације (резултате). Рачунарски систем чине заједно хардвер и софтвер. „Хардвер“ је назив за електронске и механичке компоненте система (*енгл*. hardware), док је „софтвер“ збирни назив за програме које користи рачунар (*енгл*. software). Према: Цигурски О.: *Информатика*, Факултет цивилне одбране, Београд, 2002, стр. 54, 65.

[3] Термин *информационо ратовање* (*енгл*. information warfare) први је употребио др Томас Рона 1976. године. Информационо ратовање обухвата било коју активност уперену против знања и система вредности одређене земље или организације. Оно се, због пропагандних делатности, често повезује са психолошким ратовањем. Информационо ратовање дефинише се као вид специјалног рата који подразумева активности усмерене на заштиту, експлоатацију, запоседање, оповргавање или уништавање информација или информационих ресурса у циљу постизања значајне предности, циља или победе над противником. Према: Alger J.: "Introduction", in Schwartau W.: *Information warfare: Cyberterrorism: Protecting your personal security in the information age*, Thunder's Mouth Press, New York, 1996, p. 814.

Историјски посматрано, информационо ратовање није нова појава. Историја људске цивилизације сведочи о бројним примерима информационог ратовања који указују на значај информације у постизању информационе супериорности у односу на противника. Израз *информација у рату* претходио је изразу *информационо ратовање*.[4] Данас се у војним доктринама већине Западних земаља синонимно употребљава и израз *информационе операције*.[5] Алвин и Хајди Тофлер су, пак, употребили појам *доктори за ефекат* (*енгл.* spin doctors) како би именовали стручњаке за информациони рат, тј. оне који стварају жељени ефекат помоћу информације, проналазећи и измишљајући начине да се она уверљиво представи.[6] Без обзира на плуралитет израза и непостојање консензуса по питању њихове употребе, можемо констатовати да сви они истичу војни аспект пропагандних активности те да реферирају на офанзивну и дефанзивну употребу информација и средстава информисања у смислу искоришћавања, поткупљивања, кварења и уништења противничких информација и система који их преносе, уз истовремену заштиту властитих информација и система. У складу са овим одређењем, може се тврдити да се вођење информационог рата, тј. информационих операција заснива на три принципа: сазнати, спречити другога да дође до сазнања, навести друге да дођу до неистинитог сазнања. Филијала Међународне асоцијације савета одбране (International Association of Defense Counsel – IADC) разликује три вида информационог рата: рат *за* информацију; рат *кроз* информацију (помоћу дезинформације) и рат *против* информације.[7]

Крај осамдесетих и почетак деведесетих година двадесетог века обележио је настанак савремених информационих система чију основу чине персонални рачунари и рачунарске мреже.[8] Распрострањена употреба рачунара и рачунарских

---

[4] Први израз односио се на тактичко и стратешко заваравање, ратну пропаганду и уништавање командних и контролних система. Пример информације у рату је употреба пропагандних форми разгледница, памфлета, говора и постера које су растурали Американци и Немци током оба светска рата. Према: Милашиновић Р., Милашиновић С.: *Увод у теорије конфликата,* Факултет цивилне одбране, Београд, 2004, стр. 289 – 314.

[5] Информационе операције су планске активности усмерене на пренос одабраних информација на страно становништво како би се утицало на јавно мњење, осећаје и објективно просуђивање, те самим тим на понашање страних влада, организација и група. Сврха информационих операција је утицање на стране ставове и понашање у циљу постизања политичких и војних циљева иницијатора информационих операција. У овим операцијама се често користе и пропагандне методе из подручја психолошког ратовања па се такве операције често називају и информационо-пропагандне активности. Према: Greenberg L., Goodman S., Soo Hoo K.: *Information Warfare and International Law*, National Defense University, Washington DC, 1998.

[6] Тофлер А., Тофлер Х.: *Рат и антират,* Paideia, Београд, 1998.

[7] International Association of Defense Counsel, http://www.iadclaw.org/books.cfm

[8] Рачунарска мрежа представља скуп рачунара повезаних одговарајућом комуникационом инфраструктуром. Она настаје повезивањем више рачунара, блиских или удаљених, помоћу мрежних контролера (мрежна картица) и/или специјалних периферијских уређаја за комуникацију (модем, рутер, бриџ итд.). Према: Џигурски О.: *Информатика*, Факултет цивилне одбране, Београд, 2002, стр. 85

мрежа у последњој декади XX века отворила је енормне могућности за вођење информационог рата. Нови борбени фронт информационог рата препознат је у тзв. кибернетском простору[9], тј. Интернету као његовом најексплоатисанијем репрезенту. Због значаја који је кибер простор попримио за вођење информационог рата, последњих је година све чешће у употреби термин *кибер ратовање*.[10]

Експанзија кибер ратовања односно информатичког ратовања, дакле, почиње у последњој деценији XX века са развојем савремених информационо-комуникационих технологија или, прецизније речено, са пуштањем Интернета у комерцијалну употребу.[11] Основна специфичност кибер ратовања јесте да бојиште

---

[9] *Кибернетски простор* или *кибер простор* (*енгл.* cyberspace) јесте виртуелни простор који настаје у контакту човека и рачунара. У свакодневном говору под тим изразом најчешће се подразумева дигитални свет конструисан уз помоћ рачунарских мрежа, попут нпр. Интернета. То место, иако заиста постоји, могло би се описати пре као комуникацијски медиј него као потпуно другачија галаксија, јер се многе од свакодневних пракси и дискурса кроз њега преламају и структуришу га кроз известан однос узајамне повезаности. Иако се кибер простор најчешће перципира као нематеријално краљевство података или као нека врста виртуелне стварности, он заправо има и сасвим физичку инфраструктуру сачињену од жица које се налазе изнад и око наших глава, каблова који леже поред наших ногу и сателита на небу који круже око наше планете; све то омогућује интеракцију која на нивоу сензација материјализује квалитет нематеријалности којим кибер простор најчешће описују његови конзументи. Кибер простор је нова форма менталне димензије људске егзистенције унутар које настаје симулирана реалност као последица интеракције између људског и артифицијелног *интерфејса.* Он представља алтернативну просторну димензију унутар које се успоставља веза између различитих персоналних рачунара, рачунарских мрежа, различитих виртуелних заједница и појединаца који могу, али и не морају да буду њихови чланови. Кибер простор се налази у перманентном процесу промене и практично може бити бесконачан у „величини“, иако унутар њега просторна и временска димензија често добијају посве померена/измењена значења. Комуникација са и унутар кибер простора се успоставља тренутно, при чему је физичка локација корисника у највећем броју случајева потпуно неважна. Има аутора који у појам кибер простор укључују и видео и телефонску трансмисију. Према: *Социолошки речник*, прир. Аљоша Мимица и Марија Богдановић, Завод за уџбенике, Београд, 2007, стр. 60.

У српском језику, међутим, област рачунарске терминологије је готово потпуно ненормирана. Због тога је чест случај да се у литератури паралелно користе два облика – „кибер“ и „сајбер“ – настала транскрипцијом грчког односно *енгл*еског корена. Академик Иван Клајн сматра да је оправдано користити термин „сајбер“ пошто се већ прилично одомаћио у српском језику управо у терминима као што су „сајбер простор“, „сајбер свет“, „сајбер секс“ и сличнима. Математичари и информатичари, пак, углавном инсистирају на термину „кибер“ као изведеници, тј. скраћеници од грчког корена „кибернетика“. Али, тиме се проблем доследности не решава, јер многи технички термини немају никакав превод на српски, већ се користе *енгл*ески термини. Због тога сматрамо да није нужно инсистирати на доследности. У овом раду смо се определили за префикс „кибер“ уважавајући препоруку комисије изречену на одбрани магистарске тезе.

[10] Изрази *информационо ратовање* и *кибер ратовање* (*енгл.* cyber warfare) се у научној и стручној литератури често синонимно употребљавају. Други појам је, међутим, ужи по обиму јер снажно наглашава рачунарске и мрежне аспекте информационог ратовања. Према: Knapp K., Boulton W.: *Ten Information Warfare Trends*, in Janczewski L., Colarik A.: *Cyber Warfare and Cyber Terrorism*, Information Science Reference (an imprint of IGI Global), Hershey, 2008, p. 25.

[11] Одлучујући потез у овом смислу представљало је дефинисање нове - World Wide Web (WWW) - архитектуре од стране CERN-а (Европски савет за нуклеарна истраживања) 1991. године. Нова архитектура је знатно поједноставила навигацију на Интернету. Године 1993. створен је и први графички инструмент за претрагу Интернета – програм *Mosaic.* Од 1994. World Wide Web је претворио Интернет у инструмент масовне комуникације.

није физички, већ виртуелни свет. Кибер ратовање се, према томе, може дефинисати као подврста информационог ратовања, којој није потребно традиционално бојно поље, већ се одвија у кибернетском простору. На кибер простор може утицати било која група која поседује рачунаре који се могу повезати у постојеће рачунарске мреже. Кибер напади неке друштвене групе могу бити усмерени на намерно убацивање дезинформација на одређене web сајтове[12], форуме[13], енциклопедије и блогове или могу бити строго усмерени према мрежној саботажи. Онемогућавање нормалног функционисања информационих система, у савременом друштву које је постало од њих зависно, може имати врло озбиљне последице на све сфере друштвеног живота. Последице могу бити чак и фаталне уколико се угрозе *критичне информационе инфраструктуре*[14] као што су, на пример, системи за контролу копненог и ваздушног саобраћаја, хидро-брана, нуклеарних електрана, безбедносних и здравствених служби или, пак, системи за дистрибуцију електричне енергије. Арсенал кибер рата (оружје које се користи за изазивање дисфункције информационе инфраструктуре)[15] веома је разноврстан и специфичан – он подразумева примену различитих информатичких инструмената, програма, и техника. Предуслов за вођење кибер рата је, дакле, поседовање информатичког знања.

Modus operandi кибер ратовања, према томе, проширен је у односу на конвенционално информационо ратовање низом активности, усмерених на софтверско угрожавање информационе инфраструктуре, док је пропагандни аспект информационог ратовања попримио форму злоупотребе Интернета као средства масовне комуникације. Кибер простор, „виртуелни свет“, на тај је начин постао не само циљ напада већ и моћно средство у рукама високообразованих „информатичких ратника“. У прилог овој тези можемо навести и чињеницу да је у савременим војним

---

[12] Web сајт (*енгл.* web site, који се чешће назива само сајт) је скуп web страница, односно докумената којима се може приступити путем World Wide Web у Интернету. За приступ web сајту неопходно је користити специјалне апликације софтвера зване web browser (на пример: Internet Explorer, Mozilla i Opera).

[13] Интернет-форум (*енгл.* Message board) јесте апликација која регистрованим корисницима неког web сајта омогућава онлајн дискусију путем порука објављених на сајту. Одређени чланови форума могу бити модератори сајта, са правом да бришу поруке или прекину писање о темама које нису у складу са правилником сајта.

[14] Критичне информационе инфраструктуре јесу информационе инфраструктуре које гарантују оперативност и тачност информатичких структура. Уништење упоришта ових структура и њихове пратеће опреме, односно нарушавање њихове оперативности током дужег временског периода, може у значајној мери угрозити безбедност популације. Према: *Regional Development Glossary*, http://www.emergence.nu/toolkit/glossary.php

[15] Информационе инфраструктуре – електронски уређаји који се могу програмирати, као и конективне и комуникационе мрежне структуре, заједно са у њима садржаним подацима. Према: *Regional Development Glossary*, http://www.emergence.nu/toolkit/glossary.php

доктринама кибер простор стекао статус петог борбеног простора, заједно са копном, водом, ваздухом и космосом. Све више аутора сматра да је „инфосфера“ простор где би се могле водити примарне борбе у будућности, а поједине државе се увелико припремају за такав концепт вођења ратова.[16]

У битно обележје кибер ратовања можемо још сврстати и тенденцију његовог померања изван војних граница на индивидуалну, друштвену и комерцијалну раван. Док је појмовно одређење информационог ратовања истицало његову војну димензију, данас већи део литературе о кибер ратовању истиче аспект његовог проширења ван војних области.[17] Проширење делокруга кибер ратовања изван војних активности је, у техничком смислу, омогућено дифузном и децентрализованом структуром глобалне рачунарске мреже – Интернета. Суштински, феномен сукобљавања у кибер простору помоћу оружја које нуди сам кибер простор, и његово преливање у сфере „цивилног“ света узроковано је противречном природом процеса глобализације и идеолошким, политичким, културним и социјалним диспаритетима које овај процес носи.

Информационо-комуникационе технологије на глобалном нивоу увећавају улогу држава, организација, мултинационалних компанија, невладиних организација, транснационалних криминалних организација и, чак, појединаца у међународној арени.[18] Савремене технологије омогућавају ширење информације али и дезинформације, фаворизују културну и економску интеграцију (или дезинтеграцију) и дају визибилност и хитност догађајима, где год да се они дешавају у тзв. глобалном селу. Природа кибер простора је таква да се токови информација могу тешко ограничити и контролисати. Може се рећи да кибер простор не познаје политичке и географске границе. Две тачке су увек близу без обзира на дистанцу која их раздваја, веза између два удаљена рачунара има исте потешкоће које може имати веза у једној згради. То са једне стране узрокује интензивирање односа између

---

[16] *L' Armement*, No. 60, XII., Paris, 1997 - I. 1998.; *From cybercrime to cyberwarfare*, “Défense nationale et sécurité collective”, No 6, The Committee for National Defence Studies, Paris, 2008.

[17] Cronin B., Crawford H.: “Information warfare: Its applications in military and civilian contexts”, *Information Society*, 15(4), 1999.; Hutchinson W.: “Concepts in information warfare”, *Logistics Information Management*, 15(5/6), 2002.

[18] Williams P.: “Transnational Criminal Organizations and International Security”, y: Arquilla J., Ronfeldt D. F.: *Cyberware is coming!, Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, 1997, p. 329, http://www.rand.org

међународних актера, а са друге, лаку дистрибуцију нежељених информација. Из тог разлога неке владе су, чак, одлучиле да усвоје рестриктивне политике или да својим грађанима онемогуће приступ Интернету.[19]

Државе које се ослањају на информационе технологије изложеније су и рањивије на било који облик штетне преправке, прекида или уништења технологија од којих зависе информациони токови као што су, на пример, индустријска друштва рањивија од аграрних друштава по питању континуираног снабдевања енергијом.

Неједнака доступност и способност коришћења информационих технологија, са друге стране, продубљује јаз између богатих и сиромашних друштава.[20] Овај јаз је присутан како на међудржавном, тако и на унутардржавном нивоу. Уколико би технолошки јаз наставио да се шири, осећај ускраћености код сиромашних популација могао би изазвати унутардржавне, али и међународне тензије.

Безбедносне претње у савременим околностима су, дакле, асиметричне.[21] Земље са нижим нивоом зависности од нових технологија не само да су мање рањиве, већ могу да искористе рањивост развијенијих земаља за достизање својих стратешких циљева. Могућност извршавања деструктивних акција је, са економске тачке гледишта, све доступнија. Развијање офанзивних стратегија у кибер простору не захтева високе инвестиције, попут оних неопходних за конвенционално ратовање и, изнад свега, ове стратегије доступне су великом броју актера. За разлику од технолошки софистицираног оружја, кибер оружје могу развијати појединци или

---

[19] У том смислу најбољи пример је Кина, земља са тоталитарним режимом, која је међу првима схватила и значај Интернета и важност његове контроле од стране државе. Она је једна од ретких земаља која је успела да споји два контрадикторна аспекта – да фаворизује приступ Мрежи (тренутно има око 130 милиона корисника) и да, истовремено, спроведе контролу над информацијама, која подразумева потпуну блокаду било какве критике режима на web-у. У основи овог успеха налази се знаачко дозирање технологије (распрострањена употреба инструмената за филтрирање садржаја), репресија, цензура и обесхрабривање (у 20 провинција раде посебна полицијска одељења обучена да прате „субверзивне" кориснике). Информација преузета из: Reporters Without Borders, http://www.rsf.org

[20] Реч је о такозваном „дигиталном јазу" (*енгл.* digital divide). Овим изразом се означава разлика између оних који имају способност и могућност приступа информационим технологијама и оних који ту могућност немају. Дигитални јаз постоји између становника градова и становника руралних крајева, између образованих и мање образованих, између нижих и виших социјалних класа и, глобално, између развијених и мање развијених земаља.

[21] Vatis M. A.: *Cyber attacks during the war on terrorism: a predictive analysis*, Institute for Security Technology Studies at Dartmouth College, September 22, 2001, http://www.ists.dartmouth.edu

групе за шта су им једино потребни знање и мотивација. То омогућава државама или актерима којима до сада није придаван значај у стратешком контексту, да теже другачијој позицији у кибер простору, где знање одређује равнотежу моћи пре него количина војног арсенала.

Осим тога, у кибер простору је мање изражена веза између безбедности и територије. Геополитичка позиција која је одувек била централни, средишњи, елемент безбедносне политике државе постепено губи свој значај. Данас није више неопходно физички ући у неку територију, нити је напасти кинетичким оружјем. Дакле, комплетна контрола физичких ентитета као што су ваздушни или копнени простор није довољна да гарантује безбедност једној држави. Војна надмоћ не значи сигурност у кибер простору где је неопходно развити нове стратегије одбране кибер инфраструктуре, што је посебно тешко због типичног амбигвитета кибер напада. Уколико је кибер напад извршен професионално, врло је тешко одредити порекло извршиоца и мотивације из више разлога:

- сачувати анонимност у кибер простору је технички врло лако;
- напад се може извршити из било ког дела света или, ако је неопходно, и са више тачака у исто време;
- последице напада се могу манифестовати након дужег временског периода, спречавајући тако откривање средстава и актера;
- време између откривања нове рањивости и стварања офанзивних информатичких инструмената који се могу применити за извршење напада све је краће, захваљујући усавршавању моћи рачунара;
- технологија која се користи за нападе релативно је једноставна за коришћење и врло је економична;
- инструменти и технике за извршавање напада могу се лако наћи у кибер простору;
- учинковитост напада је све већа захваљујући аутоматизацији и софистицираности метода напада – само један напад може изазвати тешке последице.

Као што је раније поменуто, претња кибер рата није лако уочљива нити се актери претње могу лако категоризовати. Првенствено, не постоји јасна идентификација актера – сваки члан „електронске друштвене заједнице“ је потенцијални противник. Непријатељске државе, војни савези, терористи, незадовољни радници, обесни појединци, комерцијална или индустријска предузећа, политички активисти и криминалне организације само су примери могућих актера.

Сваки од ових актера мотивисан је различитим циљевима, ограничен различитим нивоима ресурса, сопственим могућностима и могућностима система да се брани. Тешко је пронаћи евидентне доказе у вези са непријатељским намерама могућих нападача и проценити њихове реалне способности да изведу напад на тако широком нивоу да угрозе безбедност државе.

Информационо ратовање је у прошлости сматрано искључиво војним питањем. Настанком кибер простора, истакли смо, проширује се скуп активности које се подводе под појам информационог ратовања и уводи се у употребу термин кибер ратовање. Такође, у кибер простору је изражена и тенденција преношења ових активности ван војних оквира. Различити видови конфронтације у кибер простору, сукобљавања различитих друштвених актера помоћу специфичног, кибер оружја, промовисали су феномен кибер ратовања у друштвено питање. Појам кибер ратовање се, у актуелним научним тематизацијама ове појаве, употребљава као збирни назив за свеукупност поменутих активности и тенденција.

Термин кибер ратовање се, дакле, употребљава да опише широк распон активности на индивидуалном, друштвено-социјеталном, корпоративно-економском и војном нивоу. Под ове активности могу се сврстати, на пример, хактивизам[22], фишинг,[23] покретање напада усмерених на опструкцију услуга (Denial of service – DoS и Distributed denial of service - DDoS)[24] као и развијање војних дефанзивних и

---

[22] Под изразом *хактивизам* подразумева се идеолошки мотивисано извођење информатичких напада. Реч је о борби која се води на електронском пољу или, другачије речено, о хактивистичким групама чије је деловање усмерено против електронских контролних и информационих система и технологија непријатељских земаља. Хактивисти у кибер простору виде инструмент којим недржавни актери могу да учествују у конфликтима ван националних граница. Према: Denning D.: „Cyberwarriors, Activists and Terrorists Turn to Cyberspace“, *Harvard International Review*, Vol. XXIII, No. 2, Summer 2001, pp. 70-75. Пример хактивизма био би напад који је извршила албанска хакерска група са Косова на сајт Министарства пољопривреде Републике Србије 4. августа 2008. године. Да подсетимо, претходних дана извршено је неколико сличних напада на сајтове: Српске православне цркве, Скупштине Црне Горе, авио-компаније „Монтенегро ерлајнз“ и дневног листа „Вијести“. Извор: агенције *FoNet* и *Tanjug*, 4. август 2008.

[23] Термин *фишинг* користи се да опише поступак илегалног прикупљања осетљивих информација у кибер простору, помоћу техника обмане. Фишинг напади, дакле, подразумевају активности којима злонамерни актери коришћењем лажних порука електронске поште и лажних web страница финансијских организација покушавају да наведу корисника на откривање поверљивих личних података. Према: *Know your enemy: phishing – Behind the scenes of phishing attacks*, The Honeynet Project & Research Alliance, http://www.honeynet.org

[24] Кибер напади под називом *лишавање услуге* (Denial of service - DoS) и *дистрибуирано лишавање услуге* (Distributed denial of service - DDoS) имају за циљ да онемогуће клијенте или организацију да користе услуге рачунарске мреже или информационих ресурса. Опструкција електронских услуга постиже се нападом на системе који омогућавају те услуге (на пример, нападом на сервер на коме су ускладиштени web сајтови или на сервер електронске поште). Најчешће коришћен метод за извођење ове врсте напада је излагање рачунара или рачунарских мрежа огромном броју захтева концентрисаних у кратком временском периоду.

офанзивних оперативних способности. Повезаност између ових различитих „светова“, наравно, није непропусна - аматери постају стручњаци, стручњаци продају своје услуге, терористи усвајају методе које су употребиле криминалне организације итд. Међутим, мотивација актера, употребљени ресурси и, надасве, потенцијални ризици по безбедност друштва умногоме се разликују.

Употреба израза кибер ратовање за описивање савремених сукоба у кибер простору може се чинити непримереном у односу на традиционално поимање рата као организованог, интензивног конфликта између држава, савеза држава, етничких и верских група или класа средствима оружаног насиља у циљу остваривања одређене политичке, војне и друге добити. Тешко је говорити о стварном рату, кад такве операције немају конкретне последице у смислу физичке штете или губитка људских живота. Чињеница је да хакинг банке има само ограничен економски учинак. Модификација web странице неке институције тек изазива љутњу или губитак пословног угледа. Што се тиче терористичких група, оне употребљавају Интернет за комуникацију, регрутовање, припремање и финансирање операција. У том смислу оправдана је констатација да се терористички напади још увек спроводе помоћу експлозива а не помоћу информатичких кодова. Традиционални начин је јефтинији и има више утицаја на јавно мњење.

И поред тога, претња од кибер рата је присутна а ризик од ескалације ове врсте конфликта се увећава те га не би требало подцењивати. На ову чињеницу указали су рачунарски напади које је трпела Естонија током априла и маја 2007. године.[25] Природно, тип напада (*дистрибуирано лишавање услуге* - DDoS) био је релативно конвенционалан и од почетка се чинило да је резултат хактивизма. Ово је био први случај да су политички, медијски и економски елементи унутар земље били истовремено на мети, доводећи до привремене паралисаности државе. Ово је такође био први случај да је конфликт у кибер простору попримио политичку димензију која је могла да ескалира у ратни сукоб: неколико дана након напада, естонски министар спољних послова је као виновника напада оптужио руску владу

[25] Напад је почео 9. маја 2007. године, био је усмерен на опструкцију званичних Интернет сајтова Естоније, једне од најинформатизованијих земаља на свету. Током неколико недеља, колико је напад трајао, Естонија се носила са по обиму најширим нападом ове врсте до сада. Услед напада, сајтови естонске владе (Министарства иностраних послова и Министарства правде), медија и банака били су блокирани**.** Овај напад дистрибуираног лишавања услуге подстакао је интензивне расправе о безбедности кибер простора на међународном нивоу. Према: *BBC NEWS*, Published: 2007/05/02, http://news.bbc.co.uk/go/pr/fr/-/2/hi/europe/6614273.stm; *The economist*, Published: May 10, 2007, http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598; *Telegraph*, Published: 19/05/2007, http://www.telegraph.co.uk

захтевајући примену члана 5 НАТО-а који предвиђа колективну одбрану нападнуте земље.[26] Ово је, стога, био и први пут да је суверенитет државе био директно угрожен рачунарским нападом, који је био спроведен од стране недодирљивог непријатеља.

Гледано из историјске перспективе, преокрет у перцепцији претње кибер ратовања наступио је оног тренутка када су рачунарски напади погодили системе контроле који су „срца“ критичне инфраструктуре.[27] Системи контроле пружају повезаност између реалног и виртуелног света. Било који хакерски напад на DCS и SCADA системе могао би имати драматичне последице. На срећу, за сада је евидентирано само неколико успешних напада против ових система. Али њихова растућа међуповезаност унутар Интернета и употреба стандардних протокола из економских разлога, али и из разлога повећања узајмне оперативности, знатно повећавају ризик.

Кибер ратовање је стога, у дословном значењу термина, постало реалност. За овај вид сукобљавања тренутно се припрема преко 120 држава, али и Северноатланска алијанса, развијајући војне доктрине и стратегије кибер ратовања.

1.1.1. Досадашња искуства и уочени проблеми у научној тематизацији проблема истраживања

Анализа феномена кибер ратовања везана је за јавно доступне информације из такозваних отворених извора, јер се готово ништа не зна о истраживањима националних и наднационалних обавештајних агенција, нарочито када се говори о намерама, мотивацијама и способностима протагониста кибер рата.

Реално сагледавање феномена кибер ратовања отежано је и „сликом“ коју стварају медији, где расправа о овим питањима поприма алармантан и сензационалистички тон. Уопштено, можемо констатовати да се концепту кибер рата у

---

[26] Да подсетимо, први и једини пут Алијанса је активирала члан 5 Северноатлантске повеље, 12. септембра 2001. године, као одговор на терористичке нападе на САД од претходног дана.

[27] Међу системима контроле два су посебно битна за безбедност критичних инфраструктура: 1) дистрибуирани систем управљања (*енгл.* Distributed Control Systems – DCS), који се користи у појединачним структурама или малим географским областима, и 2) систем за прикупљање, пренос и контролу података и аутоматизацију и управљање индустријским процесима (*енгл.* SCADA), који се најчешће користи у пространим географским областима. Према: *Supervisory Control and Data Acquisition (SCADA) Systems*, National Communications System, 2004, p. 12, http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf

водећим Западним мас-медијима, али све чешће и код нас, придаје врло велики значај и када је реч о онима који га афирмишу и када се говори о онима који су жртве. Реторичка драматизација се често користи и даје општи утисак да претња кибер ратом постаје све већа и опаснија.

Проблем несигурности кибер простора постао је, почетком XXI века, једна од важних тема научне, стручне али и шире јавности у свим технолошки развијеним земљама. У прилог овој тврдњи говоре све учесталије научне тематизације овог проблема[28], али и спроведене законодавне реформе у одређеним земљама, затим семинари, пројекти и скупови на националном и међународном нивоу[29], као и бројне јавне дебате о потреби редефинисања стратегија за заштиту кибер простора. На основу претходно реченог може се констатовати да је претња кибер ратом веома актуелан друштвени проблем који захтева свестрану научну анализу.

Међутим, на основу увида у доступну домаћу[30] и иностранu[31] научну и стручну литературу можемо констатовати да је приметан фрагментаран приступ у

---

[28] Palmar I. C., Potter G. A.: *Computer security risk magement*, Jessica Kingsley Publishers, London, 1989; Alberts David S. and Papp Daniel S.: *The Information Age: An Anthology of Its Impacts and Consequences*, Volume III, National Defense University Press, Washington D.C., 2001; Arquilla J., Ronfeldt D. F.: *Cyberware is coming!* In Athena's Camp: *Preparing for Conflict in the Information Age*, Santa Monica 1997, http://www.rand.org; Virilio P., in Der Derian J.: "Speed pollution", *Wired*, http://www.wired.com; *Control systems cyber security awareness*, http://www.cert-us.gov; Datz T.: *Industrial Control Systems: Out of Control?*, http://ses.symantec.com; Denning D.: *Is Cyber Terror Next?*, http://www.ssrc.org/sept11/essays/denning.htm; Skoudis Ed: *Counter Hack: A Step-By-Step Guide to Computer Attacks and Effective Defenses*, New Jersey, Prentice Hall, 2002.

[29] 2003 World Summit on the Information Society, *Declaration of principles building the Information Society: a global challenge in the new millennium*, document WSIS- 03/GENEVA/DOC/4-E, www.itu.int; 2003; World Summit on the Information Society: *Plan of action*, document WSIS-03/GENEVA/DOC/5-E, http://www.itu.int; UK National Infrastructure Security Co-Ordination Centre, "The UN Resolution on CIIP", *The Quarterly*, No. 2, http://www.niscc.gov.uk/; *UK Terrorism act 2000*, http://www.opsi.gov.uk; G8, "Okinawa charter on global information society", G8, Okinawa, http://lacnet.unicttaskforce.org/; *An Analysis of Issues and Options*, http://csrc.nist.gov; T*he Report of the President's Commission on Critical Infrastructure Protection*, cover letter, http://www.securityfocus.com

[30] Из прилично оскудног домаћег фонда издвајамо: Вулетић Д.: „Шта је информационо ратовање?", *Безбедност*, број 3/'05, Београд, 2005; Синковски С.: „Информациона безбедност – компонента националне безбедности", *Војно дело*, број 2/2005, ВИЗ, Београд, 2005; Петровић С.: „Кибертероризам", *Војно дело*, број 2/2001, ВИЗ, Београд, 2001; *Безбедност и информационе технологије: нова средства и изазови*, Парламентарни надзор безбедносног сектора: начела, механизми и пракса, Приручник за посланике број 5, Центар за цивилно-војне односе, Београд, 2003

[31] Janczewski L., Colarik A.: *Cyber Warfare and Cyber Terrorism*, Information Science Reference (an imprint of IGI Global), Hershey, 2008; Denning D.: *Information Warfare and Security*, Addison-Wesley, 1999; Arquilla J., Ronfeldt D.: *Networks and Netwars: The Future of Terror, Crime, and Militancy*, RAND, Santa Monica, California, 2001; Fialka J.: *War by Other Means: Economic Espionage in America*, W.W. Norton, New York 1997; Greenberg L., Goodman S., Soo Hoo K.: *Information Warfare and International Law*, National Defense University, Washington DC, 1998; Denning D.: "Cyberwarriors, Activists and Terrorists Turn to Cyberspace", *Harvard International Review*, Vol. XXIII, No. 2, Summer 2001, pp. 70-75, http://www.hir.harvard.edu.

истраживању ове тематике. Проблем који се, дакле, поставља пред истраживача је непостојање јасно дефинисаног појмовног апарата и чврстог теоријског оквира.

1.2. Предмет истраживања

С обзиром на уочене недостатке у досадашњој тематизацији проблема истраживања, сматрамо да је неопходно заузети холистички приступ у истраживању феномена кибер ратовања. Такав би приступ подразумевао интегративно проучавање које би обухватило све димензије ове комплексне појаве. Узимајући у обзир фрагментарност досадашњих истраживања, недовољну развијеност теоријског оквира и непостојање јасно дефинисаних основних појмова, ми смо се усредсредили на исцрпну дескрипцију и класификацију манифестних облика овог феномена са аспекта безбедносних наука у циљу синтетизовања полазне грађе за будуће теоријске и емпиријске радове који ће се бавити овом тематиком.

На основу прегледа литературе (од 1990. до 2011. године), могу се уочити одређене, битне, тенденције кибер ратовања. Намера нам је да интегришемо тенденције у један оквир показујући тиме како се кибер ратовање помера изван војних граница на индивидуалну, друштвену и комерцијалну раван.

На основу претходно формулисаног проблема, предмет овог истраживања се може дефинисати као **идентификација и класификација савремених облика сукобљавања у кибер простору**.

1.2.1. Операционално одређење предмета истраживања

Истраживање комплексног садржаја феномена кибер ратовања реализовано је кроз четири фазе, тј. поглавља.

Прво поглавље (општи део рада) односи се на друштвени контекст у коме настаје феномен кибер ратовања. У том смислу, ово поглавље садржи генезу и теоријско одређење кључних појмова: информациони системи, кибер простор, Интернет, информационе инфраструктуре и информационо друштво. Овај део рада, такође, садржи кратак осврт на теоријска сазнања о природи, узроцима и елементима друштвених конфликата. Објашњени су критеријуми класификације конфликата, као и критеријуми категоризације екстремних видова сукоба – ратних конфликата. Посебан акценат стављен је на објашњење одлика савремених друштвених

конфликата кроз призму техничко-технолошког развоја и стратешког контекста информационог доба.

Након тога, у другом поглављу, приказана је генеза концепта кибер ратовања. Феномен кибер ратовања је, затим, анализиран у складу са приступом конфликтолошке анализе која подразумева засебно, рашчлањено, проучавање елемената структуре конфликта. На овај начин дошло се до егзактних сазнања о актерима кибер ратовања, објектима кибер ратовања и методама и средствима који се користе приликом конфронтација у кибер простору.

У трећем поглављу извршена је класификација активности које подразумева кибер ратовање на основу мотивације субјеката и циља који се жели постићи, као критеријума класификације. У том смислу, покушали смо да синтетизујемо досадашња научна сазнања о овом феномену те да детаљно опишемо четири до сада препозната аспекта кибер ратовања.

У четвртој целини су, на систематичан начин, елаборирane будуће тенденције ове појаве. У овом поглављу су, такође, приказане мере и активности које су до сада предузете у циљу супротстављања претњи кибер рата на националном и међународном нивоу. Осим тога, у овом поглављу су размотрене и могућности превенирања сукоба у кибер простору са техничког и законодавног аспекта.

1.2.1. Временско и просторно одређење предмета истраживања

Предмет истраживања, са временског аспекта, обухвата период од настанка глобално умреженог друштва до данас. За почетак глобалног умрежавања узима се 1994. година када је *World Wide Web* претворио Интернет у инструмент масовне комуникације.

Са аспекта физичког, еуклидовског простора, предмет истраживања се односи на целокупну екумену информационог друштва. Са аспекта нееуклидовског простора, предмет истраживања се односи на кибер простор.

1.2.2. Дисциплинарно одређење предмета истраживања

Предмет истраживања тематски припада већем броју научних дисциплина. Он обухвата сазнања и проблеме социологије, наука безбедности, информационих и

математичких наука и њихових посебних дисциплина (као што су криптографија и криптоанализа), војних, правних, криминалистичких и криминолошких наука, што несумњиво упућује на његов интердисциплинарни карактер.

1.3. Циљеви истраживања

С обзиром на то да је у домаћој научној литератури феномен кибер ратовања недовољно обрађиван, научни циљ овог истраживања био је научно објашњење феномена кибер ратовања. Научно објашњење ове актуелне друштвене појаве подразумевало је систематизацију досадашњих сазнања о кибер ратовању што је претпостављало сагледавање, дескрипцију и исцрпну класификацију различитих облика сукобљавања у кибернетском простору.

Спроведена анализа може, такође, да допринесе разјашњењу појмовног и терминолошког корпуса ове специфичне области.

На практичном нивоу, резултати истраживања могу допринети бољем разумевању ове проблематике, што је од великог значаја за развијање стратегија превенције, сузбијања и управљања безбедносним ризицима у кибер простору како на корпоративном нивоу тако и на националном нивоу.

Брз улазак „информационих конфликата“ унутар цивилних и корпоративних оквира, тј. експанзија кибер ратовања у комерцијални свет, представља озбиљан проблем менаџерима који су одговорни за заштиту и безбедност информационе инфраструктуре. Управљачке структуре у комерцијалној и привредној делатности морају бити свесне ширине спектра потенцијалних напада, укључујући савремену шпијунажу, организовани криминал, перцептивне битке, као и нападе хакера и група спонзорисаних од стране држава или пословних конкурената.

Концепт управљања безбедносним ризицима у кибер простору са аспекта националне безбедности, пак, захтева усаглашавање националног законодавства са постојећим међународним стандардима. С обзиром на неминовност предстојеће убрзане информатизације нашег друштва, процес стандардизације у овој области намеће се као један од приоритета националне безбедности.

1.4. Хипотетички оквир истраживања

С обзиром на претежно квалитативни и експлоративни карактер овог истраживања, оно је засновано на генералном, широком и неспецифичном хипотетичком оквиру који обухвата испитивање сета следећих претпостављених односа:

1. Настанком кибер простора проширује се скуп активности које су традиционално биле подвођене под појам информационог ратовања.
2. Растућа друштвена зависност од кибер технологија повећава његову изложеност опасним изворима претњи кибер ратовања.
3. Идентификовани облици кибер ратовања траже редефинисање постојећих стратегија за одговор на њих.

1.5. Методе истраживања

Начин истраживања и избор метода одређени су дефинисаним проблемом истраживања, теоријским и операционализованим предметом истраживања, претпостављеном хипотетичком основом и комплексношћу предмета истраживања.

Истраживање овако комплексног феномена нужно намеће мултиметодски приступ и захтева комплементарну анализу доступних и новостворених извора података. Реч је о доминантно квалитативном истраживачком приступу, а недовољна теоријска изграђеност је условила претежно експлораторну природу успостављених истраживачких захтева.

Дефинисани предмет истраживања захтевао је употребу одговарајућих научних метода којима су обухваћени сви релевантни извори сазнања. Феномен кибер ратовања и његови појавни облици сложено су поље за проучавање, и за њихову ваљану и обухватну анализу неопходно је користити различите методе и теоријска знања из више научних дисциплина.

Због комплексности проучаваног феномена, у раду смо анализирали податке из различитих извора. Постојећи извори података из којих се креирала базична искуствена евиденција јесу:

- научни и стручни радови који се, посредно или непосредно, баве феноменом информационог, тј. кибер ратовања;
- научни и стручни истраживачки пројекати из ове области;

- позитивноправни прописи (национални, регионални и међународни);
- институционални извори (статистички извештаји, документа из архива државних институција, евиденције невладиних организација, извештаји осталих релевантних институција);
- евиденције државних и међународних тела задужених за праћење криминалитета;
- међународни документи, конвенције, протоколи, међународни уговори и други акти, који су директно или индиректно везани за проблем безбедности кибер простора.

Затим, током истраживања, пре свега путем метода анализе садржаја различитих облика комуникација, стварана је искуствена грађа релевантна за извођење закључака о испитиваној појави.

У циљу постизања што већег степена поузданости и обухватности, ово истраживање је обухватило како анализу различитих извора података, тако и комплементарно коришћење различитих истраживачких метода:

1. преглед научне и стручне литературе;
2. анализа правних докумената;
3. метод секундарне анализе;
4. метод анализе садржаја;
5. принцип триангулације.

Преглед научне и стручне литературе

Преглед литературе представља метод којим се на систематичан и објективан начин долази до постојећих сазнања, резултата и налаза о предмету истраживања остварених у одговарајућим научним дисциплинама. Применом овог метода дошли смо до релевантних сазнања о различитим теоријским становиштима и приступима у проучаваној области и постојећим научним знањима о предмету нашег истраживања.

За потребе конципирања овог истраживања углавном су била коришћена и анализирана иностранa литература и истраживачка искуства (већи број стручних књига, монографија, студија, приручника и чланака). У нашој литератури проблем кибер ратовања врло је ретко обрађиван. У постојећој, штурој домаћој литератури проблеми везани за ову појаву нису свеобухватно нити на систематски начин тематизовани, те је домаћа литература, углавном, коришћена за разматрање основних појмова и националне законске регулативе.

Анализа правних докумената

Анализа правних докумената је у овом истраживању обухватила примену правно-догматског и нормативног метода.

Правно-догматски метод се користи за научну обраду нормативних садржаја. Њиме се врши тумачење садржине правних норми у циљу сазнавања правог значења језичко-логичких симбола којима су оне изражене. Применом овог метода правне науке анализирали смо домаће и, упоредно, међународне позитивноправне прописе којима се санкционишу деликти против безбедности информационих система и кибер простора. Нормативна акта која су била анализирана у овом истраживању односе се како на домаће, тако и на иностранo законодавство, пре свега на нормативу Сједињених Америчких Држава, Велике Британије и Европске уније.

Нормативни метод се користи за научну анализу правних система и његовом применом се изграђују основни правни појмови и утврђују њихове међусобне везе. Овим смо се методом служили приликом обраде, анализе и синтезе правних појмова.

Метод секундарне анализе

Многи документи, створени у различите сврхе послужили су нам као извори сазнања о посматраној појави. Овим методом смо анализирали постојећу искуствену евиденцију из доступних архивисаних база података из до сада спроведених научних истраживања у области кибер ратовања, као и званичне евиденције релевантних цивилних и војних институција, текстове из новина, извештаје и другу документарну грађу. Употреба метода секундарне анализе података била нам је посебно значајна јер, из објективних разлога, нисмо у прилици да спроводимо истраживања у којима би учесници били актери кибер рата.

Основни проблеми примене секундарне анализе података јесу веродостојност и поузданост података који се анализирају. Ова чињеница је наметала посебан опрез у избору извора података и детаљну проверу њихове адекватности и објективности. У том циљу је спровођена континуирана евалуација постојећих података намењених секундарној анализи, анализирани су циљеви због којих су настали, начини узорковања, операционалне дефиниције и методе прикупљања података.

Метод анализе садржаја

Материјал докумената масовне комуникације обрађен је методом анализе комуникационог садржаја. Материјал је прикупљен на систематски начин, из различитих медијских садржаја – новина, часописа, филмова, радија, телевизије и Интернет сајтова.

При коришћењу методе анализе комуникационог садржаја примењивана је техника ,,узорак популарности“, која се базира на опсегу публике. Извођење узорка у комуникационим анализама извршено је у три фазе:

1. Разврставање извора (које штампане медије, које електронске медије итд., треба анализирати);
2. Разврставање временских секвенци (који период треба покрити истраживањем);
3. Разврставање јединица (које аспекте комуникација треба анализирати).

Принцип триангулације

Основни истраживачки принцип којим се руководило ово истраживање био је принцип комплементарности, односно триангулације. Овај истраживачки принцип захтева комплементарну примену различитих извора података, начина њиховог прикупљања и анализе, типа истраживачке стратегије, теоријских перспектива. Тиме се постиже методолошка свестраност, креира адекватан методолошки приступ, повећавају поузданост и ваљаност истраживања.

У циљу свеобухватног сагледавања феномена кибер ратовања и његових различитих појавних облика примењене су различите методе истраживања, а подаци добијени коришћењем сваке од њих омогућили су анализу различитих аспеката везаних за овај проблем. Поштовање овог принципа омогућило је проверу и употпуњавање података добијених различитим методским приступима, чиме су у извесној мери, умањени недостаци у примени појединачних метода.

2. КАРАКТЕРИСТИКЕ РАТНИХ СУКОБА НА РАЗМЕЂУ ВЕКОВА

Рат као феномен је био предмет истраживања многих наука, првенствено историје, права и политике. Данас се питањима рата баве бројне друштвене науке попут: историје, социологије, војних наука, наука о међународним односима, међународног јавног права и економских наука али и неке природне и техничке науке. Свака научна дисциплина настоји да, из свог угла, дефинише рат и идентификује његове основне карактеристике и законитости.

Традиционално поимање рата подразумева постојање одређених, основних, обележја и карактеристика овог феномена. У том смислу, сматра се да је рат, а пре свега онај нападачки, увек продукт политичких интереса државе која њиме настоји да их реализује, а ти политички интереси најчешће у себи сублимирају одређене економске интересе. Другим речима, рат је средство коме се прибегава ради остварења унапред дефинисаних политичких интереса, односно онда када се ти интереси не могу остварити применом других средстава принуде и притисака.

Осим тога, опште је прихваћено становиште да рат представља оружани сукоб између организованих политичких субјеката (држава, устаници, снаге Уједињених нација итсл.). Овај организовани облик насиља се врши помоћу оружја (оружане силе) да би се скршио отпор противника и остварио интерес због којег се води.

Међу основне карактеристике рата још се сврстава и та да је рат израз воље једне од зараћених страна која је потребна да би се створило ратно стање. Међутим, забележен је велики број случајева када су се државе налазиле у стању рата а да то стање нису прогласиле. Рат, као специфичан друштвени однос између зараћених страна, је уређен уговорним и обичајним правилима међународног ратног права. Стране у сукобу су обавезне да се понашају у складу са његовим правилима и правно су одговорне за њихово кршење. Важно је подсетити се да је савремени међународноправни поредак ставио нападачки рат ван закона и прогласио га међународним злочином, док је легалност употребе оружане силе редуковао само на

случајеве индивидуалне или колективне самоодбране, односно колективне акције Уједињених нација у складу са Главом VII Повеље УН.[32]

Међутим, револуционарни развој ратне технике последњих деценија радикално је изменио физиономију и стратегију ратовања која је стављена у функцију брзог сламања отпора противника, тако да се све чешће поставља питање могу ли се многобројни оружани сукоби, вођени у свету, поистоветити са ратом у његовом традиционалном значењу. Ову дилему подстиче и околност да се ратови одавно не покрећу применом класичне процедуре - њиховом објавом, да се примена оружане силе врши редуковано и да се она најчешће оправдава ограниченим политичким циљевима. У том смислу Зоран Вучинић пише: „Данас су скоро ретки случајеви да оружани сукоби почињу на вековима устаљен начин, тј. сударом комплетних армија сукобљених страна. Пракса великих сила, такође, показује да оне, по правилу, такве сукобе започињу употребом одређених видова и родова, а тендеција њихове војне стратегије све више се креће ка сламању отпора противника дејством различитих врста оружја са велике дистанце, дакле без употребе пешадије.“[33]

2.1. Рат као екстремна форма друштвених конфликата

2.1.1. Појмовно одређење друштвених конфликата

Друштвени конфликти су једна од најупечатљивијих карактеристика историје људског рода. Они су историјска али и актуелна константа људских заједница, те су као такав феномен од давнина привлачили пажњу теоретичара из области филозофије, историје, права, психологије, социологије, војних и других наука. Данас, услед изражене специјализације наука конфликти, или барем одређене врсте конфликата и њихови посебни појавни облици, постају предмет изучавања уско специјализованих научних дисциплина. Легитимност оваквих приступа проистиче из чињенице да су конфликти присутни, и да ће вероватно бити присутни,

[32] Вучинић З.: *Међународно ратно и хуманитарно право*, Службени гласник, Београд, 2006, стр. 51.
[33] *Ibid.*, стр. 52.

у сваком социјалном окружењу, у сваком облику људског организовања, без обзира на комплексност организационе структуре.

Једну јединствену, потпуну и свеобухватну теорију друштвених сукоба досадашњи развој друштвених теорија није пружио. Постоје, наиме, само одређени садржаји и модели, превасходно услед различите природе конфликата, њихових узрока, функција, фаза, циљева, начина њиховог регулисања и разрешавања.

Теоријска мисао о друштвеним сукобима има дугу историју и веома широк распон. Полазећи од различитих критеријума у литератури која се бави питањима друштвених сукоба, теоријски дискурс је веома широк - од теолошких, моралистичких, биолошких, природноправних, утопистичких и геополитичких учења до различитих варијанти психолошких, социопсихолошких и социолошких теорија, затим математичких теорија, а у оквиру њих различитих варијанти микро и макро теорија сукоба.

Интерес социологије за проблем друштвеног сукоба, значајног поља социолошког истраживања, варирао је од придавања велике пажње од стране класичне социолошке мисли деветнаестог века, преко релативног слабљења интереса у периоду педесетих година XX века, када је нарочито у Америци неприкосновено владала функционалистичка теорија коју сукоб као социолошка категорија није интересовао. Социолошка закономерност показује да се сваки конфликт посматра као несрећан случај, као један догађај у систему социјалних односа друштва све дотле док се унутар друштва систем свагдашњих рутина, законских правила, институционализованих норми, очекиваних улога и ритуала интеракција разуме, док својим члановима гарантује мир и олакшање у устаљеним облицима понашања. Међутим, када такве незгоде преовладају, и пре свега свој отворени израз нађу у кризи, рату или револуцији као битном својству целокупног друштвеног система и сама преинака друштвене теорије постаје нужна.[34]

Библиографија радова из области теорије сукоба почела је нагло расти од шездесетих година прошлог века и данас је достигла такве размере да се појединачним напором више и не може савладати. То дакако, доказује са једне

[34] Благојевић М.: „Социолошко проучавање друштвеног сукоба“, *На граници векова*, бр. 1-96, Универзитет у Београду, Београд, 1996, стр. 75.

стране, колико је друштвени сукоб у својим различитим формама свеприсутна, свакидашња појава људског индивидуалног и колективног искуства, а са друге стране упућује на значај који друштвени сукоб има за савремене политичке системе и на значај његовог проучавања не само у социолошком, већ и у психолошком, антрополошком, историјском, па и војном прилазу.

Међутим, појам друштвеног сукоба у својој свакодневној употреби али и у теорији, ствара извесне тешкоће и неодређености, посебно по питању на шта се он првенствено односи: на стање, процес, интеракцију, (дез)интеграцију, несагласност или антагонизам, исход или решење. Осим тога, врло често се у теорији и сам појам друштвеног конфликта не одређује ближе нити прецизно, што резултира са једне стране, његовим тумачењем са становишта саморазумљивости; док се са друге стране, за неке сродне али не и истоветне друштвене појаве и процесе (сукоби интереса, социјални протести, револуције, оружани сукоби и сл.), користи исти израз и појам, што свакако са научне стране није прихватљиво.[35]

О сложености феномена друштвеног конфликта довољно говори њихов социолошки третман као нечег неприродног и непожељног (рани функционализам), па до схватања да су они елемент саме суштине друштвеног живота, да доприносе кохезији друштва и његовој интеграцији. Комплексност друштвених сукоба уочава се и у ставовима да су они основни покретач друштвеног развоја (Маркс), болести које треба лечити (Конт), материјализација животне снаге, воље за моћи (Gumplowicz, Ward), односно средство „одабраних“ за потчињавање, поробљавање људи па и целих народа.[36]

Руски социолог Голенкова, друштвени конфликт одређује као „сукоб супротних интереса, циљева, погледа и идеологија различитих индивидуа, социјалних група и класа“. Речју, сукоб је „увек конфликт интереса, борба за поседовање економске вредности, власти као и културних и моралних вредности.“[37]

---

[35] Милашиновић Р., Милашиновић С.: *Основи теорије конфликата*, Факултет безбедности, Београд, 2007, стр. 21.

[36] *Ibid*., стр. 17.

[37] Голенкова З. Т.: „Социјалне неједнакости и социјални конфликти“, Зборник: *Социјални конфликти у земљама транзиције*, Институт друштвених наука Београд и Руска академија наука, Институт за социолошка истраживања, Београд, 1996, стр. 25-27.

Научница Улрике Ц. Васмут са Института за Педагогију мира у Тибингену, пак, сматра да се непостојање конфликата може оценити као проблематично или чак штетно за мир. Она дефинише конфликт као „социјално стање у коме учествују најмање две стране (појединци, групе, државе) које имају сасвим различите полазне тачке - интересе, на први поглед непомирљиве, које може остварити само једна од страна, употребом различитих средства за остваривање свог примарног циља.“[38]

Познати социолог и један од првих истраживача друштвених конфликата, Г. Зимел, сматра да је „сукоб облик подруштвљавања и да ниједна друштвена група не може бити потпуно хармонична јер би, у том случају, била лишена развитка.“[39] А. Турен истиче да „конфликт представља јасну одредницу супарника или актера са којима се такмичи, као и извора око којих се води борба око значајних добара и вредности,“[40] док аутори друштвених дезорганизација, А. Елиот и Ф. Мерил, социјалне конфликте сматрају крајњим изразом патолошког стања друштва. Покушај интердисциплинарног одређења суштине сукоба даје С. Шпигл који сматра да је конфликт „резултат судара култура, дисхармоније интереса и диспарантности перцепција - што је пре свега последица неспособности страна да се адаптирају на средину у којој живе. Непосредан контекст било ког сукоба стварају својства и интеракције страна учесница.“[41]

Према Визеу, представнику немачке формалне социологије, сви друштвени односи (схваћени као односи између појединаца, између друштвених група и између група и појединаца), могу се поделити у две велике класе: приближавање и удаљавање, које се опет по интензитету могу делити у неколико група. Тако се приближавање дели по интезитету на контакт, приближавање (у ужем смислу) и асимилацију. У другом смеру, у смеру удаљавања су конкуренција, опозиција и борба као најоштрији степен опозиције који се разрешава насиљем.[42]

---

[38] Васмут Ц. У.: *Педагогија мира*, www.dadalos.org/frieden_bih/grundkurs_4/konflikt.htm

[39] Coser L.: *Functions of Social Conflict*, The Free Press, Cohtier-Macmillian Ltd. London, 1996, p. 24.

[40] Турен А.: „Увод у проучавање друштвених покрета“, *Обнова утопијских енергија*, Београд, 1987, стр. 48.

[41] Милашиновић Р., Милашиновић С., *op. cit*., стр. 22, према: Spiegel, S.: “Introduction”, *Conflict in World Politics*, Cambrige, 1971. p. 4.

[42] *Ibid*., стр. 23.

Професори Радомир и Срђан Милашиновић су сагласни са Визеовом тврдњом да је основа друштвених сукоба у надметању, супротностима и инкопатибилност циљева, средстава, вредности и интереса, те да конфликти изражавају неслагања ставова и супротстављено понашање и залагање на основу тих ставова. Међутим, поменути аутори сматрају да то није и њихова суштина. Неслагања и залагања кроз супротстављене ставове није карактеристика само друштвених конфликата - то је одлика сваке расправе у којој се излажу различити (супротстављени) ставови и који се бране од оних који их заступају. Заступање и одбрана ставова карактеристична је и за појединца и за групу. Друштвени сукоби, суштински и квалитативно, су много више од неслагања или супротстављања ставова. Они су, према схватању поменутих аутора, велике и масовне социјалне акције, односно свесна, усмерена, динамична и практична међусобна сукобљавања и борбе колективних друштвених субјеката због значајних и по својој природи ограничених добара.[43]

Према томе, може се констатовати да су са социолошког аспекта значајни они сукоби који се изражавају као масовне друштвене акције и борбе и које се воде око ограничених вредности и добара и њихових извора.

У покушају да обухвате и поједноставе различита одређења социјалних сукоба, Радомир и Срђан Милашиновић износе битне атрибуте друштвених конфликата. Према њиховом одређењу, друштвени конфликти су стања социјалних интеракција, отворених антагонизама, са конфронтацијом и борбом као основним усмерењима; они су конститутивни елемент сваког друштеног система и чине основу сваке његове прогредирајуће и пожељне динамике. Основни садржај и суштину овако одређеног социјалног сукоба чине унутаргрупне и међугрупне борбе за остваривање међусобно опречних интереса, вредности и ограничених али битних ресурса. Та борба може бити „рат без правила“ али готово увек је ограничена, у већој или мањој мери, ширим социјалним, правним, моралним, верским, техничким или другим нормама и правилима.[44]

---

[43] *Ibid*., стр. 24.

[44] *Ibid*., стр. 25.

2.1.2. Различити приступи у класификацији друштвених конфликата

Друштвени сукоби су сложени и структуирани јер произлазе из разлика у положају, интересима и вредносним оријентацијама социјалних група које се сукобљавају. Разликују се и по својој природи, функцији, интензитиету, носиоцима, средстима која се користе, последицама, начинима разрешавања, окончавања итд. Дакле, критеријуми класификације друштвених конфликата су бројни и разноврсни.

Прилично је позната класификација сукоба коју даје А. Рапапорт на борбе, игре и дебате и која садржи значајне елементе математичко-логичке анализе и психолошког приступа. Његова класификација полази од начина и степена утицаја учесника у сукобу на његов ток и исход: за борбу је карактеристична компонента стихијности, где самоконтрола и узајамна контрола учесника брзо опадају, тако да долази до ескалације, која производи отворена непријатељства, укључујући и насиље. Овај тип сукоба карактеристичан је за велике друштвене групе (националне, верске) али и односе између држава. Други тип сукоба су игре за које је карактеристично да, за разлику од „борби“, учесници задржавају рационалну контролу над својим потезима, али не нужно и над исходима сукоба. Под дебатама А. Рапопорт подразумева оне конфликте у којима учесници настоје да утичу један на другога у правцу измене мотива, вредности и представа о реалности.[45]

Семјуел Хантингтон сукобе дели на партикуларистичке (сукоби између кланова, племена, етничких група, религијских заједница и народа), који су укорењени у идентитету људи и комуналне – због неодговарајућих граница. Носиоци тих сукоба су државе и невладине групе, а могу бити између држава, невладиних група или између држава и невладиних група, и то ради контроле над територијама, а ређе над људима.[46] Сличну поделу сукоба цивилизација (аграрне, индустријске и информатичке) интерпретирају и Тофлерови у свом делу *Рат и антират*.[47]

---

[45] *Ibid*., стр. 191.

[46] Хантингтон С.: *Сукоб цивилизација*, ЦИД, Подгорица, 1998, стр. 279–282.

[47] Тофлер, А., Тофлер, Х.: *Рат и антират,* Paideia, Београд, 1998.

Међутим, у друштву је чест случај да постоји један конфликт који је централни и доминантан. Он успева да апсорбује све остале конфликте. Упоредо са њим могу постојати и други сукоби различитог интензитета и значаја, као што је могуће постојање више конфликтних поља приближно исте динамике. Такође су честе ситуације да се интереси конфликтних група делимично или потпуно поклапају што ствара феномен укрштених или, с друге стране, померених конфликата. О њима се може говорити са различитих становишта али је примарно оно са којег се могу сагледати последични елементи. Тиме се намеће потреба теоријског идентификовања основних сукоба (кроз узрочно последичну везу) који су провлађујући и карактеристични за дату епоху и друштво.[48]

На основу изнетих становишта недвосмислено се може закључити да се конфликти у аналитичке сврхе могу класификовати на више начина, на основу различитих критеријума. Критеријуми за класификацију друштвених сукоба јесу бројни, и условљени су теоријском и методолошком оријентацијом појединих аутора. Најчешће коришћене класификације сачињене су на основу носилаца сукоба као критеријума или пак на основу интензитета конфликата и њихових последица. Ниједна класификација се не може сматрати потпуном и довољном али су оне неопходно, помоћно, средство за систематизовање сазнања и лакше разумевање феномена друштвеног конфликта.

Најчешћи критеријуми за класификацију друштвених сукоба су:

- према врсти социјалних група, тј. чесника у конфликту (интраперсонални и интерперсонални, унутаргрупни и међугрупни, унутардржавни и међудржавни, тј. на индивидуалном, групном или међународном плану);
- према последицама које конфликти имају на дати политички систем (системски и умерени);
- чињеници да ли је конфликт средство за остваривање интереса и циљева страна у сукобу или је конфликт циљ по себи (реалистички и нереалистички);
- према природи и поводима за његово јављање, средствима која се користе, интензитету, последицама и начинима којим се регулишу или решавају.

---

[48] Милашиновић Р., Путник Н.: „Герила као специфичан вид друштвеног конфликта“, *Герила на Балкану: борци за слободу, бунтовници или бандити*, Tokyo: University Meiji, Institute for Disarmament and Peace Studies, Београд: Институт за савремену историју, Факултет безбедности, 2006, стр. 336.

Осим поменутог, сукоби се могу класификовати и према одређеним специфичностима на доминантне и латентне, насилне и ненасилне, институционализоване и неконтролисане, регионалне и глобалне, идеолошке, економске, између култура и цивилизација, модернизма и традиционализма, регионализма и унитаризма, оне који се могу разрешавати и оне који су перманентни и неразрешиви у датим друштвеним околностима и слично.[49]

Радомир и Срђан Милашиновић сматрају да би најзначајнија подела била на оружане и не-оружане сукобе, уколико се у градњи критеријума за класификацију пође од највиших вредности - људског живота и последица конфликта на друштво и његову структуру. При том, сматрају аутори, мора се уважавати значајна чињеница да сви социјални сукоби могу бити врло лако трансформисани у оружане. Међутим, оружани сукоби се тешко претварају у не-оружане и релативно институционализоване конфликте.[50]

У том контексту важно је истаћи да у „насилним социјалним сукобима, поготову оружаним, постоји непредвидиво дејство логике конкретне ситуације". Мноштво чинилаца и околности може утицати у правцу претварања не-оружаног конфликта у оружано насиље. При том, разлика између та два вида сукоба квалитативна је, суштинска. То се по правилу догађа у оним историјским ситуацијама када се од стране власти или политичких лидера доносе погрешне одлуке, које као своју последицу проузрокују страхове, претње и гомилање наоружања. Овакве друштвене и политичке околности најчешће резултују масовним људским жртвама и дуготрајним истребљивањима између националних и конфесионалних заједница, политичких групација и слично, о чему сведоче примери бивше СФРЈ и СРЈ.[51]

У том смислу, поменути аутори истичу посебан значај специфичних и екстремних врста друштвених конфликата, међу које сврставају: социјалне протесте, револуцију и ратне конфликте.

---

[49] Милашиновић Р., Милашиновић С., *op. cit*., 2007. стр. 190.

[50] *Ibid*., стр. 192.

[51] Milašinović S.: "Social conflicts and postsocialist east-european societies", *Science – Security – Police, Journal of Academy of Criminalistic and Police Studies*, Belgrade, Vol. VI, No. 2/2001.

2.1.3. Појмовно одређење ратних конфликата

Феноменом рата су се, кроз историју, бавили филозофи, научници, публицисти, књижевници, као и практичари – војсковође, државници и политичари. Због тога не изненађује плуралитет запажања и закључака о узроцима, поводима, току и исходима ратних сукоба. Проблему појмовног одређења рата посебну пажњу су посветили и бројни савремени теоретичари који су са различитих аспеката и полазишта покушали да пруже задовољавајуће дефиниције овог сложеног феномена.

Историја човечанства говори да готово и није било периода у којем није било ратова. Према истраживањима швајцарског научника Жан-Жака Бабела, за нешто више од пет и по хиљада година своје историје, човечанство је водило око 14.500 ратова са преко 3,6 милијарди људских жртава, уз непроцењива материјална разарања. Без обзира на то што подаци о тим питањима у теорији варирају, ове бројке су врло ислустративне са аскпекта учесталости рата и његове деструктивности.[52]

Иако није познато када је вођен први рат у историји човечанства, претпоставља се да су ратови најстарији облик друштвених сукоба. Сматра се да су ратови вођени још у време првобитне заједнице. Свим ратовима, од првобитне заједнице до данас заједничко је то да се воде зарад остваривања конкретних интереса, најчешће економских и политичких - освајања територија, стицања радне снаге, борбе за сировине, освајање тржишта итд.

Ратни сукоб је свакако један од најекстремнијих облика друштвених конфликата. Рат је комплексан и интензиван сукоб који може бити проузрокован класним, економским, политичким, расним и верским противречностима. Рат представља друштвену појаву која се може разматрати са различитих аспеката: војног, историјског, етичког, економског, политичког итд. Међутим, потпуно разумевање ове појаве постаје остварив једино методом мултидисциплинарног приступа.

---

[52] Ковачевић Б.: *Рат*, Светови, Нови Сад, 1995.

2.1.3.1. Појам рата

О рату постоје многе дефиниције и теорије, врло различите, најчешће са нагласком на појединим његовим сегментима или карактеристикама. Теоријска одређења овог појма најчешће су оптерећена професионалним интересовањем или идеолошким опредељењем аутора.

Поједини аутори у одређењу појма *рат* полазе од његових компонената – политичке, економске, војне, пропагандне, етничке или психолошке. Други аутори су, пак, изузетан значај придавали одређеном, по правилу тада актуелном, погледу на свет или друштво, стање и односе у њему, било са конзервативних, левичарских или неких неутралних позиција, често занемарујући реалне – објективне услове живота и историјског периода у којем се налази одређена држава или међународна заједница.

Истакнути пруски генерал и познати писац из области теорије рата Карл фон Клаузевиц се по свом доприносу научној теорији издваја међу војним теоретичарима. Његово дело се, до данас, сматра најутицајним, уз мисао древног кинеског писца Сун Цуа, и формира камен темељац модерне стратешке мисли. У својој студији *О рату* Клаузевиц је први дефинисао рат као продужење политике другим средствима и, на тај начин, указао на карактер рата као сложене друштвено – историјске појаве.[53] Под другим средствима најчешће су подразумевани наоружање и ратна техника. Клаузевиц је дефинисао рат као чин насиља који има за циљ да примора непријатеља да реализује наметнуту вољу. По његовом мишљењу, кључна карактеристика сваког посебног рата се мора тражити у политичкој ситуацији, циљевима и одлукама које воде до сукоба. Што су политички циљеви и амбиције јаснији и имају снажнију подршку у јавности, то су обично крвавији и разорнији ратови у које владе увлаче своје народе.[54] Клаузевиц види могућност престанка утицаја политике на ток вођења рата само у једном случају: „када би ратови из чистих непријатељстава били вођени као борба на живот и смрт“.[55]

---

[53] Клаузевиц К.: *О рату*, Војно дело, Београд, 1951.

[54] Ван Кревелд М.: *Трансформација рата*, Јавно предузеће Службени Гласник и Факултет безбедности, Београд, 2010, стр. 42.

[55] Беговић А., Прелевић М., Мркић С.: *Теорија о рату*, Војноиздавачки завод, Београд, 1978, стр. 51.

Мишовић и Ковач дефинишу ратни сукоб на следећи начин: „Рат је најсложенија друштвена појава, највиши ниво друштвеног сукоба, израз највећег степена међусобне искључивости интереса и воља, крајње средство политика сукобљених на политичком, економском, верском, идеолошком, војном и другим плановима“.[56]

Свечин наглашава политички аспект рата. Овај теоретичар сматра да „рат није нека самостална појава, већ је само надоградња мирнодопског живота људи. Рату се прибегава ради остварења одређених политичких циљева, тако да његове главне црте одређује политика.“[57]

Ковачевић такође истиче само једну страну рата – ону према којој је рат сукоб актера са супротним и искључивим циљевима: „Рат је друштвена појава која се може посматрати као израз постојања интеракције између друштвених група, и то оног облика интеракције који би се могао назвати дисјунктивним.“ [58]

Према потпунијој дефиницији коју је понудио Вукићевић, рат је „дисјунктивни друштвени процес, однос који је настао из последице класних и социјалних антагонизама, односно као наставак политике другим (насилним) средствима, који доводи до оружане борбе између великих друштвених група или држава, односно друштвених организација.“[59]

Војни лексикон из 1989. године истиче оружану борбу као дистинктивно обележје ратног сукоба. Под одредницом „рат“ може се наћи следећа дефиниција: „Рат је комплексан, интезиван и масован сукоб држава, војно-политичких савеза или различитих друштвених снага унутар једне земље у којој се масовно и организовано примењује и води *оружана борба*. Оружана борба је основни садржај рата, али се рат не своди само на њу, већ укључује и друге облике борбе (политичку, економску, психолошку, моралну) што га чини тоталним сукобом.[60]

---

[56] Мишовић С., Ковач М.: *Системи одбране* , Факултет безбедности, Београд, 2006.

[57] Свечин: *Стратегија*, Војно дело, Београд, 1956, стр. 15.

[58] Ковачевић Б., *ор. cit*., стр. 10.

[59] Вукићевић В.: *Култура и народна одбрана*, ВИЗ, Београд, 1976, стр.16.

[60] Ратковић Б.: *Војни лексикон, одредница рат*, 2-3 Београд, 1989, стр. 508-509.

Ротмистров такође инсистира на оружаној борби као најбитнијем обележју рата. У његовој *Историји ратне вештине* рат је дефинисан на следећи начин: „Рат је сложена друштвена појава која представља организовану, оружану, економску, политичку и идеолошку борбу између одређених друштвених класа или држава у име одређених економских и политичких циљева.“ Осим тога, наводе се следеће карактеристике рата: две или више наоружаних војски учествује у борбама. При томе је најмање једна од њих регуларна војска неке државе; поступци свих учесника спроводе се централизовано у организованој форми, а када ово није случај, онда се ради о организованој оружаној одбрани или испланираним упадима; оружани сукоб не састоји се од спонтаних и спорадичних напада. Обе зарађене стране делују систематски.[61]

Група домаћих аутора из 1996. године на следећи начин одређује садржај спорног појма: „Рат је комплексан, интензиван и масован сукоб држава, војнополитичких савеза или различитих друштвених снага унутар једне земље, у којем се масовно и организовано примењује оружано насиље и води оружана борба класа, држава и народа“[62]

Стратегија оружане борбе из 1983. године такође наглашава значај оружане борбе. Према овом документу „рат је сукоб држава, војно-политичких савеза, класа, нација или других друштвених група, у којем се масовно и организовано примењује оружано насиље и води оружана борба, уз истовремено вођење борбе у свим областима друштвеног живота, ради остваривања одређених политичких, економских и других циљева.“ [63]

Социолошки лексикон даје следећу дефиницију: „Рат је тотални друштвени сукоб изазван класним, економским и политичким противуречностима, у којем се применом масовне оружане борбе тежи ка остваривању циљева класа, држава и народа. Оружана борба представља конститутивни елемент и основни садржај рата.

---

61 Ротмистров: *Историја ратне вештине*, том I, Београд, 1966, стр. 12-13.

62 Група аутора: *Методологија ратне вештине*, ЦВШ, Београд, 1996, стр. 38.

63 *Стратегија оружане борбе*, ЦЦНО, Београд, 1983, стр. 20.

Осим ње, рат укључује и друге компоненте: економску, политичку, психолошку и др.“[64]

Према Социолошком речнику из 2007. године рат је „врста друштвеног сукоба који се испољава у међусобној оружаној борби друштвених група (класа, слојева, нација, верских скупина), или пак глобалних друштвених заједница (држава).“[65]

Љубомир Тадић рат дефинише као „најжешћи облик сукоба међу политичким заједницама са циљем или да се уништи непријатељска страна или да се присили да прихвати диктиране услове мира“.[66] На другом месту исти аутор пише: „Рат је најжешћи и најокрутнији сукоб међу политичким заједницама са циљем да се непријатељ уништи или принуди на прихватање наметнутих услова мира. Рат је нека врста принудног стања (у негативном смислу), супротно друштвеном или грађанском стању. Он је последица антагонистичких односа који одвајкада владају светом.“[67]

У намери да пружи једну свеобухватну дефиницију рата Слободан Микић износи следећу тврдњу: „Рат је сложена дисјунктивна друштвено-историјска процесна појава у којој се сукобљавају државе, војнополитички савези или друштвене скупине унутар појединих држава (нације, народи, етничке групе, племена, класе, слојеви, верске и друге интересне заједнице и групе) масовно и интензивно примењујући оружану, политичку, економску и психолошку борбу и друге врсте борби, ради остваривања својих економских и других интереса и циљева, када сукобљене стране међусобне неспоразуме, проблеме и сукобе не желе или нису у стању да реше другим, мирољубивим методама и средствима.“[68]

Анализом наведених дефиниција рата уочава се да нема потпуне сагласности око садржаја овог појма. Свака од наведених дефиниција, може се

---

64 *Социолошки лексикон*, Савремена администрација, Београд, 1982, стр. 537.

65 *Социолошки речник*, прир. Аљоша Мимица и Марија Богдановић, Завод за уџбенике, Београд, 2007, одредница рат.

66 Тадић Љ.: *Наука о политици*, Издавачка радна организација „Рад“, Београд, 1988, стр. 118.

67 Тадић Љ.: *Политиколошки лексикон*, Завод за уџбенике и наставна средства, Београд, 1966, стр. 182.

68 Микић С.: *Поглед на ра*т, Генералштаб војске Србије и Црне Горе, Управа за школство и обуку, Војна академија, Београд, 2003, стр 28.

констатовати, на неки начин је недостатна јер не истиче неку од битних одлика или садржаја рата.

Као сложена друштвена појава, рат представља оквир у којем делују бројни чиниоци који му дају специфичан израз и садржај. Рат представља обједињено деловање пропагандних, политичких, економских, војних, моралних, психолошких, научних, културних и других услова, садржаја, чинилаца и снага. Рат се састоји од огромног броја непосредно повезаних процеса и потпроцеса и великог броја актера. Процеси се одвијају на свакој од ратујућих страна, и у оквиру субјекта двају сложених процеса тих страна, које наступају са супротних и супротстављених интереса и циљева којима теже, и које ратом настоје да остваре.

Из наведених дефиниција може се закључити да традиционалистичко схватање конвенционалног рата међу битна обележја овог феномена укључује масовност и оружану борбу. Слика конвенционалног рата подразумева сукоб у којем учествују масе људи (за разлику од гериле и тероризма) а не само групе или мање скупине. Као учесници у рату могу се јавити државе или војно-политички савези (међудржавни рат) или пак нације, етничке групе, племена, класе, друштвени слојеви, верске конфесије, територијалне јединице, партије (грађански рат). Рат подразумева обавезно оружану борбу али и пропаганду, политичку, економску и друге врсте борби, које у савременим условима попримају све већу улогу и значај. Од њих, данас, у највећој мери зависе ток и резултат рата.

Рат настаје када сукобљене стране своје неспоразуме, интересе и сукобе нису у стању, или пак не желе, да решавају на уобичајен и на праву заснован начин, мирољубивим средствима. Неретко, на то их подстичу и други чланови међународне заједнице или интересне групе и организације, зарад својих интереса.[69]

2.1.3.2. Класификација ратова

Карактеристике ратова (садржај, облици и начини реализације) мењале су се у складу с историјским развојем друштва на технолошком, материјалном, и

[69] Микић С.: *О рату*, Прометеј, Нови Сад, 2006, стр. 46.

духовном плану. Поред општих карактеристика, сваки рат има и одређене специфичности које га чине посебним и, у некој мери, различитим од других.

Проблемом класификације ратова бавили су се многи теоретичари. За већину њих било је то мање значајно питање, због чега су истицали и разматрали само поједине врсте ратова, изузимајући остале облике ратова, и не ослањајући се на принципе и основе једне потпуније и научно засноване класификације. Теоретичари су најчешће анализирали властита искуства из ратова или, пак, искуства њихових савременика. Осим тога, теоријска мисао је за предмет изучавања најчешће имала праксу, односно војну вештину испољену у конкретним примерима ратова, коју су примењивале врховне команде или поједине истакнуте војсковође.[70]

Клаузевиц, на пример, истиче три врсте ратова - ратове коалиција, ограничене ратове и ратове за наношење пораза непријатељу. Ерих Лудендорф пише о тоталном рату као основном. Жомини се више бави питањем врсте ратова, разматрањем циљева страна у рату, те могућих ситуација и комбинација ратова у односу на дипломатију. [71]

Маркс, Енгелс, Лењин и Троцки бавили су се проблемом револуција, народних и грађанских ратова у условима капитализма, полазећи од циља да се створе социјалистичке државе и односи, у којима би на власти била радничка класа. Лењин је посебан акценат стављао на поделу ратова која истиче праведне и неправедне ратове што је, у ствари, идеолошки и политички карактер рата једне од страна учесница.[72]

Уочљиво је да се велики број теоретичара бавио само неком од врста или категорија рата која, према њиховом мишљењу, има истакнуту улогу у остваривању ратних циљева. Тако, на пример, Ћулио Дует даје предност ваздушној моћи, као одлучујућој у рату.[73] Совјетски војсковођа и теоретичар Михаил Фрунзе предност даје маневарском рату и офанзиви.[74]

---

[70] *Ibid*., стр. 119.

[71] Жомини: *Преглед ратне вештине*, Војно дело, Београд, 1952, стр. 41-61.

[72] Драшковић Д.: *Савремени ратови*, ИШ Стручна књига, Београд, 1999, стр. 340-348.

[73] Ерл М.: *Творци модерне стратегије*, Војно дело, Београд, 1952, стр. 515-593.

[74] *Ibid*., стр. 365.

Проблем класификације ратова се потпуније и систематичније разматра у периоду после Другог светског рата, мада су и у овом периоду уочљиве једностраности у приступу. Након Другог светског рата војни теоретичари се махом баве проблемом врста могућих ратова али без улажења у суштинска питања класификације. Увек се опредељују за неке, по њима, најзначајније врсте ратова, при том полазећи од теме која је предмет њиховог разматрања. Узроке томе треба тражити у идеологизацији и политизацији војне науке уопште, па према томе и ових питања.

Совјетски маршал Василиј Соколовски разматра врсте ратова (националноослободилачке револуције, освајачке ратове и ратове између капиталистичких земаља) и категорије ратова (рат између лагера социјализма и лагера империјализма, империјалистичке ратове, националноослободилачке, грађанске и друге народне ратове). С обзиром на размере ратови, према мишљењу овог аутора, могу да буду ратови светских размера и локални ратови.[75]

Андре Бофр истиче тоталност рата као његову најопштију карактеристику. Поменути аутор разматра и питања хладног рата, револуционарног и атомског рата.[76]

Класификација ратова може се извршити на основу неких њихових битних одлика, које су бројне и врло често испреплетане. Тако се према легалности употребе оружане силе ратови могу поделити на: легалне и нелегалне; према критеријуму циљева због којих се дати ратови воде на: одбрамбене, верске, ослободилачке итд.

Према мишљењу Смиље Аврамов најприхватљивија подела ратних сукоба је на: међудржавне и грађанске. „За разлику од међународних ратова, где се као ратујуће стране постављају суверене државе, основна карактеристика грађанских ратова је да ратујуће стране припадају истом друштву, те је спиралу насиља из којих се рађају тешко контролисати.“[77] Док се у међудржавним ратовима противник присиљава на неповољне услове мира, у грађанским ратовима се тежи његовом потпуном уништењу.

---

[75] Соколовски: *Војна стратегија*, ВИЗ, Београд, 1965.

[76] *Доктрипа сукоба ниског интензитета*, ЦОСИС, Београд, 1990, стр. 288.

[77] Аврамов С.: *Постхеројски рат запада против Југославије*, I том, Ветерник, 1997, стр. 205.

Поједини амерички теоретичари, када разматрају могуће сукобе, поред осталог наводе и герилски рат и дуготрајни герилски рат. [78]

Према Вишњићу подела и класификација ратова се може извршити на основу следећих критеријума.[79]

- Према филозофском критеријуму на: праведне и неправедне;
- Према друштвено-историјском критеријуму на: светске, регионалне и локалне;
- Према социолошком критеријуму на: грађанске, народне и међународне;
- Према идеолошком критеријуму на: револуционарне и контрареволуционарне;
- Према техничко-технолошком критеријуму на: класичне и савремене;
- Према географском критеријуму на: копнене, поморске, ваздушне и космичке;
- Према друштвено-политичком критеријуму на: нападачке и одбрамбене.

Слободан Микић одбацује претходне класификације. Он настоји да понуди једну потпунију класификацију која се заснива на прецизно утврђеним правилима. Појам рата може се успешно делити на уже појмове (врсте ратова), уз коришћење следећих правила: принцип одређености предмета поделе; принцип јединствености; принцип релативне посебности сваког члана поделе у оквиру појма рат; принцип јединства посебних чланова поделе; принцип потпуности поделе појма рата.

Уз неведене принципе, успешна класификација захтева и дефинисане критеријуме поделе. Критеријуми за поделу ратова на врсте могли би да имају следећа полазишта, сматра Микић:

- историјско;
- простор захваћен ратом и снаге које су ангажоване;
- амбијент у којем се изводе ратна дејства;
- време трајања ратова;
- груписање (обухват) држава за рат;
- војнотехничке карактеристике;

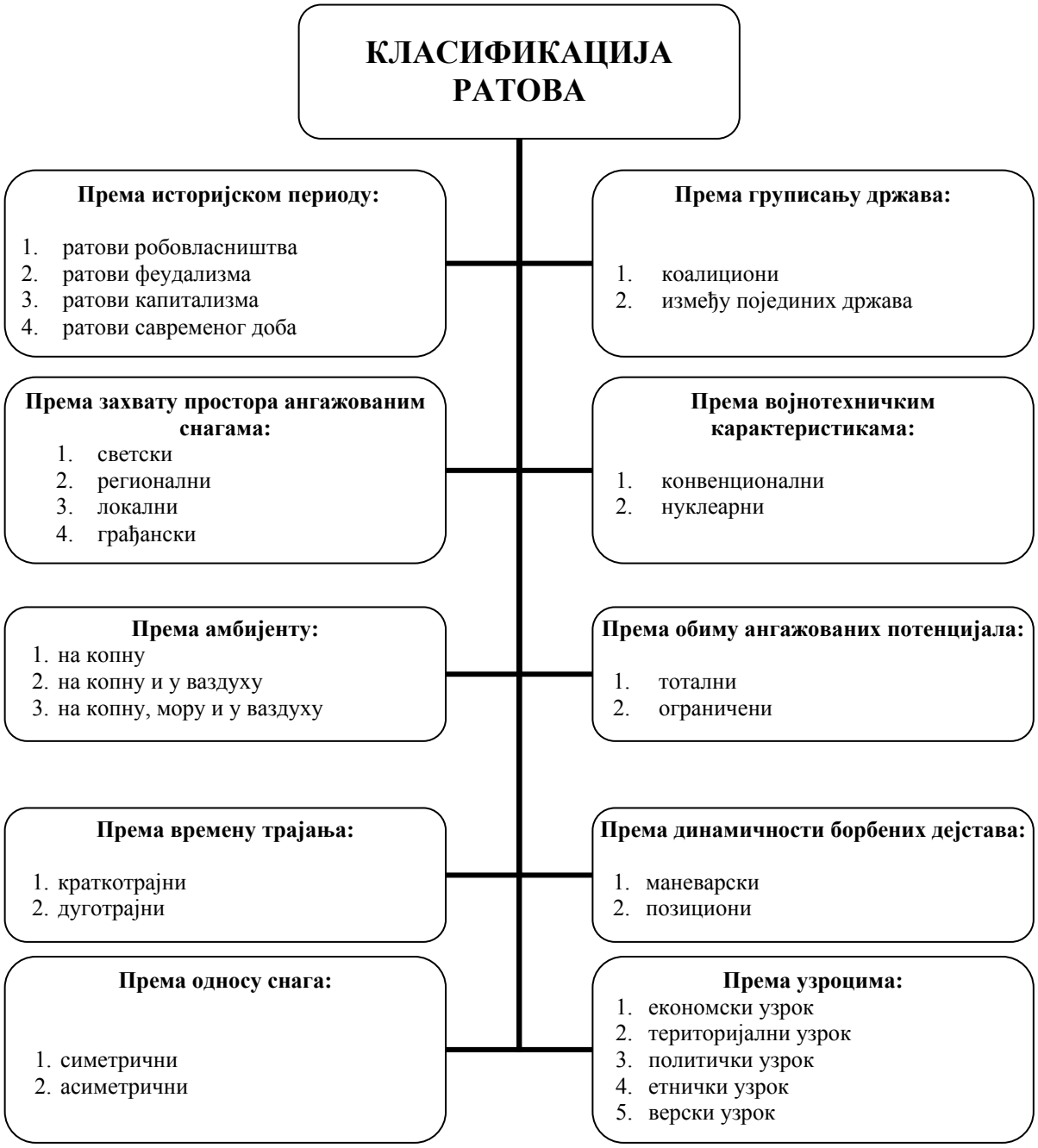
---

[78] *Доктрина сукоба ниског интензитета*, *op. cit*., стр. 414.

[79] Вишњић Д.: *Појам оружане борбе*, ВИНЦ, Београд, 1988, стр. 9.

- степен ангажовања потенцијала и снага;
- степен покретљивости снага у рату;
- однос снага;
- узроке рата.[80]

Схема бр. 1: *Класификација ратова*



[80] Микић С.: *О рату*, Прометеј, Нови Сад, 2006, стр. 123-127.

Према историјском критеријуму, ратови се могу груписати у следеће категорије:

- ратови робовласничког друштва (од око 4000. године пре нове ере до 500. године нове ере);
- ратови у периоду феудализма (од VI до XVII века);
- ратови епохе капитализма (од XVIII до средине XX века); и
- ратови савременог доба.

Сваки од иаведених периода имао је знатан утицај на организацију војске, наоружање, услове, узроке, садржаје и ток ратова.

Према простору захваћеним ратом, размерама и ангажованим снагама ратови могу да буду: интердржавни (светски, регионални и локални) и интрадржавни (све врсте грађанских ратова).

Према *амбијенту у којем се изводе ратна дејства* ратови могу да буду: на копну, у ваздушном простору, на мору и у космосу. Поједини аутори сматрају да се ратови могу водити и у кибер простору. У том смислу је Центар за информациону безбедност Универзитета у Даласу 2005. године сачинио историјску анализу ратовања у којој Интернет, као вид амбијенталне одреднице, добија запажено место међу критеријумима категоризације.[81]

---

[81] Ова студија идентификује следеће критеријуме категоризације ратних конфликата:
– Према епохи и периоду;
– Према трајању;
– Према степену и нивоу разарања;
– Према месту одигравања, географској регији или временским условима;
– Према типу (племенско, цивилно, екстериторијално, герилско, објављено, необјављено, жестоко, хладно итд.);
– Према амбијенту (копно, море, ваздух, свемир, Интернет, неки од ових или свих пет);
– Према наоружању, технологији, обавештајној делатности;
– Према националним ресурсима или националним периодима и етапама;
– Према особеностима вођа;
– Према облицима или структурама влада;
– Према стратегијама и тактикама;
– Према побудама и разлозима за вођење и сл.
Према: Nugent J., Raisinghani M.: "Bits and Bytes vs. Bullets and Bombs: A New Form of Warfare", у: Janczewski, L., Colarik, A.: *Cyber Warfare and Cyber Terrorism*, Information Science Reference (an imprint of IGI Global), Hershey, 2008, p. 27.

Према *времену трајања* ратови могу да буду краткотрајни и дуготрајни. Ратови који трају мање од годину дана су краткотрајни, а ратови који трају дуже од годину дана су дуготрајни ратови.

Према *груписању држава учесница* ратови могу да буду: коалициони и између појединих држава.

Војнотехничке карактеристике ратова имају за основ врсте и степен коришћења оружја. Постоје конвенционални и нуклеарни ратови. Конвенцнонални рат је до краја XX века био једина врста рата, с обзиром на борбена средства која су коришћена у ратовима. Као што је познато, у првим ратовима је коришћено хладно, а у каснијим ватрено оружје.

Појавом нуклеарног оружја отпочиње ера производње и наоружавања нуклеарним оружјем. Истовремено се осмишљавају и израђују доктрине и стратегије планирања и употребе овог оружја у будућим ратовима. Присутност овог оружја у наоружању великих сила и неколико других држава (Индије, Пакистана, Јужноафричке Републике, Израела, а вероватно и Бразила) представља претњу опстанку човечанства и уједно налаже потребу за изучавањем проблема које оно собом доноси, уколико би дошло до његове употребе у будућим ратовима.[82]

У категорију војнотехничких карактеристика ратова спадају и *техничке карактеристике оружја и ратне технике* који се у њима употребљавају. По том основу, зависно од технолошког развоја друштва, у ратовима се користе: оруђа (копље, лук, стрела и др.), експлозив (барут), машинска техника, машинско-аутоматска техника, електронска техника, ракетна техника и информатичка техника.

У односу на *начине и ефекте дејства* у ратовима се користи: хладно оружје, ватрено оружје, електронско оружје, ракетно оружје и нуклеарно, хемијско и биолошко оружје. У литератури новијег датума све чешће се истиче могућност

---

[82] Осим тога, у неким ратовима је употребљавано и хемијско оружје, а по неким подацима и биолошко. Чињеница да многе земље та оружја истражују, да их производе и њима тајно располажу, намеће потребу да се теорија (али и пракса) бави питањем могућности (истина, са малом вероватноћом) да некада може доћи до нуклеарног, хемијског и биолошког рата. Коришћење таквих врста оружја утиче на потребу да се нађу одговори на многа питања организације и опремања, а поготово борбене употребе и начина дејства оружаних снага, али и да се реше проблеми који би настали код становништва и других структура друштва. *Ibid*., стр. 132.

коришћења и других оружја као што су: геофизичка, метеоролошка, неокортикална, информатичка и др.

Према обиму и степену ангажовања потенцијала, снага и средстава, ратови могу да будутотални и ограничени.

У односу на степен покретљивости оружаних снага и динамичност борбених дејстава, ратови могу да буду: претежно маневарски и претежно позициони.

Према *односу снага* као критеријуму категоризације у ратовима могу бити изражене: *симетрија*, *дисиметрија* и *асиметрија*. Са стратегијског становишта симетрија се поима као борба равноправних противника, борба у којој противници ангажују приближно једнаке снаге и потенцијале. У пракси нема апсолутно симетричних ратова већ само релативно симетричних. Под појмом дисиметрија се подразумева настојање једног од противника да стекне квалитативну и/или квантитативну предност. Асиметрични су они ратови у којима се сукобљавају противници са изразито неједнаким снагама и потенцијалима. Асиметричне ратове карактерише настојање страна у сукобу да искористе све слабости супарника и нанесу му што већу штету.[83]

У савременој литератури можемо наићи и на разноврсне поделе које ратове деле на епохе, таласе и генерације.

Једна од последњих теорија рата дели ову појаву на генерације. Вилијам Линд и група официра употребили су 1989. године појам „рат четврте генерације“ да би њиме именовали недржавне асиметричне насилне сукобе.[84] У равни са претходно поменутим епохама и таласима, подела ратова на генерације изгледа свеобухватнија.

Наиме, према овој класификацији технике рата прве генерације везују се за Наполеонов начин вођења борбе – праволинијски распоређена војска која се фронтално супротставља непријатељу.

Бодљикава жица, аутоматско оружје и индиректна ватра утицали су на тактику рата друге генерације, који се заснивао на масовној ватреној моћи, а не на

---

[83] О појму асиметрије, тј. асиметричног рата, више видети у: Курмон Б., Рибникар Д.: *Асиметрични ратови – сукоби јуче и данас, тероризам и нове претње*, НИЦ Војска, Београд, 2003.

[84] Lind W.: *The Changing Face of War: Into the Fourth Generation*, Marine Corps Gazette, October 1989, pp. 22-26.

масовним војним формацијама. Рат друге генерације остао је линеаран, а сукоби су углавном били ратови исцрпљивања. У рату треће генерације први пут је употребљена нелинеарна тактика. Сам рат био је заснован на маневру у комбинацији са ватреном моћи, а не на исцрпљивању.

У рату четврте генерације у сукобу учествује целокупан народ, уместо оружаних снага. Циљ је да се изазове колапс непријатеља изнутра а не да се физички униште противничке оружане снаге. Борбени простор рата четврте генерације не укључује само оперативни простор оружаних снага, већ мање-више обухвата читаво друштво непријатеља. Услед тога што модерна друштва зависе од нафте, електричне енергије, технолошке опреме и комуникација, она постају веома рањива на различите типове напада.

Асиметрични учесници у сукобу четврте генерације нису ограничени само на војне циљеве већ укључују политичке, социјалне, економске, па чак и психолошке аспекте. Рат четврте генерације још увек није попримио своју коначну форму. Могло би се рећи да је он аморфан и адаптиван. Актери који користе технике рата четврте генерације принуђени су да изналазе нове могућности за одговор на напад противника. Стога рат четврте генерације постаје логичан избор за терористичке групе и остале учеснике у конфликтима које карактерише асиметричност.[85] Рат четврте генерације укључује многе аспекте познатијих дефиниција малих ратова, ограничених ратова, асиметричних ратова и сукоба ниског интензитета.

Међу основне карактеристике ратова четврте генерације, могу се уврстити следеће:

- Све већа деконцентрација (растреситост) снага на бојишту. Бојиште четврте генерације обухвата читаво друштво непријатеља. Таква деконцентрација заједно са повећаним значајем акција које изводе веома мале групе бораца, захтеваће да чак и најнижи ниво дејствује флексибилно на основу задате мисије.
- Смањена зависност од централизоване логистике. Деконцентрација заједно са повећаном важношћу која се даје темпу извођења дејстава, захтеваће висок ниво способности за опстанак на непријатељској територији.

---

[85] Huntington S.: "The Age of Muslim Wars", *Nesweek*, Special Davos Edition, December 2001, p. 8.

- Повећан нагласак на маневру. Масовност живе силе или ватрене моћи више неће бити преовлађујући фактор. У ствари, масовност живе силе може да постане сметња, пошто постаје лака мета. Мале веома покретне, агилне снаге биће доминантне.
- Циљ је да се непријатељ сломије изнутра, а не да се физички уништи. Објекти дејства ће бити такве ствари као што су подршка становништва рату, као и култура непријатеља. Исправна идентификација стратегијских центара гравитације непријатеља је изузетно значајна.

Актери у рату четврте генерације могу бити националне државе, терористи или екстремистичке организације. Борци у рату четврте генерације показују велику иновативност и креативност – у њиховим рукама практично све може постати оружје - авион, аутомобил, акт-ташна, резач папира или ципеле.[86] Употреба ових, наизглед безопасних средстава отежава идентификовање и праћење претње и процену намере, као и њено неутралисање.

2.1.4. Појмовно одређење савременог рата

Сваки покушај научне елаборације одређеног проблема претпоставља утврђивање и дескрипцију историјског контекста у коме је изучавана појава присутна. Такав приступ захтева, са аспекта друштвених наука, ослањање на техничке периодизације које су, по правилу, недостатне али ипак неопходне. Начелно, може се рећи да је у друштвеним наукама прихваћена периодизација која под периодом „модерности“, у техничком смислу, обухвата време од XVII до XIX века, док се под „савременошћу“ подразумева XX и почетак XXI века.[87]

Када је реч о *савременим ратовима*, међутим, присутан је проблем временског одређења овог појма. Другим речима, под одредницом „савремен“ не подразумевају сви теоретичари период од почетка XX века до данас. Међу теоретичарима не постоји сагласност о периодизацији која би била општеприхваћена.

---

[86] Вујановић Н.: „Савремене војне технологије и њихов утицај на б/д“, *Нови Гласник*, Година 2, бр 1, 1994, стр. 5-12.

[87] Милашиновић С.: *Друштвени сукоби у земљама Централне и Југоисточне Европе*, Докторска дисертација, Факултет политичких наука у Београду, 2003.

Тако, на пример, Драшковић термин *савремени рат* везује за период након Другог светског рата и њиме именује оне ратове који се воде најмодернијим оружјем (нуклеарним и конвенционалним) и борбеном техником која је у употреби или ће бити у наоружању војних формација. Исти аутор касније закључује: „Према томе, за одређивање појма 'савремени рат' релевантни су ови фактори:

- вријеме у коме се воде ратови;
- борбене могућности и квалитет савременог оружја, борбене технике;
- амбијент у коме се води рат (космос);
- посљедице које савремени ратови могу да имају на међународне односе, сарадњу међу државама, подстицање разоружања, борбу за мир, продубљивање кризних жаришта и сукоба".[88]

Павле Јакшић је тај појам дефинисао исказом: „Под савременим ратом подразумевају се ратови у блиској прошлости, садашњости и блиској будућности, јер у четвородимензионалном опредељењу - нарочито у бурној друштвено-политичкој и научно-техничкој револуцији - друкчије не може бити".[89]

Микић сматра да у савремене ратове не би требало убрајати све ратове који су се догодили од Другог светског рата до данас, будући да су многи од ратова из периода од 1945. до 1990. године превазиђени по скоро свим аспектима и садржајима.

Овај аутор је мишљења да сваки приступ дефинисању појма о савременом рату мора полазити од уобичајеног језичког значења атрибута савремен, јер је то значење веома јасно и уобичајено је у комуникацији међу људима.

Према томе и Микић, као и претходно поменути Јакшић, наглашава временску компоненту као критеријум савремености. То би требало да значи да су савремени ратови сви они ратови који су се одвијали у блиској прошлости, који се одвијају у садашњости или ће се одвијати у блиској будућности. Према томе: „савремени рат је сваки онај рат који се води у садашњем времену, или у времену најближе ирошлости н будућности. У конкретнијем случају, под савременим ратом

---

[88] Драшковић Д.: *Савремени ратови*, ИШ Стручна књига, Београд, 1999, стр. 11-12.

[89] Јакшић П.: *Савремени рат II*, Вук Караџић, Београд, 1969, стр. 268.

подразумеваће се ратови који су се догодили на крају XX и на почетку XXI века, односно после 1990. године.“ [90]

2.1.5. Карактеристике савремених ратова

Узроци свих досадашњих ратова и конфликата, па и савремених, превасходно се налазе у економским мотивима и политичким интересима.

Слободан Микић истиче значај међународних услова који утичу на настајање конфликата у међународној заједници, у првом реду: злоупотребе глобализације, неравноправних међународних економских односа и интереса војноиндустријског комплекса.[91]

Опште узев, можемо констатовати да, као и сви конфликти, и ратни сукоби настају из супротности и противречности интереса. Савремени ратови су последица различитих и бројних фактора и чинилаца, како унутар појединих држава тако и на глобалном плану. Унутрашњи услови попут: структурних фактора, политичких фактора, економских фактора и културно-перцептуалних фактора имају одлучујући утицај на настајање грађанских и локалних ратова. Локални ратови су у мањој, а регионални ратови у већој мери последица међународних односа.

Двадесети век се често означава као век оружаних сукоба, век у коме су ратна страдања достигла размере веће него икада раније. Велики број ратова у XX веку је довео до огромних људских жртава и материјалних разарања. Развој технологије је значајно утицао на интензитет и количину штете проузроковане употребом различитог наоружања, а бројни проналасци су првенствено коришћени у војне сврхе. Поред бројних локалних и регионалних сукоба у XX веку су се десила и два светска рата. Други светски рат је донео и употребу атомске бомбе која је за свега неколико минута разорила два града Хирошиму и Нагасаки.

Крај Другог светског рата није донео мир народима међународне заједнице већ даљи наставак оружаних сукоба. Према доступним подацима, свет је након 1945. године био само двадесет шест дана без рата. После Другог светског рата вођено је

---

[90] Микић С.: *О рату,* Прометеј, Нови Сад, 2006, стр. 226.

[91] *Ibid*., стр. 234.

око 265 регионалних и локалних оружаних сукоба од чега су САД започеле или водиле око 227. Учесталост ратова расте а трајање ратова се продужава: 41 рат је трајао више од 10 година док је 26 ратова трајало дуже од пет година. Изградња новог светског поретка праћена је милионским жртвама, неизмерним ратним разарањима и повећањем броја начина разарања. Сматра се да је број жртава у минулом веку био четири пута већи од броја жртава у претходна четири века. Само у последњих педесет година свет су потресали насилни сукоби који су однели животе неколико милиона цивила, узроковали расељавање десетина милиона људи, уназадили привреду, донели незапосленост, сиромаштво, глад, епидемије и безнађе.[92] Оружане конфликте у XX веку, посебно је обележило проширење мета на цивилне објекте и увећање броја цивилних жртава. Удео цивилног становништва у укупном броју ратних жртава порастао је од 50% са краја седамдесетих година, преко 75% у осамдесетим годинама на скоро 90% у деведесетим годинама. Укупан број жртава у свим ратовима од 1945. до 1988. године износи између 25 и 35 милиона.[93]

Скоро пола века после Другог светског рата, од 1945. до 1991. године, свет је почивао на биполарном моделу који се показао као релативно стабилан. Две главне суперсиле, НАТО и Варшавски пакт, су прећутно прихватале постојање недодирљивих интересних сфера супарника, што се видело са наглашеном уздржаношћу САД, током совјетских интервенција у Мађарској 1956. године и Чехословачкој 1968. године. Геополитичка утакмица водила се у сивим зонама Трећег света (Блиски исток, Индокина, Ангола, Никарагва итд.),[94] али су правила игре почивала на релативно рационалном прорачуну односа између цене и користи спољнополитичких потеза, док су ратови клијената остајали локализовани.

---

92 Zolberg R. A., Suhrke A., Aguayo C.: *Escape From Violence: Conflict and the Refugee Crisis in the Developing World*, Oxford University Press, New York, 1989, pp. 3-16.

93 Вишњић Д.: *Тезе о рату*, ЦВШ ВЈ, Београд, 1988. стр. 23.

94 Према француском мислиоцу Вирилију, локални и регионални ратови функционишу као сигурносни вентил који има задатак да, геополитички простор Западне Европе и Северне Америке заштити од евентуалне појаве великог светског или тоталног рата. То значи да периферни сукоби спречавају конфликт у епицентру Западне Цивилизације која је управо преко рата и уз помоћ рата, данас постала заштићена зона мира и сигурности. На овај начин свет наизглед доживљава непосредне промене али ипак постоји суморни вид континуитета рата и насиља. Према: Кегли Ч., Виткоф Ј.: *Светска политика, тренд и трансформација*, Желнид, Београд, 2006, стр. 581.

Једна од кључних карактеристика периода Хладног рата била је трка у наоружању и развоју технологија коришћених у војне сврхе које су, на послетку, довеле и до освајања свемира. Трка у наоружању је трајала до почетка 70-их година XIX века када је тадашњи председник САД-а Ричард Никсон започео политику детанта у односима са СССР-ом.

Последња декада XX века обележена је завршетком Хладног рата, који је променио глобално-политичку слику света. Упркос тој важној промени, историјске токове и даље обележава стратегија конфликта која је до недавно била узрок блоковске поделе света. Нада да ће крај Хладног рата означити почетак мирне и безконфликтне фазе, убрзо је суочена са новим препрекама. Нова геополитичка клима након краја Хладног рата, подстакла је пролиферацију локалних, етничких, верских и националних сукоба.[95]

Данашњи свет поново постаје мултиполаран. Моћ једне државе више није пресудно одређена само величином територије, бројем становника, војном моћи, богаством и изворима енергије. Значајни извори моћи у међународним односима су и степен технолошког развоја, образовна и старосна структура као и утицај који нека држава има на доношење одлука у раду међународних организација[96].

Свет је данас, више него икада раније, суочен са потчињавањем земаља и народа од стране доминантних сила не само средствима и методама рата и уобичајеним дипломатским активностима, већ све више чиниоцима чија се активност карактерише највећим степеном криминогених садржаја[97]. Креатори светске политике оцењују да је у датим условима њихова примена најсврсисходнија, пошто често уобичајеним средствима није могуће ефикасно натерати нападнуту страну на безусловно потчињавање.

Укупне међународне односе компликују постојање низа кризних жаришта, заоштравање односа између новостворених земаља и њихово надметање и сукоби

---

[95] Симић Д.: *Наука о безбедности, савремени приступи безбедности*, Службени лист, Београд, 2002, стр. 66.

[96] *Ibid*., стр. 37.

[97] Милашиновић Р.: *Терор Запада над светом - савремени механизми разарања и подчињавања суверених земаља и народа*, Институт за криминолошка истраживања, Београд, 1998, стр. 7.

као и различити облици пенетрације на просторима других суверених земаља[98]. Главни снабдевачи оружјем земаља у развоју које су ратовале и које ратују јесу најразвијеније земље света које су у томе нашле богате изворе прихода и широко тржиште за пласман својих производа. Земље у развоју дају око 100 милијарди долара за увоз ових производа, а у тој трговини САД највише профитирају и њихов удео у светском извозу оружја и војне опреме износи 37%, Француске 10%, Велике Британије 4%, Италије 3,5%, Немачке 2,5% итд[99]. Према томе, може се рећи да рат и конфликт данас представљају активну силу која обликује економску структуру. Они су кључ за подизање профитне стопе, моторна снага водећих технолошких грана.

Појава нових чинилаца на светској сцени и све већа асиметрија снага представљају позадину савремених оружаних сукоба. У низу локалних ратова крајем XX века испољене су нове тенденције због којих их неки аутори сврставају у посебну категорију, тзв. трећу врсту сукоба, јер нису ни класични грађански ратови ни међудржавни а тесно су повезани са фрагментацијом државе. Ову врсту сукоба одликује брисање разлике између државе и друштва, војника и цивила, рата и организованог криминала. У војне и паравојне формације регрутују се деца, спроводи се систематско уништавање културних споменика али и социјалне инфраструктуре, као део стратегије поништавања културног идентитета и успостављања потпуне контроле над становништвом путем терора и страха. Такође су изражене тенденције развијања паралелне привреде посредством трговине ресурсима, дрогом, оружјем или пљачком.

У исцрпној студији о савременим ратовима Слободан Микић износи став да су ратови из последње деценије XX века попримили одређене, специфичне карактеристике. Према мишљењу овог аутора, основне карактеристике савремених ратова могле би се груписати у три категорије:

- карактеристике претходних ратова, које су потврђене у савременим ратовима;
- карактеристике које представљају еволуцију својстава претходних ратова;
- особености које издвајају савремене од претходних ратова.

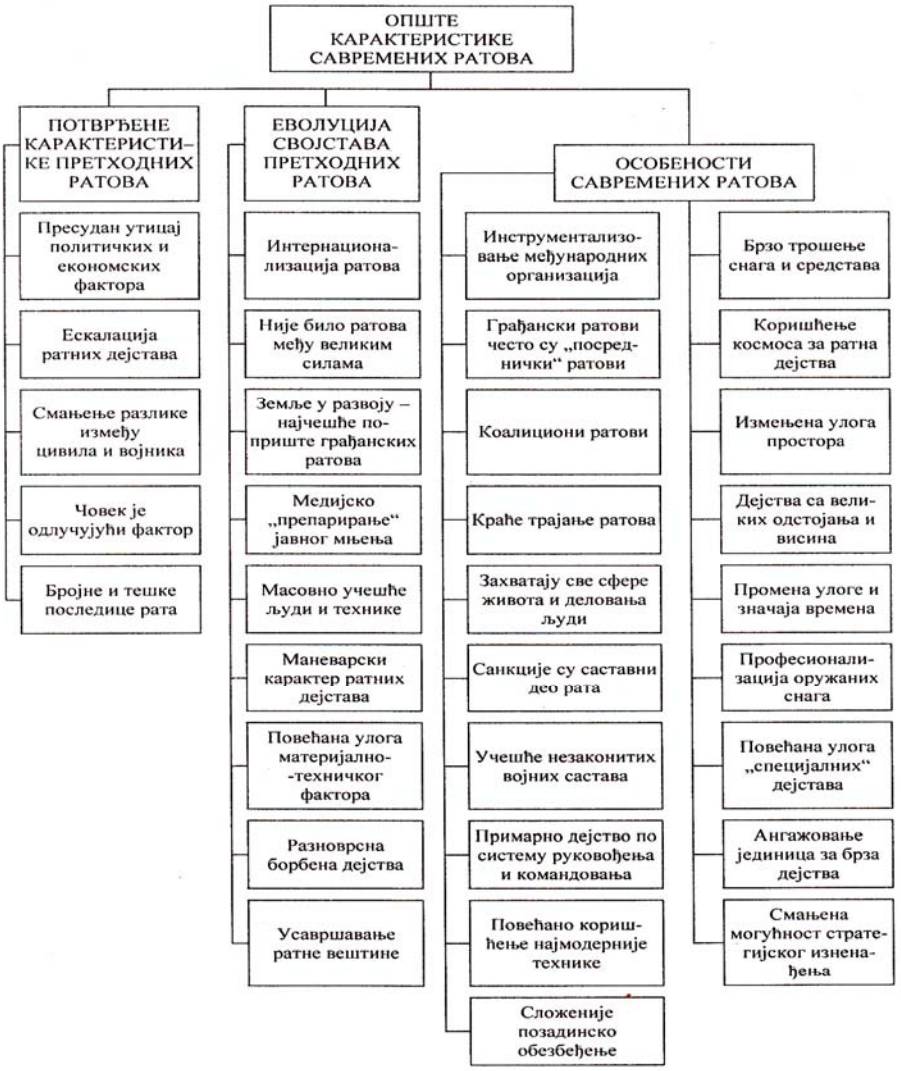
Опште карактеристике савремених ратова, ради прегледности, дајемо у форми схематског приказа.

---

[98] *Историја XX века*, Према: http://www.ceeol.com

[99] Biznis & Finansije #2, Према: http://www.docstoc.com/docs/4052048/Biznis-and-Finansije-2

Схема бр. 2*: Опште карактеристике савремених ратова*



Извор: Микић С.: *О рату*, Прометеј, Нови Сад, 2006, стр. 247.

Особености које издвајају савремене ратове од претходних ратова произашле су, добрим делом, као последица употребе нових технологија у војне сврхе. Из тог разлога, али и због самог предмета истраживања овог рада, неопходно је посветити посебну пажњу месту и улози техничко-технолошког фактора у савременом ратовању.

2.2. Техничко-технолошки фактор и савремено ратовање

У свим досадашњим оружаним сукобима техничко-технолошки фактор је имао значајну улогу. Технолошка надмоћ значила је, у највећем броју случајева, и победу у рату. Ни данас није другачије. Тежње за освајањем нових технологија у циљу израде што деструктивнијег оружја не само да су опстале, већ су се и увећале. Може се рећи да је знање, као предуслов технолошког развоја, постало примарни и доминантни ресурс, неопходан за победу у сукобу.

Процес растуће милитаризације савременог друштва изнедрио је и идеју да се усавршавањем ратне технике феномен рата може укинути. Веровало се да се рат може учинити немогућим уколико се освоји технологија израде „оружја над оружјем“, оружја чији ће деструктивни потенцијал деловати превентивно против порива рата. Међутим, ниједно оружје - од барута, нуклеарне бомбе, до ракетног штита није зауставило логику рата. Оно је само подстицало трку за његовим ексклузивним поседовањем, или његовим ирационалним, квантитативним, увећавањем. Последица тога је улагање огромних финансијских средстава у наоружање, и бескрајно увећавање капацитета за уништење планете. Једном речју, технолошка креативност није елиминисала опасности од конфликата већ их је, напротив, увећала.

Из историјске перспективе гледано, може се рећи да је матрица рата остала, у суштини, непрекинута од Првог светског рата до данас. Показало се да сваки талас оптимизма поништавају савременија, моћнија средства деструкције и њима узроковане нове форме насиља. Тако је било на почетку прошлог века, тако је и на почетку новог. Досадашња филозофска промишљања мира и научна истраживања показала су се као недовољна и неделотворна да одговоре захтевима времена. Кад год би се, у одређеном историјском тренутку, поставило питање практичне употребљивости таквих сазнања о рату и миру, у мирном решавању сукоба, закључило би се да је потребан један нов интердисциплинаран напор науке и филозофије који ће се суштински разликовати од ранијих промишљања рата и мира.[100] То нам говори да нисмо стекли довољно продубљена сазнања о свим силама

[100] Симић Д.: *Позитиван мир – схватања Јохана Галтунга*, Академија Нова, Архив Књакић, Београд, 1993, стр. 11.

рата, сазнања која би увећала моћи друштвених наука да поуздано предвиђају будуће расплете у арени рата и мира.

Када говоримо о новим одликама рата имамо у виду тенденције које су снажиле од Другог светског рата до данас. У оквиру међународних сукоба, дакле, испољена је тежња да се однос између технологије и исхода рата доведе у апсолутну корелацију, да технолошки супериорну моћ не може поразити инфериорна моћ. Када постоји асиметрија моћи, исход сукоба не може бити неизвестан. Надаље, испољена је тежња да се скрати време ратовања и да се на страни најмоћнијих сила света, уједно и најразвијених земаља, број жртава приближи нултој стопи. Назначене тежње водиле су, последњих деценија, ка постепеном премештању борбених дејстава са копна и мора у ваздух и свемир а, током последњих двадесет година, и у кибер простор. Убрзани развој информационе и комуникационе технологије у последњим декадама XX века довео је до споја машине, тј. рачунара и војника, којим се дистанца између супротстављених страна увећава а самим тим и равнодушност према жртвама.

Паралелно са активностима на развијању и усавршавању могућности и средстава за вођење конвенционалних сукоба кинетичким оружјем, високо развијене земље су користиле своју технолошку предност за унапређивање способности вођења специјалног рата.

На почетку XXI века, дакле, суочени смо са чињеницом да су, осим оружане агресије као средства за остваривање циљева агресивне политике, присутни и други облици силе који су садржани у „арсеналу“ специјалног рата. Познато је да је Пентагону омиљен метод упућивање других да извлаче врућe кестене из ватре.[101] У вези са поменутим, неки аутори наводе да многе америчке научноистраживачке установе и лабораторије које раде за ове снаге, интезивно разрађују, усавршавају и испробавају нова оружја и диверзантска средства, бешумне пиштоље, аутомате, снајперске пушке, минобацаче, фугасе, ампуле са отровима, борбена отровна средства и смртоносне бактерије.[102]

---

[101] Милашиновић Р.: *Терор Запада над светом - савремени механизми разарања и подчињавања суверених земаља и народа*, Ветерник, 1998, стр 7.

[102] Agee P.: *Dnevnik agenta*, Globus, Zagreb, 1975, стр. 477 – 501.

Нова технолошка достигнућа се, по правилу, јављају као одговор на потребе саме војске. Осим што своју примену налазе у војсци, ова достигнућа се користе у свим сегментима „безбедносне делатности“. У савременом контексту безбедности „глобални рат против тероризма“, напори да се контролише илегална имиграција (кроз увођење биометријских метода идентификације), удвостручени напори да се задржи висок ступање војне спремности против стварних и потенцијалних претњи, који укључују повећану потребу за системима јавног надзора, утичу на високу владину и корпоративну потрошњу на напредне информационе технологије како у САД тако и у Европи.

На пример, Агенција за напредна истраживања Министарства одбране САД (DARPA) покушава да створи читав опсег нових технологија повезаних са вођењем „глобалног рата против тероризма“ које би у будућности могле имати и комерцијалну примену. DARPA је помогла при стварању Интернет технологија током шездесетих и седамдесетих година прошлог века ARPANet-ом и архитектуром везаном за TCP/IP мрежне протоколе. Током деведесетих година, DARPA је учествовала у осмишљавању сателитске навигације, која се сада употребљава у цивилном саобраћају, а такође је асистирала и при развоју система *стелт* технологије.[103]

Поред тога што ради на напретку свемирске технологије (као што су нано-сателити) DARPA је предвидела и напредак у мрежно-центричном ратовању; атомски сат са интегралним колом дизајниран за већу прецизност у приказивању времена како би се осигурале мрежне комуникације; технологије којима се могу идентификовати и осујетити терористичке активности (попут производње и распоређивања импровизованих експлозивних уређаја); брзе беспилотне летелице које могу лебдети током дугих временских периода; суперкомпјутере за војне сврхе који истовремено могу извршавати велики број операција; висококвалитетно машинско превођење текста и говора у реалном времену; развој протетике која може бити мождано перципирана и контролисана; испитивање квантног феномена на пољу рачунара, криптографије и комуникација; додатне алтернативне технологије и

[103] *DARPA Strategic Plan* (2007), http://www.darpa.mil/body/news/2007/2007StrategicPlan.pdf

изворе енергије како би се превазишла суштинска зависност војске од нафте и њених деривата.[104]

Поред тога, DARPA развија и паноптичке компјутерске системе за идентификацију како би слика лица на камери за надзор могла бити спојена са начином хода, висином, тежином и осталим елементима битним за распознавање особа. Треба додати и то да се нове пан-сензитивне технологије за надзор развијају тако да могу детектовати радио сигнале које емитују људи, те да могу детектовати откуцаје срца и дисање кроз чврсте препреке. Предвиђа се да би нови уређаји, који могу дати назнаке о ономе о чему људи размишљају, могли бити доступни за десетак година.[105]

2.2.1. Трендови у војним издацима

Потреба за ојачавањем војне моћи и система безбедности приморава државе да инвестирају у наоружање и војну опрему и да улажу у друге облике војне потрошње. То, опште узев, одржава војне издатке на врло високом нивоу. Готово парадоксално звучи податак да данас, када се говори о побољшаној безбедности у највећем делу света и смањеној могућности избијања рата великих размера, војни издаци и даље расту. За то постоје бројни разлози а један од најзначајнијих је тај што у развијеним државама војна потрошња има значајан утицај на развој.[106]

Анализирајући војну потрошњу САД после Другог светског рата, за време и након завршетка Хладног рата, могу се уочити осцилације у војним издацима које претходе значајним догађајима на међународној политичкој сцени (Корејски и Вијетнамски рат, Кубанска криза, криза Варшавског пакта, завршетак хладноратовског периода, припреме и освајање Евроазије и слично) или их прате. Војна потрошња САД у том периоду приказана је у Табели 1.

---

[104] *Ibid*.

[105] Hawksley H.: *Big Brother is watching us all*, BBC News, 15 September 2007, http://news.bbc.co.uk/2/hi/programmes/from_our_own_ correspon-dent/6995061.stm

[106] *Cross-dimensional aspects of security*, OSCE, SEC.GAL/150/04, 29 June 2004, p. 6.

Табела бр. 1: *Војна потрошња САД у периоду 1945-2008. године (у милијардама УСД)*

Година	Потрошња	Година	Потрошња	Година	Потрошња	Година	Потрошња
1945	962,7	1961	291,1	1977	232,7	1993	312,1
1946	500,6	1962	300,0	1978	233,2	1994	290,3
1947	133,7	1963	293,3	1979	237,4	1995	272,1
1948	94,7	1964	294,8	1980	246,2	1996	265,6
1949	127,8	1965	268,3	1981	260,8	1997	336,2
1950	133,0	1966	297,3	1982	282,0	1998	328,6
1951	225,7	1967	354,1	1983	303,2	1999	329,4
1952	408,5	1968	388,9	1984	318,1	2000	342,2
1953	437,0	1969	371,8	1985	343,7	2001	344,9
1954	402,1	1970	346,0	1986	363,7	2002	387,3
1955	344,5	1971	311,7	1987	371,1	2003	440,8
1956	320,7	1972	289,1	1988	372,8	2004	480,5
1957	322,4	1973	259,5	1989	376,2	2005	503,4
1958	317,9	1974	243,8	1990	358,7	2006	511,2
1959	306,9	1975	242,0	1991	316,5	2007	546,8
1960	289,6	1976	234,0	1992	328,6	2008	607

Извор: Center for Defense Information U.S. Military Spending (1945-1996.) and SIPRI, Military Expenditure of USA and SIPRI Yearbook 2009 (1997-2008.), http://www.cdi.org/Issues/milspend.html, http://milexdata.sipri.org/result.php4

Војни издаци на светском и регионалном нивоу у периоду 1988-2007. године указују на то да су:

- војни издаци у 2007. години, у односу на војне издатке у 1988. години повећани у свим регионима света, осим у Европи (и њеним подрегионима), што говори да се осим богатих, односно Севера, на јачање војне моћи оријентисао и највећи број држава Југа, при чему се проценат повећања креће од 12,6% (Северна Америка) до чак 135,7% (Северна Африка);
- подрегиони са највећим војним издацима у 2007. години су Северна Америка и Западна Европа, и на њих одлази преко 67% војних издатака на светском нивоу;
- пад војних издатака у Европи (посебно у Источној) резултат је пре свега распада Варшавског пакта и СССР-а и понашања Западне Европе (боље улагати у развој и квалитет живота, пошто је она иначе под безбедносним кишобраном САД);
- на светском нивоу, војни издаци су падали од 1988. године (1987. године је остварен максимум у војним издацима) до 1998. године, када почињу поново да расту. У посматраном периоду они су у просеку 3% мањи од

војних издатака у 1988. години али тренд њиховог раста у последњим годинама није заустављен.[107]

Анализа војних издатака за петнаест држава са највећом војном потрошњом у 2007. години (Табела 2) показује да:

- је војна потрошња за 2007. годину процењена на 1214 милијарди УСД, што чини 2,5% од БДП на светском нивоу или средњу потрошњу од 183 УСД *per capita*;
- петнаест прворангираних држава у војној потрошњи учествује у 83% укупне војне потрошње, док на САД отпада 45%, затим следе Велика Британија, Кина, Француска и Јапан са учешћем сваке од њих са око 4%;
- Кина и Индија, две светске долазеће економске силе доприносе укупном расту војне потрошње, при чему је повећање војне потрошње сваке до њих чврсто усклађено са њиховим економским растом;
- је војна потрошња у 2007. години порасла за око 18% (213 милијарди УСД) у односу на војну потрошњу у 2005. години (војна потрошња у 2005. години износила је 1 001 милијарду УСД).[108]

Табела бр. 2: *Државе са највећом војном потрошњом у 2007. години (у милијардама УСД)*

Војна потрошња према МЕР мерилима						**Војна потрошња у ППП мерилима**		
Ред. Број	**Држава**	**Потрошња (у мд $)**	**Светско учешће (%)**	**Потрош. по глави**	**% од БДП, 2006**	**Ред. број**	**Држава**	**Потрош. (у мд $)**
1.	САД	547	45	1 799	4,0	1.	САД	547
2.	В. Британија	59,7	5	995	2,6	2.	Кина	(140)
3.	Кина	(58,3)	(5)	(44)	2,1	3.	Русија	(78,8)
4.	Француска	53,6	4	880	2,4	4.	Индија	72,7
5.	Јапан	43,6	4	339	1,0	5.	В. Брит.	54,7
6.	Немачка	36,9	3	447	1,3	6.	С. Арабија	52,8
7.	Русија	(35,4)	(3)	(249)	3,6	7.	Француска	47,9
8.	С. Арабија	33,8	3	1 310	8,5	8.	Јапан	37,0
9.	Италија	33,1	3	568	1,8	9.	Немачка	33,0
10.	Индија	24,2	2	21	2,7	10.	Италија	29,6
11.	Ј. Кореја	22,6	2	470	2,5	11.	Ј. Кореја	29,4
12.	Бразил	15,3	1	80	1,5	12.	Бразил	26,7
13.	Канада	15,2	1	461	1,2	13.	Иран	22,1
14.	Аустралија	15,1	1	733	1,9	14.	Турска	16,5
15.	Шпанија	14,6	1	336	1,2	15.	Тајван	15,8

Извор: SIPRI, *The fifteen major spenders in 2007*, http://archives.sipri.org/contents/milap/milex/mex_trends.html

[107] *Ibid*.

[108] Према: http://www.sipri.org/

Од средине тридесетих година XX века војни издаци су се повећали петнаест пута. Стопа раста војних издатака је превазишла стопу раста светске популације, стопу експанзије глобалне економске производње и трошкове за здравство. Сваког минута на војне трошкове потроши се два милиона УСД.[109]

Историјски гледано, богате државе имају највеће војне издатке и такав тренд се и даље наставља. Из приказане статистике види се да на развијене државе отпада око 80% укупних светских издатака за одбрану. Последњих неколико година војни издаци у богатим државама Севера и сиромашним државама Југа, конвергирају једни другима, односно пораст војних издатака богатих прати пораст војних издатака у сиромашним државама. При томе, државе Севера троше око 2,5% од свог БДП (САД 4%, В. Британија и Француска по 2%, итд) а државе сиромашног Југа између 5 и 10% од свог БДП. Тако је амерички војни буџет за 2009. годину износио 515 милијарди долара, а кинески 56 милијарди или 1,4% БДП НР Кине. То указује на чињеницу да ниво перципираних претњи у сваком региону од потенцијалних конфликата унутар држава и ширења конвенционалног и другог оружја за масовно уништење, врши велики утицај на повећање нивоа војних издатака сваке државе. Слични закључци се намећу и у вези са различитим регионалним организацијама и војним савезима.

2.2.2. Трендови у војним технологијама

Савремене оружане снаге данас карактеришу пре свега савремено наоружање и војна опрема за ратовање, коју пре свега чине авиони без људске посаде, авионске бомбе и ракете високе прецизности, брзи и прецизни ракетни системи, пројектили са самонавођењем, оружја са усмереном енергијом и др. Жеља држава за изградњом ефикасног безбедносног система, свеукупним јачањем (укључујући и јачање војне моћи) и очувањем националних интереса, доводи до тежње за престижом а то се у крајњој мери претвара у општу трку у наоружању.

Производњу савременог оружја могуће је реализовати на најмање два начина. Прво, усавршавањем постојећег наоружања и војне опреме, чиме оно постаје

[109] Кегли Ч., Виткоф Ј., *op. cit*., стр. 656.

прецизније, ефикасније, отпорније на дејства противника и др. што му продужава животни век и смањује трошкове одржавања и производње. Други начин подразумева производњу нових врста оружја заснованих на савременим војним технологијама. У том смислу приметна је непрекидна трка у истраживању и развоју нових војних технологија и нових врста оружја за шта се издвајају огромна финансијска средства. Војно-индустријски комплекси и њихови истраживачки и производни ресурси у развијеним државама свакодневно јачају прерастајући у нову делатност и уносно занимање. Војно-индустријски комплекс, као спрега између војске и индустрије, представља покретачку снагу трке у наоружању и стварања ратних жаришта у свету. Дакле, почетак XXI века карактерише револуција у истраживању војних технологија и њихове примене у производњи оружја.

Присталице технолошке револуције и производње савременог оружја тврде да се на тај начин рат може учинити мање деструктивним, односно да нова оружја могу послужити као политички инструмент демонстрирања моћи и то на начине цивилизованог коришћења војне силе. С друге стране, заговорници забране трке у наоружању и истраживања нових технологија за војне потребе, доводе у питање ефикасност ратовања и етику роботског убијања на даљину несмртоносним оружјима. Уз то постављају питања: да ли су паметне бомбе довољно паметне? Да ли су прецизна оружја заиста ефикасна? Шта је са великом вероватноћом техничке и људске грешке?

Мада истраживање и развој војних технологија увек иде испред осталих истраживања и стварни је покретач свеукупног научно-техничког прогреса, оба ова поља заједно са револуцијом која се дешава на пољу информатике чине основу производње савремених оружја. У основи овог концепта су опције засноване на микропроцесорима, глобалним комуникацијама и технологији прецизно вођених пројектила (муниције, бомби, ракета) с циљем вођења или спречавање будућих сукоба али без ослањања на оружја за масовно уништење. Заправо, присталице технолошке револуције у војним пословима верују да ће финије и суптилније оружје трансформисати начине на који ће се водити ратови.[110]

[110] *Ibid*., стр. 674.

У основи технолошке револуције налази се веровање да је несмртоносно оружје практично, јер може користити вештачку интелигенцију рачунара и напредне технологије која омогућава прецизне ударе који могу „заслепети, имобилисати и држати противника на удаљености уз истовремено индентификовање и уништавање циљева.“ Део арсенала ових оружја и њихових могућности примењен је у Другом заливском рату (1990 - 1991.) и рату против СРЈ 1999. године, када је циљ остварен без и једног изгубљеног америчког војника.

Говорити о невидљивости, прецизности, ефикасности, информативној доминантности, доминацији у телекомуникацијама, ракетној одбрани, значи очекивати дан када ће роботи заменити војнике у борби, када ће авиони летети без пилота носећи најсавременија оружја за уништавање циљева и на земљи и у ваздуху а одбрана заснована на кибернетици и коришћењу паметног и бриљантног система оружја омогућити доношење софистицираних одлука о томе где, када и како деловати.

Нуклеарно оружје. Процењује се да је највећи број нуклеарних сила већ развио нуклеарно оружје треће генерације које је способно да уништи противникове стратегијске циљеве у било ком сукобу у ваздуху и на земљи. Његова основна разлика у односу на класичне нуклеарне бојеве главе је та што има врло мали удео у ефектима глобалне контаминације уз задржавање истих ефеката разарања.

Ласерско оружје. САД су развиле ласерско оружје за онеспособљавање органа вида. О његовој примени, односно увођењу у наоружање, нема јавно доступних података. Поред овог, САД и друге развијене и војно јаке државе развиле су читав арсенал ласера велике снаге и ласерских јединица на копну, мору и у ваздуху, намењених за онеспособљавање електрооптичких уређаја противника. У ову групу, мада не егзактно, могу се сврстати и оружја на бази некохерентног светла на којима се врше интензивна истраживања.

Оружја на бази електромагнетне енергије. Електромагнетна енергија односно електромагнетни таласи (ЕМТ) јесу основа за напредак човечанства будући да ЕМТ игра кључну улогу у компјутеризацији и телекомуникацијама.. Међутим, ЕМТ чине и широку основу даљих истраживања ради примене у војне сврхе. Осим што се ЕМТ већ увелико користе у свим управљачко-вођеним системима и пројектилима, актуелна истраживања се спроводе у циљу изградње новог оружја заснованог искључиво на ЕМТ. У стручној литератури се могу прочитати чланци о

уређајима велике снаге (пар стотина мегавата) који емитују електро-магнетну енергију у импулсима (врло кратког времена трајања – неколико нано секунди). Ти таласи (тзв. „таласи смрти“) брзином светлости „предају“ своју енергију одабраном циљу који се загрева, топи и испарава. Постоје и друга истраживања са ЕМТ, па се у америчким научним часописима могу наћи текстови о електронском аутомату, пушкомитраљезу и сл., дакле новим оружјима који ће уместо класичног зрна „испаљивати“ ЕМТ, а не смемо заборавити ни њихов значај када је у питању неокортикални рат.

Несмртоносна оружја. Несмртоносна оружја су она оружја која не садрже експлозивна средства (и често се одликују малим степеном разарања). Намењена су за уништавање противникове живе силе, односно њено привремено или трајно онеспособљавање за дејства и ометање, онеспособљавање и уништење електро-оптичких, рачунарских и свих других електро средстава. У ову групу спадају: ласерско оружје, оружја на бази емитовања некохерентног светла, оружја на бази електромагнетних таласа и друга.

Постоје и друга бројна истраживања за потребе производње нових оружја и већина њих су базирана на неком од решења са усмереном енергијом. Тако Американци раде на оружјима која би пружила ефикасну заштиту носачима авиона или, пак, која би била применљива у евентуалном рату у космосу а Руси на усмереном честичном оружју енормне снаге чији би разарајући потенцијал могао да буде усмерен на целокупну територију неке државе или неки део земаљске кугле. Нанотехнологија и њој сродне технологије колико сутра могу наћи своје место у производњи оружја а то радикално може изменити све постојеће односе снага и војне моћи, па чак и битно утицати на ниво међународних односа уопште. Примена ових и сличних идеја у блиској будућности може битно изменити све планетарне услове у којима живимо данас. [111]

[111] Kaufman M.: “Bush Sets Defense As Space Priority”, *Washington post*, October 18, 2006.

2.2.3. Значај информационо-комуникационих технологија

Убрзани развој науке и технологије, нарочито у другој половини двадесетог века, достигао је такав темпо да су се нови технолошки и културни обрасци смењивали не више на сваки век или пола века, већ сваке деценије, а пред крај те епохе и чешће. Тешко је пронаћи адекватан заједнички атрибут за претходно столеће. У различитој публицистичкој, али и научној литератури оно је називано не само веком светских ратова већ и атомским веком, веком глобалне културе и економије, веком медијâ, првом свемирском ером, епохом мултиполаризма, столећем пластике итд.

И за друштвене науке именовање претходног столећа још представља изазов. Са социолошког аспекта посебно је значајан развој информационе и комуникационе технологије након Другог светског рата, јер је довео до важних промена у начину организовања и функционисања друштва. Настанак комуникационих инструмената, попут телевизије, првих генерација рачунара и сателита, у великој је мери повећао брзину и могућности за размену информација, али је утицао и на промене у свим сферама друштвених активности па и оних у погледу ратовања.

У намери да нагласи актуелне промене у друштвеном животу, али и потребу за усклађивањем социолошке терминологије са захтевима времена, социолог Данијел Бел 1973. године употребљава термин „постиндустријско доба“ односно „постиндустријско друштво“.[112] Бел је, у фази настајања, уочио следеће карактеристике постиндустријског друштва:

- развој почива на производњи информација,
- у производњи доминира креативно-иновативни рад,
- серијска и појединачна производња добара,
- иновативност,
- флексибилност у системима вредности,
- флексибилност и покретљивост у организацији (штрафтасти оковратници),

[112] Bell D.: *The Coming of Post-Industrial Society: A Venture in Social Forecasting*, Basic Books, New York, 1973.

- претварање хијерархијске у хоризонталну структуру, како у производњи, тако и у друштву,
- губљење јасних и прецизних разлика у социјалној структури, и
- стварање мрежних информационих система и флексибилних аутономних облика одлучивања.

Потреба за информацијом и знањем, коју је први уочио Бел, и даље се сматра једним од најбитнијих обележја савременог света. Информација и знање су, међутим, одувек били битни ресурси за човечанство – у толикој мери да је мања или већа могућност приступа и преношења информација могла да, током историје, одреди успех или неуспех цивилизација и култура. Потреба за комуникацијом и разменом информација, дакле, није карактеристика само нашег времена.

2.2.3.1. Информација као стратешки ресурс информационог доба

Данас нема јединственог приступа феномену информације, а још мање једнозначне и општеприхваћене дефиниције информације. Информација је постала релевантан појам за све науке које се баве симболичком комуникацијом, у распону од математике до рачунарске науке, или од логике до лингвистике, односно од електронике до библиотекарства, као и од хуманистичких наука и уметности до документаристике, али и од друштвених наука до медицине. То је информацији дало интердисциплинарну димензију, јер је свака наука покушала и још покушава да протумачи тај комплексан појам. Све ово нам говори да појам „информација“ није лако схватити нити једноставно протумачити.

Реч „информација“ изведена је из латинске речи *informatio*, што значи појам, порука, скуп спознаја, представа. Појам информације би се могао одредити као садржај о одређеном догађају, појму, збивању, процесу који отклања неку неодређеност и на тај начин увећава сазнање, а увек се креће од обавештенијег субјекта ка примаоцу нижег нивоа обавештености. Према Шафранском, информација је „садржај или значење поруке“. Информације се генеришу (и/или перципирају) као визија (слика), звук, укус, мирис и све остало што прихватају људска чула.[113]

[113] Вулетић Д.: „Шта је информационо ратовање?“, *Безбедност*, бр. 3/05, Београд, 2005, стр. 494.

„Енкартин“ (Encarta) електронски енглески речник из 2005. дефинише информацију као „одређено знање стечено о нечему или некоме; прикупљене чињенице и подаци о одређеној ствари“.[114] Информација је кратког трајања и поседује временски ограничен квалитет, који се често контролише на основу комплета динамичких услова и одлука. Догађаји могу утицати на то да нека од информација буде ирелевантна или толико нерепрезентативна да представља изузетно нетачну слику реалности.

Норберт Винер, творац кибернетике, сматра да су информације значајан ступањ у непрекидном процесу посматрања спољног света и утицаја на њега. Винер види информације као меру реда, која у неком затвореном систему по правилу тежи да се смањи, насупрот ентропији, која представља меру нереда и тежи да се спонтано повећава. Он информацију дефинише као садржај „који је размењен са спољашњим светом у поступку усаглашавања са њим“,[115] чиме наглашава доминантно прагматички аспект информације.

Људска цивилизација се одувек заснивала на потреби и способности комуницирања, те је у ту сврху развијала одређене технолошке форме за размену информација. Бубњеви, бакље, димни сигнали, пиктограми, записи на керамичким или каменим таблама и књиге примери су технолошких форми којима се човек служио да би смањио ограничења наметнута простором и временом у комуникацији и преносу знања. Биле ове форме примитивне или напредне, њихова ефикасност је увек била условљена раздаљином, позицијом комуниканата или амбијенталних услова у којима се комуникација одвијала (видљивост, клима итд).

Половином XIX века дошло је до прве суштинске промене у способности комуникације, промене која се континуирано наставила следећих 150 година, са толико великим варијететима и модалитетима да је попримила револуционарне карактеристике. Стога се тај период може сагледати као јединствена информациона

---

[114] Важно је начинити разлику између податка и информације, појмова који се често поистовећују. На пример, број 6 је податак и он као такав нема посебно значење, међутим, „Сада је 6 часова“ јесте информација, јер је податку додељено неко значење. Тако можемо увидети да се информација састоји од податка и значења које му је додељено.

[115] Винер Н.: *Кибернетика и друштво*, Нолит, Београд, 1973.

револуција[116] еволутивног карактера или, пак, као три одвојена раздобља, подједнако важна да се сматрају засебним револуцијама.[117]

Прва информациона револуција почиње половином XIX века и траје једно столеће. Типични инструменти комуникације овог периода јесу телеграф, радио и телефон.

Следећа револуција је почела половином XX века и завршила се почетком осамдесетих година. Њена средства су телевизија, прве генерације рачунара и сателити. Телевизија је представљала прогрес у односу на радио, а захваљујући њој је постало могуће пренети већи број информација у ефикаснијем формату. Рачунари су, са друге стране, повећали могућност сакупљања, анализе и употребе информација, док су сателити створили глобалну инфраструктуру телекомуникација.

Савремени информациони системи развијени су крајем осамдесетих и почетком деведесетих година прошлог века. Њихову основу чине персонални рачунари и рачунарске мреже. Развој и примена информатике и информационих система засенили су све оно што је у претходним двема револуцијама постигнуто у сфери размене информација и дефинисали су Трећу информациону револуцију, која се често, из разумљивих разлога, назива и информатичком револуцијом. Трећа информациона револуција заснива се, пре свега, на осам технолошких достигнућа: унапређени полупроводници, рачунари нове генерације, оптичка влакна, мобилна телефонија, сателитска технологија, унапређен начин мрежног повезивања рачунара, унапређена интеракција човек–рачунар и дигитални пренос. Обједињене, ове технологије се генерално означавају као информационо-комуникационе технологије. Свака од њих понаособ значајно ојачава способност коришћења и размене информација, а ослобађа се ограничења времена, раздаљине и позиције.

Системи за размену информација и преношење знања, констатовали смо, постојали су и постоје у свакој људској заједници, без обзира на степен њеног

---

[116] Под појмом информационе револуције подразумевамо иновативна техничко-технолошка достигнућа која су омогућила значајан квалитативан помак у начину и брзини преношења информације.

[117] Papp D. S., Alberts, D., Tuyahov, A.: "Historical Impacts of Information Technologies: An Overview", у: *The Information Age: An Anthology of Its Impact and Consequences*, vol. I, ed. David S. Alberts & Daniel S. Papp, CCRP Publication Series, 1997.

технолошког развоја. Међутим, за разлику од претходних, савремени информациони системи су углавном мрежно организовани и баве се производњом, чувањем, обрадом и дисеминацијом информација применом одговарајућих информационо-комуникационих технологија.[118]

Синергијско коришћење информационо-комуникационих технологија довело је до револуције чији смо сведоци. Последице ове револуције могу се сажети у следеће тезе:

- већа брзина преноса информације, те бржа интеракција између учесника (појединаца, организација, држава итд);
- већа способност вођења, обраде и тумачења великог броја информација, која даје шире могућности доносиоцима одлука, организацијама или појединцима да стекну јаснију слику ситуације према којој доносе одлуке;
- екстремна флексибилност тока информација: информација може бити (истовремено) објављена на више локација, примљена из више извора, и то у кориснијим формама (текстуалним или мултимедијалним), док се комуникација може одвијати и само између заинтересованих кореспондената;
- већа могућност приступа информацијама него икад раније. То нас, према неким експертима, доводи до демократизације тока информација и комуникација свуда у свету, па самим тим и до смањења могућности настанка „монопола над информацијама“ од стране привилегованих (владе, организације или власти уопште узев), тј. доминације информативних канала.

С обзиром на то да је променила саме могућности стварања и ширења знања, Трећа информациона револуција се понекад назива и „првом револуцијом знања“.

Достигнућа Треће информационе револуције, попут настанка персоналних рачунара[119] и стварања, прво, технолошки неусавршених локалних рачунарских мрежа, а затим и глобалне мреже – Интернета – утицала су на економску, политичку и културну сферу друштвеног живота свих развијенијих држава света. Ови

---

[118] Џигурски О., *op. cit*., стр. 149.

[119] Први персонални рачунар, под називом „IBM Pesronal Computer – PC“, представљен је јавности 1981. године. Убрзо након тога PC је постао централни производ рачунарске индустрије, око којег се концентришу сви тржишни и развојни концепти.

информационо-комуникациони инструменти нашли су широку примену у друштву, постали су „технологија масе“, али и запослених у различитим делатностима и постепено су надмашили број радника.[120] Рачунарске мреже су постале централни елемент друштва а, у апстрактном смислу, термин „мрежа“ је постао метафора многих аспеката модерног живота. Из наведених разлога данас многи теоретичари употребљавају појам „информационо друштво“.[121]

Развој друштвених и технолошких формација – мрежа – карактеристичних за „информационо друштво“ почива на тековинама западне мисли које сасвим јасно можемо да распознамо још у револуцији математичке логике, двадесетих и тридесетих година XX века, или тек нешто каснијем развоју кибернетике као опште теорије система. Термин „информационо друштво“ налази своју примену од седамдесетих година XX века, а карактеристичан је за друштвене описе тек у последње две деценије.

Паралелно са изразом „информационо друштво“ користи се и израз „информационо доба“. Порекло израза „информационо доба“ приписује се футуролозима Алвину и Хајди Тофлер, који су га први пут употребили 1980. године

---

[120] Kushnick B.: *The Unauthorized Biography of the Baby Bells & Info-Scandal*, New Networks Institute, 1999, p. 22.

[121] На основу прегледа домаће литературе може се закључити да је у српском језику чешћа употреба термина „информатичко“ од „информационо“. Међутим, поставља се питање да ли је то и оправдано. Др Србислав Букумировић тврди да је „феномен информација и буран развој ове делатности после Другог светског рата условио различит приступ овом појму и различиту терминологију“. Тако је за теорију научних информација шездесетих година прошлог века у Француској и бившем СССР-у усвојен термин „информатика“, док је у англосаксонским земљама коришћен термин „computer science“. Данас се тамо користи израз „наука о информацијама“ („information science“), а у енциклопедији *Википедија* се наводи да неки аутори сматрају како је информатика синоним за науку о информацијама.

Развојем делатности у вези са информацијама и широком применом информационо-комуникационих технологија у друштву, а посебно развојем Интернета, почела је да се прави разлика између науке о информацијама и њене широке примене у друштву као делатности (као што се разликују здравство као делатност и медицина као наука).

Откада је специјализована агенција УН за просвету, науку и културу УНЕСКО задужена и за информације, почео је да се уводи неки терминолошки ред у овој области. Тако је већ прва, а посебно друга конференција UNISIST донела низ терминолошких објашњења и речник термина на крају документа. Преовладавајући је израз „информационо-комуникационе технологије“, а исти је случај и са „информационим друштвом“ – и два светска самита су носила овај назив (Светски самит о информационом друштву WISIS – World Summit on the Information Society). Сви светски језици употребљавају израз „информациони“, истиче професор Букумировић (дневни лист *Политика*, 22. мај 2007). Мишљења смо да треба прихватити аргументе ауторитетâ у овој области, те да у циљу редукције терминолошких забуна, следствено светским трендовима, нашу терминологију треба ускладити са терминологијом УН.

у књизи *The Third Wave*.[122] Употреба термина „информационо доба“ данас се најчешће среће код аутора који сматрају да је галопирајућа дифузија нових информационих технологија сасвим сигуран знак да је на хоризонту догађаја приступна једна до сада непозната, сасвим нова форма друштвене организације.

Концепт „информационог друштва“, често довођен у везу са развојем Треће индустријске револуције, окупирао је разне политичке, научне и популарне дискурсе у последњој деценији XX века. Као што примећују неки аутори, друштвена и научна дебата о информационом друштву рекапитулира еволуцију друштвених типологија чије корене налазимо још у XVIII веку. На начин на који данас говоримо о савременом друштву као информационом, у претходним временима смо говорили о капиталистичком, социјалистичком, либералном, потрошачком, постмодерном итд. друштву.[123]

У одређењима концепта „информационог друштва“, разна схватања наглашавају различите аспекте људског односења према централном појму информације.

Флеч, у студији „The Information Society: The Role of Networks and Information“, представља следеће схватање концепта информационог друштва:

„Термин информационо друштво имплицира централну улогу информације. У овој новој ери извор продуктивности се све више налази у технологији стварања знања, обраде информација и комуникације. Посебно се употреба постојећих знања у долажењу до нових увида карактеристично везује за потенцијал информационог друштва. Овај изузетан круг позитивних ефеката почива на два главна ослонца: информацијима и технологији.

Суштински покретач информационог друштва су информације. Али информације су одувек представљале кључни фактор у друштвима широм света. Разлика је у томе што сада располажемо софистицираним средствима у форми ИКТ

---

[122] Тофлер А.: *Трећи талас*, Просвета, Београд, 1983.

[123] Миловановић Г.: *Концепт информационог друштва и друштвени ефекти интернета*, Центар за проучавање информационих технологија, Београдска отворена школа, Београд, стр. 2.

која омогућавају тренутну обраду, дупликацију и дистрибуцију информација и знања по скоро ништавној цени.“[124]

Као се може видети, Флечово схватање циља на суштинско одређење информационог друштва, представљајући концепт информације као централан, овлаш уводећи анализу односа технологије и постојећег фонда знања у процесу долажења до новог знања. Схватање овог аутора доста је карактеристично за теоријски усмерене ауторе и по олакој опасци о „ништавној цени“ средстава за обраду информација, којом се ставља у заграду чињеница да озбиљан приступ информационим технологијама данас себи може да приушти тек око десет процената становника наше планете, бар уколико је о Интернету реч.[125]

Canadian Forest Service нуди један од најбољих онлајн извора за читаоце заинтересоване за дисциплину менаџмента знањем (*knowledge management*) и у оквиру своје презентације нуди следеће сажето разумевање информационог друштва:

„Информационо друштво: друштво у коме се људи налазе у интеракцији са технологијом као битним делом живота и друштвене организације у функцији размене информација на глобалној скали.“

Можда ово одређење информационог друштва заиста представља језгровит начин да се овај концепт представи али се не можемо сложити са једном битном одредницом у њему, наиме, да је реч о „размени информација на глобалној скали“.

Да је таква размена информација могућа, сасвим је тачно, као и то да се она свакако одвија; међутим, језичке, културне и економске баријере у великој мери нас још увек раздвајају од Маклуановог глобалног села. Овакво схватање информационог друштва представља добар пример честог превида у коме се изоставља да је за глобалну размену информација, и глобално учешће човечанства у тој размени, потребно много више од просте чињенице да се приступ Интернету може технички да оствари скоро ма где. Основна писменост, познавање страних

---

[124] Flach M.: *The Information Society - The Role of Networks and Information*, http://artilect.org/altman/moritz.pdf

[125] Миловановић Г., *op. cit*., стр. 4.

језика, претходно образовање и, свакако, информатичка писменост, само су неки од услова који морају бити претходно задовољени.

Коначно, завршни документ прве фазе Светског самита о информационом друштву (World Summit on the Information Society – WSIS), одржаном под покровитељством Уједињених Нација 10 - 12. децембра 2003. у Женеви[126], понудио је следеће схватање овог концепта:

„[...] Информационо друштво, у коме свако може да ствара, приступа, користи и дели информације и знање, омогућавајући тако појединцима, друштвима и народима да развију своје потенцијале потпуно у промоцији сопственог одрживог развоја и унапређењу квалитета живота [...].“[127]

Формулација која је употребљена у завршном документу Самита је сасвим очекивано усидрена у дискурс развојних планова Уједињених нација. Добра страна овог одређења је свакако у томе што поставља концепт информационог друштва у позитиван оквир који наглашава искоришћавање људских потенцијала и остваривање добробити. Међутим, ова радна дефиниција може бити корисна за формулисање политичких платформи развоја, али тешко да ће у било којој научној расправи бити од користи пука чињеница да у информационом друштву сви имају приступ информацијама и знању.

На основу само претходна три карактеристична одређења, видимо да схватање информационог друштва садржи у себи и технолошке и социолошке одреднице, нагласак на битном односу интеракције човека и технологије, подсећање на конститутивну улогу информација у људском друштву независно од текуће технолошке револуције, племените визије о будућности у којој су знање и информације ресурси доступни свима... Иако се можемо сложити да Флечова дефиниција представља најбоље полазно тле за анализе у друштвеним наукама од

---

[126] На Самиту је 175 земаља света усвојило два важна документа – Декларацију о принципима и Акциони план. Том скупу присуствовало је педесет председника држава и заменика председника, 82 министра, највиши представници међународних организација, приватног сектора и цивилног друштва, који су пружили политичку подршку овом амбициозном пројекту. Самит је одржан у организацији једне од агенција УН – Интернационалне телекомуникационе уније (International Telecommunication Union – ITU), која тренутно броји 191 државу чланицу.

[127] *Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. Document WSIS-03/GENEVA/DOC/4-E, 12 December 2003.*

понуђених схватања, концепт информационог друштва очигледно има сопствени, развијен „друштвени живот знака“ у оквиру једног дискурса за који се верује да представља глобални дискурс садашњице. Међутим, оно што је карактеристично за сва изнета схватања је да она непосредно везују концепт информационог друштва за информационе технологије, не наглашавајући са њима повезане политичке, економске и културне промене.

У сваком случају, можемо закључити да не постоји коначна или академски прихваћена дефиниција „информационог друштва“, због различитих гледишта са којих се може посматрати утицај који оно има на људске активности (економски, технолошки, социјално-политички итд). Евентуално се може рећи да је информационо друштво оно друштво које у свом развоју и производњи као главну „погонску снагу“ има производњу и размену информација. То је друштво произашло из информационе револуције, засновано и формирано на употреби информационих и комуникационих технологија.

У информационом друштву су стварање, дистрибуција и коришћење информација, али и манипулација информацијом, постале централне активности већине грађана, на радним местима и унутар институција. У односу на индустријска и аграрна друштва, радни инструменти информационог друштва јесу рачунари и средства телекомуникације, а средства транспорта су Интернет и мас-медији. У складу са великом важношћу рачунарских мрежа, у литератури се често користи и израз „умрежено друштво“.[128]

Коришћење Интернета и осталих видова модерног комуницирања, нарочито у последњих петнаестак година, постало је више од „статусног симбола“, тј. постало је потреба како појединца, организације или шире заједнице, тако и државе. Развој информационе и комуникационе технологије повећао је брзину и обим интеракција у „умреженом друштву“ и тиме допринео интензивирању како друштвених односа у сфери политике, економије, науке и културе, тако и међузависности појединаца, група и нација широм света. Повећање међузависности, као последица „глобалног

[128] *Социолошки речник*, прир. Аљоша Мимица и Марија Богдановић, Завод за уџбенике, Београд, 2007, стр. 74.

умрежавања“, тј. „сажимања простора и времена“, у новије време је подстакло чак и расправе о превазиђености форме националне државе.[129]

Данас готово да и нема друштвене делатности у којој се не примењује, или у којој барем не би могла бити применљива, информационо-комуникациона технологија. Отуда је каткад у употреби и израз „информатизовано друштво“ који се као синоним користи за израз „информационо друштво“. Први израз, међутим, снажније наглашава технолошку зависност савременог друштва од информационо-комуникационих технологија, док други израз истиче значај друштвених активности везаних за стварање, обраду и размену информација.

Мишљења смо да је управо зависност од информационих технологија једна од основних карактеристика друштва у „техно-троничној ери“. Уколико бисмо покушали да објаснимо концепт „информатизованог друштва“, бар на најширим основама, могли бисмо да тврдимо да је то друштво за које је карактеристичан висок степен зависности економских, политичких, културних, и уопште друштвених структура од човеку екстерних процеса обраде информација.

Под екстерним процесима обраде информација овде се, у првом реду, подразумевају технологије аутоматске обраде информација, односно технолошки производи развоја електронике и разних грана математичких и техничких дисциплина у XX веку. За непуних сто година, прећен је пут од формалних скица првих система за обраду информација, преко раних рачунара који су заузимали читаве просторије и окупирали тимове запослених, до комфорних, ергономски задовољавајућих и технички супериорних микрокомпјутера без којих живот савременог човека постаје незамислив.

Концепт екстерне обраде информација у себи имплицитно садржи још један слој садржаја који је кључан за разумевање информатизованог друштва. Наиме, пре свега под снажним диктатом развоја економије после Другог светског рата и револуције у развоју електронских медија, савремено друштво се нашло у ситуацији у којој капацитети обраде информација који почивају на појединцу, па чак и читавим тимовима, ни из далека не могу да задовоље временске оквире у којима је потребно

[129] О овом проблему видети шире у: Цветковић В.: *Социологија*, Факултет цивилне одбране, Београд, 2005; Гиденс Е.: *Социологија*, Економски факултет, Београд, 2003.

реаговати да би се успешно учествовало у економској, политичкој, војној а данас и свакодневној динамици коју диктира огромна количина информација којом смо окружени.

2.2.3.2. Настанак и карактеристике кибер простора

2.2.3.2.1. Појмовно одређење кибер простора

Битно обележје информатичке револуције јесте настанак такозваног кибер простора (cyberspace). Префикс(оид) „кибер“ (или „сајбер“) учестало се користи кад год је потребно створити нове термине да би се објаснили концепти везани за информационе и комуникационе технологије и револуцију информације. Први га је употребио научник Норберт Винер, у другој половини четрдесетих година XX века, у својим истраживањима која су представљала основу нове научне дисциплине – кибернетике.[130]

Канадски писац Вилијем Гибсон (William Gibson) први је употребио термин „кибер простор“, 1984. године, у научнофантастичном роману *Неуромант*.[131] Гибсонов кибер простор је универзум рачунарских мрежа, дигитални свет у којем се мултинационалне компаније, друштва и информатичари-пирати боре за освајање података и информација. Његова футуристичка визија практично је антиципирала настанак новог културног и економског простора: „То је отаџбина информационог доба – место где ће грађани будућности живети.“[132]

Од издања *Неуроманта* концепт кибер простора често је коришћен. С обзиром на то да не постоји универзално прихваћена дефиниција, значење овог појма трпело је измене, мада се, и поред тога, он увек односио на информације

---

[130] Кибернетика је научна дисциплина која изучава механизме којима људи, животиње и машине комуницирају са спољашњим амбијентом и контролишу га. Она је мултидисциплинарна наука која је тесно повезана са другим дисциплинама и технологијама: филозофијом, психологијом, математиком, биологијом, физиком, вештачком интелигенцијом, теоријом контроле, теоријом комуникације, роботиком. Кибернетика посебно изучава механизме комуникације и интеракције код живих бића, у циљу бољег упознавања, али и стварања модела који могу бити вештачки репродуковани. Винер је употребио термин „кибернетика“ у тежњи да нађе одговарајући назив за опис поља контроле, реч „timonier“ (*грч*. kybernetes) учинила му се примереном. У преводу на *енгл*ески језик добија се неологизам cybernetics.

[131] Гибсон В.: *Неуромант*, IPS Media, Београд, 2008.

[132] *Ibid*.

размењене путем рачунара.[133] Тако је у онлајн речнику *Webopedia* кибер простор дефинисан као „метафора која се користи за опис не-физичког простора, створеног међусобним повезивањем рачунара, путем мреже телекомуникација, ради комуникације“.[134]

Према Швартауу (W. Schwartau) кибер простор је „неопипљиво место између рачунара, где информација накратко постоји у свом току са једног на други крај глобалне мреже. Он је етерична стварност, безброј електрона који се крећу бакарним жицама или стакленим влакнима, брзином светлости.“[135] Аркила (J. Arquilla) и Ронфелт (D. F. Ronfeldt) користе дескриптивну дефиницију: „Кибер простор постоји где год постоје телефонски каблови, линије стакленог влакна или електромагнетни таласи. Ови простори су настањени знањем електронског облика.“[136]

У *Социолошком речнику* кибер простор се дефинише на следећи начин: „Кибер простор (енгл. *cyberspace*) јесте виртуелни простор који настаје у контакту човека и рачунара. У свакодневном говору под тим изразом најчешће се подразумева дигитални свет конструисан уз помоћ рачунарских мрежа, попут нпр. Интернета. То место, иако заиста постоји, могло би се описати пре као комуникацијски медиј него као потпуно другачија галаксија, јер се многе од свакодневних пракси и дискурса кроз њега преламају и структуришу га кроз известан однос узајамне повезаности. Иако се кибер простор најчешће перципира као нематеријално краљевство података или као нека врста виртуелне стварности, он заправо има и сасвим физичку инфраструктуру, сачињену од жица које се налазе изнад и око наших глава, каблова који леже поред наших ногу и сателита на небу који круже око наше планете; све то омогућава интеракцију која на нивоу сензација материјализује квалитет нематеријалности, којим кибер простор најчешће описују његови конзументи. Кибер простор је нова форма менталне димензије људске егзистенције унутар које настаје

---

[133] Харвардски професор права J. P. Barlow први је 1990. године употребио термин „кибер простор“ за означавање електронског и социјалног простора какав данас познајемо – Интернета. Према: http://homes.eff.org/~barlow/.

[134] Дефиниција према: *Webopedia*, http://www.webopedia.com.

[135] Schwartau W.: *Information warfare: chaos on the electronic superhighway*, Thunder’s Mouth Press, New York, 1994, p. 49.

[136] Arquilla J., Ronfeldt D. F., *op. cit*., p. 23.

симулирана реалност као последица интеракције између људског и артифицијелног интерфејса. Он представља алтернативну просторну димензију унутар које се успоставља веза између различитих персоналних рачунара, рачунарских мрежа, различитих виртуелних заједница и појединаца који могу, али и не морају да буду њихови чланови. Кибер простор се налази у перманентном процесу промене и практично може бити бесконачан у 'величини', иако унутар њега просторна и временска димензија често добијају посве померена/измењена значења. Комуникација са и унутар кибер простора се успоставља тренутно, при чему је физичка локација корисника у највећем броју случајева потпуно неважна..."[137]

Чињеница је да су са настанком кибер простора нарочито идеје простора и времена претрпеле радикалну трансформацију, са релевантним последицама на остале, за њих везане концепте, као што су: удаљеност, територија, ограничења, раздвајање или граница. Баш као и физички простор, кибер простор садржи ентитете, тј. информације (различитих облика, попут порука, електронске поште, *web*-сајтова, фајлова итд), који могу бити транспортовани, испоручени или преузети. Кибер „предмети" се, међутим, крећу у димензији која се, иако садржи многе аналогије са физичком димензијом, од ње осетно разликује.[138] Где год да је публикована, информација је приступачна било коме у мрежи, у којој год он земљи био, са временом приступа информацији које више не зависи од раздаљине, већ евентуално од проблемâ чисто техничке природе.[139]

У том смислу, Пол Вирилио (P. Virilio) истиче да смо, уместо са „Фукујаминим прерано најављеним крајем Историје...", данас суочени са „... крајем простора једне мале планете која лебди у електронском етеру наших савремених

---

[137] *Социолошки речник*, прир. Аљоша Мимица и Марија Богдановић, Завод за уџбенике, Београд, 2007, стр. 60.

[138] Ако замислимо да једну поруку електронске поште послату из Србије треба да прими корисник са регистрованим „рачуном" (account) код аустралијског ISP-а (Internet service provider), појединачни пакети података, од којих је састављена порука путују кроз небројене чворове мреже у различитим земљама, а затим се меморишу у рачунару (*server*) који се физички налази у Аустралији. Због начина функционисања мреже, сваки пакет може да следи различиту руту, другачију од осталих; исто тако, аустралијски корисник прима на исти начин и поруку послату од пошиљаоца са минималне физичке удаљености. Овај процес се, у нормалним условима функционисања, обавља у врло кратком времену.

[139] На пример, од пропусне моћи конекције, ефикасности сервера, преоптерећености линија итд.

средстава за телекомуникацију“.[140] На другоме месту, он каже: „Инфосфера – односно сфера информације – намеће се геосфери. Почињемо да живимо у редимензионираном свету. Способност интеракције смањује свет готово на нулу.“[141]

У свакодневном говору „кибер простор“ се најчешће користи као синоним за Интернет, што, по мишљењу стручњака, у области информатике није оправдано. Први аргумент се састоји у тврдњи да је појам „кибер простор“ шири од појма „Интернет“, будући да обухвата и друге типове мрежно повезаних рачунарских система (као што су на пример: Интранет, LAN, WAN итд). Други аргумент је онтолошке природе. Према њему ова два појма описују две другачије стварности: док Интернет представља прецизну технолошку инфраструктуру, сачињену од физички постојећих елемената, кибер простор се односи на не-физичку димензију, нематеријални простор створен информационом инфраструктуром, у тренутку када се она користи за размену информација.

Са аспекта нашег предмета истраживања и холистичког приступа овој проблематици, сматрамо да наведена дистинкција није од пресудног значаја. Ми је имплицитно усвајамо, али у раду на њој нисмо инсистирали. У односу на наведене аргументе сматрамо да је из два разлога легитимно каткада синонимно употребљавати ове појмове: 1) уколико су различити видови безбедносних претњи[142] присутни у глобалном информационо-комуникационом систему – Интернету – они су присутни и у кибер простору или пак, по аналогији, могу бити присутни и у локалним информационим системима; 2) различите безбедносне претње, присутне у једној „не-физичкој стварности“, за свој циљ имају наношење штете или уништење друге „физичке стварности“.

Са позиција безбедносних наука сфера интересовања је превасходно усмерена на последице које кибер ратовање може проузроковати за безбедност

---

[140] Вирилио П.: *Информатичка бом*ба, Светови, Нови Сад, 2000, стр. 12.

[141] Интервју са Полом Вирилиом објављен је у чланку “Speed pollution”, *Wired*, http://www.wired.com.

[142] У подручју информационе безбедности претња се дефинише као било која акција, намерна или ненамерна, која је потенцијално у стању да компромитује приватност, интегритет или расположивост информације или система који је преносе. Према: “Cybersecurity for Critical Infrastructure Protection – Technology assessment”, United States General Accounting Office (GAO), http://www.gao.gov; *Guideline for Identifying an Information System as a National Security System*, National Institute of Standard and Technologies (NIST), http://csrc.nist.gov.

државе, њених институција, становништва и имовине. У том смислу, за потребе овог истраживања адекватан је појам кибер простора као шири, у односу на ужи појам Интернета, којим смо се служили зарад постизања прецизности у оним сегментима рада у којима је истраживање то захтевало.[143] Из тог разлога, али и зато што Интернет данас представља највећи информационо-комуникациони систем, како по величини тако и по броју корисника, и што се у односу на овај систем постављају стандарди у регулисању области информационо-комуникационих технологија, неопходно је упознати се са историјом његовог настанка.

2.2.3.2.2. Настанак, развој и архитектура Интернета

Порекло Интернета, као што је то често случај са новим технологијама, не може се приписати једној особи, јединственом пројекту или теоријском систему. Настанку глобалне информационе мреже допринели су, често посредним путем, различити људи и идеје.

Интернет се рађа у јеку Хладног рата као резултат надметања (између осталог, и технолошког) Сједињених Америчких Држава и Совјетског Савеза. Значајан технолошки успех који су остварили Совјети слањем првог сателита у орбиту („Спутњик“, 1957. године) дубоко је потресао уверење Американаца у сопствену техничко-војну надмоћ. Са циљем да преузме иницијативу, администрација САД је осмислила оснивање посебне агенције чији би основни задатак био стимулација и финансирање научних истраживања у свим секторима који би могли да имају војни значај.

Тадашњи секретар одбране Мекелрој убедио је председника Ајзенхауера у неопходност оснивања такве агенције. Конгрес је 1958. године одобрио оснивање и финансирање Агенције за напредне истраживачке пројекте (Advanced Research

---

[143] У одређеним истраживањима друштвених наука прихватање наведене дистинкције сигурно би било оправдано, на пример, у истраживањима кибер социологије (*енгл*. cyber sociology) – социолошке дисциплине која је настала средином деведесетих година XX века и која се бави проучавањем квалитета и законитости људске интеракције у измењеним комуникационим условима унутар координатног система кибер простора. Овај измењени облик људске комуникације назива се CMC (*computer mediated communication*, тј. комуникација посредована рачунаром), коју најчешће супротстављају комуникацији face-to-face (лицем у лице) у свакодневним људским контактима. Према: *Социолошки речник*, прир. Аљоша Мимица и Марија Богдановић, Завод за уџбенике, Београд, 2007, стр. 60.

Projects Agency – ARPA), са седиштем у згради Пентагона у Вашингтону. Одмах по оснивању ARPA је своје активности усмерила у истраживање ваздушног простора. Међутим, након неколико месеци ови пројекти прелазе у надлежност NASA-е, те је постало неопходно да се за ARPA-у пронађу нова поља за развојна истраживања – највише је обећавала, тада нова, наука о рачунарима.

Одлучујући импулс у том смеру дао је трећи директор Агенције, научник Џек Руjна (Jack Ruina). Руjна је увео неформалан стил рада и позвао талентоване колеге које нису биле из војних кругова. Међу њима је најзначајнију улогу одиграо психолог Ликлајдер (J. C. R. Licklider). Од самог почетка су његова интересовања била усмерена на интерфејс човек–компјутер и утицај који би рачунарске машине могле да имају на развој когнитивних и комуникационих способности човека (чак тридесет година пре него што ће ови концепти постати централни у информатичком сектору). Ликлајдер је своје идеје изложио у чланку „Симбиоза човек–компјутер“ (“Man-Computer Symbiosis”, 1960).[144]

Ликлајдер је провео кратко време у ARPA-и, али је то било довољно да утиче на даљи развој Агенције. Међу бројним наследницима идеја да се рачунари повежу у мрежу највише је заинтересовала младог научника Боба Тејлора (Bob Taylor).

Готово истовремено се у другом центру за војна истраживања RAND,[145] инжењер Пол Бејрен (Paul Baran) бавио проблемом могућности постизања континуитета операција стратешког система команде и контроле Америке у случају нуклеарног напада. Традиционалне (телефонске) мреже комуникација, на којима се заснивао цео апарат војне контроле, биле су, у то време, потенцијално врло рањиве. Бејрен је дошао до два закључка: први је гласио да једна безбедна мрежа мора имати децентрализовану и разгранату конфигурацију, како би се омогућило постојање већег броја путева за проток информација са једног на други крај исте мреже. Други закључак је био да се систем телекомуникација мора заснивати на новим машинама

[144] Scalese A.: *La sicurezza del cyberspazio: analisi e considerazioni*, Facoltà di Scienze Politiche, Università degli Studi di Trieste, 2005, p. 11.

[145] Центар „Rand“ је смештен у Калифорнији, настао је у оквиру корпорације *Douglas Aircraft*, а аутономију је стекао после Другог светског рата, са циљем да настави примењена истраживања започета током светског конфликта.

дигиталног прорачуна, које су у стању да користе софтвер за исправку или уклањање грешака и софтвер за избор комуникационих канала.

Бејрен је затим осмислио модел мреже у којој је сваки чвор везан за најмање четири друга чвора, где, за разлику од принципа телефонске мреже, ниједан од њих нема функцију концентратора. На овај начин би сваки чвор наставио да функционише примајући, обрађујући и преносећи информације, чак и у случају да су неки оближњи чворови оштећени. Бејрен је сматрао да би непостојање централног чвора, чијим би потенцијалним уништењем могао да буде угрожен рад целе мреже, смањило могућност војног напада на комуникациону инфраструктуру.[146]

Осим поменуте идеје о децентрализованој и разгранатој мрежи, Бејрен је имао још једну замисао: уместо слања поруке од једног до другог чвора у облику јединственог блока података, било је боље поделити га у одвојене делове који би могли да путују различитим путевима ка крајњој дестинацији, где би се поново објединили. Након неуспешних покушаја да убеди техничаре компаније AT&T, тадашњих монополиста у области телекомуникација, Бејрен је 1965. године дефинитивно одустао од пројекта. Истих година енглески физичар Доналд Дејвис (Donald Davies), полазећи од другачијих претпоставки, доспео је до сличних закључака као и Бејрен.

Дејвис је нудио реализацију јавне мреже, довољно брзе и ефикасне, која би омогућила размену података између удаљених рачунара нове генерације. Његово решење се базирало на подели порука у једнаке блокове, како би рачунар могао истовремено да управља слањем и примањем велике количине порука, скраћујући на тај начин време обраде сваке поруке. Он је делове (блокове) поруке назвао „пакети“ (енгл. *packet*), а овакав модел комуникације „размена пакета“ (енгл. *packet switching*), што је представљало алтернативу „циркуларној размени“, на којој су се заснивали традиционални телефонски системи.

---

[146] Према: Griffiths T. R.: *The History of Internet*, Leiden University, Leiden, 2002, http://www.let.leidenuniv.nl/history/ivh/chap2.htm

Све ове теоријске замисли, независно уобличене у различитим установама, обједињене су 1969. године у пројекту ARPANET.[147] Намера инжењерâ је била да се повежу четири рачунарске магистрале, инсталиране у различитим државама САД, у циљу омогућавања размене порука путем преноса „пакета“ података. ARPANET, претеча Интернета, приказана је јавности 1972. године. Након два периода, која, ради поједностављивања, можемо дефинисати као „војни“ (од 1969. до 1980. године) и „академски“ (од 1980. до 1991), током којих су стандардизовани и усавршени сви основни протоколи Интернета, почео је „комерцијални“, или „јавни“ период, који још траје.[148] За тридесетак година Интернет се од релативно мале мреже намењене истраживању трансформисао у важно средство за међународну економију и друштво у целини. Интересантно је напоменути да је тек 24. октобра 1995. дата формална дефиниција Интернета.[149]

Према једној од најопштијих дефиниција, Интернет представља „глобални комуникациони систем међусобно повезаних рачунарских мрежа намењен размени података различитих типова“.[150] Његова битна одлика јесте да он нема власника, тј. ниједна држава или институција нема власт над целином. Појединци, државе и институције власници су делова комуникационих канала или рачунарске и комуникационе опреме која се користи на Интернету. Поред тога, на Интернету је свако власник само свог рачунара или (интерне) мреже и има неограничено право да тај рачунар користи по својој вољи и да на њему чува садржаје које жели. При томе, власник рачунара сâм бира начин прикључења на Интернет, количину и врсту информација које ће преузимати, као и властите садржаје које ће учинити доступним

[147] Три истраживачка центра (MIT, RAND Corporation и National Physical Laboratory) поставила су теоријску основу за пројекат ARPANET.

[148] Griffiths, T. R., *op. cit*.

[149] Термин *Интернет* се, према овој дефиницији, односи на глобални информациони систем који је: логички повезан једним јединим адресним простором, заснованим на Интернет-протоколу (IP) или на његовим накнадним модификацијама, подржава комуникације коришћењем „suite TCP/IP“ или његовим накнадним модификацијама и остале протоколе компатибилне са IP; обезбеђује, користи или чини доступним, јавно или приватно, услуге високог нивоа засноване на нивоу овде описаних комуникација. Извор: Internet Society, http://www.isoc.org.

[150] Џигурски О., *op. cit*., стр. 117.

осталим корисницима мреже. Данас Интернет нуди велику количину података различитих типова, којима се приступа преко стандардних Интернет-сервиса.[151]

Интернет је заснован на два основна архитектонска принципа:[152]

1. употреби протокола комуникације (размени пакетâ) и
2. „интелигентној“ терминалној (рачунарској) контроли преноса информација.

Њима је додат трећи елемент, који, иако не чини прави архитектонски принцип, утиче на природу Интернета:

3. децентрализован процес дефинисања стандардâ и протоколâ (непостојање формалне владе мреже).

1. *Употреба протокола комуникације*. Интернет је интерконекција милионâ рачунара у целом свету, а сваким од њих независно управљају појединци или организације који су изабрали да се прикључе општим протоколима комуникације, нарочито протоколима познатим као TCP/IP (Transmission Control Protocol/Internet Protocol). Протоколи TCP/IP чине могућим Интернет, а њихова основна карактеристика је дефинисање мреже која ради на основу размене пакета, метода помоћу којег се подаци пре слања деле на стандардизоване пакете који се затим шаљу на одредиште. Трасирање путање (*routing*) обавља се помоћу безбројних посредничких диспозитива (*router*). Када један од ових посредника прими пакет података, чија дестинација није рачунар у локалној мрежи, шаље га према неком другом рутеру оптималним путем. Рачунар пошиљалац и рачунар прималац не морају да знају ништа о путањи којом пакети путују, а чест је случај да различити делови информације путују различитим путањама. Још важније је да, са техничкога гледишта, рачунари у мрежи могу комуницирати без икаквог познавања технологије мреже која преноси податке. Коришћење стандардизованих протокола TCP/IP даје

[151] World Wide Web (WWW) је тренутно најзначајнији сервис на Интернету. Овај сервис се може дефинисати као документациони систем који омогућава да странице са мултимедијалним садржајима буду доступне корисницима путем рачунара повезаног са Интернетом. Нагли развој Интернета последњих година омогућен је настанком овог сервиса. Поред тога, овај сервис полако обједињава све остале сервисе на Интернету и преузима њихову улогу.

[152] *Architectural principles of the Internet*, Network Working Group RFC-1958, 1996, p. 1, http://www.ietf.org/rfc/rfc1958.txt

илузију кориснику Интернета да је он део једне јединствене велике мреже, иако је у суштини Интернет збир независних мрежа.

2. *„Интелигентна“ терминална (рачунарска) контрола преноса информација*. Други кључни елемент архитектуре Интернета чини принцип дефинисан као „од тачке до тачке“ (*point to point*), што значи да сама мрежа не поседује „интелигенцију“, тј. не одређује начин на који ће бити употребљена, већ то чине терминали/рачунари уз помоћ протокола TCP/IP. Непостојање унутрашње интелигенције мреже чини да све пакете који су у складу са протоколом TCP/IP мрежа третира независно од њиховог информационог садржаја и врсте апликације, тј. без обзира на идентитет или намеру пошиљаоца, али и примаоца који ће пакете користити на одредишној дестинацији.

3. Трећи стожер Интернета чини *децентрализован процес дефинисања стандарда и протокола*. Интернет не припада нити подлеже управљању и контроли једне агенције или институције, већ њиме руководи међународна непрофитна невладина организација, која нема својство правног лица – Интернет-друштво (Internet Society – ISOC). Њена структура се састоји од следећих организационих јединица: Инжењерске радне групе за Интернет (Internet Engineering Task Force – IETF), Одбора за архитектуру Интернета (Internet Architecture Board – IAB), Управљачке групе за Интернет-инжењеринг (Internet Engineering Steering Group – IESG) и Истраживачке снаге Интернета (Internet Research Task Force – IRTF).

Са техничког и развојног гледишта, Интернет се одржава и развија стварањем, опробавањем и имплементацијом стандарда Интернета дефинисаним од стране IETF-а. За разлику од осталих транснационалних организација за стандардизацију, IETF нема ригидна правила, нити руководство, нити формално чланство, већ било ко може да се региструје и учествује на његовим састанцима и дискусијама.

Процес стандардизације је врло комплексан, с обзиром на то да је резултат преговарања при којем се свака одлука доноси постепено, након отворених дискусија у мрежи. Основни елементи овог процеса јесу документи названи *Захтеви за коментаре* (Requests for Comments – RFC), који се, осим стандардима, баве широким спектром тема везаних за Интернет. RFC је постао основни инструмент

размене мишљења, универзално прихваћен начин за препоручивање, реформисање и усвајање нових техничких стандарда.

Друге две организације које на неки начин имају утицаја на управљање Интернетом јесу *WWW конзорцијум* (World Wide Web Consortium – W3C) и *Интернет-корпорација за додељена имена и бројеве* (Internet Corporation for Assigned Names and Numbers – ICANN).[153] И оне, као и IETF, имају седиште у САД. Легитимитет ових организација произлази из тога што су оне биле прве које су, спонтано и волонтерски, радиле на развијању Интернета. ICANN, стационирана у Калифорнији, представља делимичан изузетак, с обзиром на то да је од стране Министарства трговине САД задужена да управља *Системом Интернет доменâ* (Domain Name System – DNS)[154] и да на њене одлуке америчка влада има право вета. Наведена архитектонска структура одредила је успех Интернета, али она, у исто време, чини и основу његове несигурности.

2.2.3.2.3. Техничко-технолошки узроци несигурности кибер простора

Примена три претходно описана архитектонска принципа Интернета (коришћење протокола комуникације, терминална контрола преноса информација и децентрализован процес дефинисања стандардâ и протоколâ) створила је глобалну рачунарску мрежу која није дискриминишућа према садржају што се путем ње размењује. Светска рачунарска мрежа суштински је анархична и лишена механизама самоодбране и заштите корисникâ. Другим речима, мрежа је суштински несигурна. Ово сазнање није изненађујуће уколико се узме у обзир чињеница да је технологија (која је у основи Интернета) створена са знатно другачијим циљем од оних који су данас разлог популарности Интернета. Мрежа је била намењена искључиво

---

[153] ICANN на светском нивоу управља додељивањем називâ домена и IP адреса. Сваки уређај (обично дефинисан термином "host") повезан у мрежу TCP/IP означен је IP адресом (слично телефонским бројевима у фиксној мрежи). IP адреса се састоји од четири броја, између 0 и 255, одвојених тачком (на пример, 192.1.23.0.213). Ова врста облежавања није практична за коришћење и тешко се може запамтити, па се, дакле, асоцира са именом домена (*domain name*), као, на пример, „fb.bg.ac.rs". *Domain name server* је програм који (као телефонски именик) повезује име домена и IP адресу хоста.

[154] DNS (*енгл*. Domain name system) јесте, у основи, систем који претвара имена рачунара (*hostnames*) у IP адресе. DNS такође обезбеђује податке о серверима електронске поште на домену (MX), почетном DNS серверу (SOA) и друге. DNS је заснован на хијерархијском принципу и једна је од основних компоненти Интернета.

техничко-научној елити, те самим тим није било потребе за њеном заштитом од злонамерне употребе. Истраживачки и развојни напори су изнад свега били усмерени ка утилитарним циљевима, поузданости и способности физичке одрживости мреже, више него према њеној безбедности. Интернет је био осмишљен тако да има максималну отпорност према спољашњим физичким нападима – пројектна решења мреже нису предвиђала софтверске нападе од стране сопствених корисника.

Осим тога, жеља је била да се створи апсолутно флексибилан и отворен инструмент који је у стању да без напора обухвати бројне хетерогене ентитете са којима би био у могућности да подели услуге и ресурсе. Резервисаност, интегритет и располагање размењеним подацима, као и сигурност у идентитет учесникâ у преношењу података (неопходних за сигурност кибер простора) били су апсолутно маргинални у односу на основне циљеве. Међутим, несигурност кибер простора не зависи само од природе Интернета (прецизније, од природе протокола TCP/IP). Иако ова природа представља погодно тло за тзв. кибер нападе, небезбедности мреже доприноси и карактеристична рањивост[155] умрежених система.

Основни проблем рањивости умрежених рачунарских система чини раширено коришћење комерцијалних хардвера и софтвера. Приликом њиховог креирања пажња произвођача је, изнад свега, усмерена пре на брзину лансирања ових производа на тржиште (као и на проширење спектра додатних функција) него на питања безбедности и поузданости.[156] Услед тога се дешава да слабости пројектовања и реализације постају основа неправилног функционисања умрежених рачунарских система. Чест је случај да поменути недостаци бивају уочени са закашњењем, када производе већ користе милиони корисника и организација у

[155] Рањивост је слабост која се може искористити за извршавање неауторизоване или нелегитимне акције у мрежи или систему. Када је рањивост искоришћена за компромитовање безбедности система или информација које он садржи, идентификује се безбедносни инцидент. Број рањивости ИКТ производа порастао је са 171 (1995. године) на 4.1.2.9 (2002. године), са мањим опадањем 2003. и 2004. године (3.784; 3.780). Године 2005. број је достигао 5.990. Извор: CERT/CC, http://www.cert.org.

[156] Scalese A.: *op. cit*., стр. 17.

целом свету.[157] Неправилности у функционисању комерцијалних компоненти представљају „слабе тачке“ рачунарских система, које неретко бивају искоришћене од стране злонамерних субјеката да оштете или „присвоје“ информационе системе који се ослањају на ове производе, наносећи, на тај начин, последице за безбедност њихових корисника.

Начелно, може се рећи да несигурност кибер простора има двојаку основу:

1) Прву чине технички дефекти производа ИКТ.
2) Другу чине грешке и пропусти организација и индивидуалних корисника приликом управљања производима и/или коришћења производâ ИКТ, такозвани „људски фактор“.

Прва категорија рањивости најчешће произлази из архитектонског избора и пројектног избора усвојеног у фази развоја производа ИКТ.[158] Рањивост која проистиче из архитектонског избора може се одстранити само мењањем архитектуре која је у основи производа ИКТ, са могућим негативним последицама на друге аспекте или функционалност самог производа и науштрб компатибилности са свим другим апликацијама. Тешко је, ако не и немогуће, накнадно уклонити ову врсту рањивости. Потенцијална угроженост се може делимично умањити једино коришћењем додатних производа, неопходних за ублажавање рањивости.[159] Лакше се могу спречити рањивости које су резултат пројектних грешака.[160] И оне, међутим, представљају проблем, с обзиром на то да врло често нису елиминисане благовремено, или уопште нису елиминисане, будући да неопходне корекције морају бити јавно обелодањене од стране произвођача.

---

[157] Најпознатији пример такве аномалије био је тзв. *миленијумски баг*, или *миленијумска бомба* (који се назива и проблем „Y2K“ – скраћеница за 2000. годину), и односио се на проблем записа датума у формату dd/mm/yy (или mm/dd/yy). Иако је недостатак отклоњен брзо, пре „доласка“ новог миленијума, он је изазвао одређену штету. Тако је, на пример, рачунарски систем у лондонској компанији „Marx & Spencer“ 1998. године, радећи инвентуру, уништио неколико тона хране. Рачунар је 2002. годину, која је била рок трајања неких прехрамбених артикала, интерпретирао као 1902, те је наредио уништавање „96 година“ старе хране.

[158] На пример, оперативни системи (као што је „Microsoft Windows“) који омогућавају извршавање програма без сагласности корисника – на тај начин омогућавају и нежељено активирање посебних програма званих „вируси“.

[159] У односу на претходни пример – коришћење антивирусног софтвера.

[160] Када су откривене, оне се лако могу уклонити применом софтверских корекција, тзв. „закрпа“ (*енгл*. patch[es]), које доставља произвођач.

Друга врста рањивости се уопштено може повезати са недостатком пажње, а неретко и образовања корисникâ о безбедности сопствених система. Недостатак безбедносне културе уочљив је како на индивидуалном нивоу тако и на нивоу предузећâ и организација које користе кибер простор у институционалне сврхе, и то не само на управљачком већ и на извршном (операционалном) нивоу.

У стручним круговима уврежено је мишљење да вртоглаву експанзију Интернета није истовремено пратила и одговарајућа специјализација стручњакâ на пољу информационе безбедности. У том смислу Е. Спафорд (E. Spafford), директор Центра за едукацију и истраживање у области информационог осигурања и безбедности универзитета Пардју, истиче: „Безбедност није могуће лако додати накнадно, што знатно отежава задатак професионалцима безбедносног сектора. Софтвер и хардвер који се данас користе пројектовани су неправилним методима, а такође се накнадно лоше тестирају, од стране особа које знају мало или готово ништа о безбедности, што је резултовало непоузданим резултатима. Затим се додају постојећој инфраструктури, која је већ пуна слабости и којом управља, и користи је, особље недовољно упознато са ризицима. Нико не би требало да се изненади повећањем броја напада и вируса у годинама које следе.“[161]

У односу на могуће последице треба истаћи да не постоје важније и мање битне рањивости. Колико год се могу чинити благим, оне „отварају врата неочекиванōм и непредвидивōм. То је нарочито тачно у доминацији технологије и информације, где скривене међусобне зависности повезују националне критичне информационе инфраструктуре.“[162] Критичне информационе инфраструктуре јесу информационе инфраструктуре државе, које гарантују оперативност и тачност информатичких структура. Уништење упоришта ових структура и њихове пратеће опреме, односно нарушавање њихове оперативности током дужег временског периода, може у значајној мери угрозити безбедност становништва.[163]

Ако пробамо да генерализујемо, може се рећи како проблем несигурности кибер простора произлази из комплексности система, вероватно најкомпликованијег

---

[161] http://www.house.gov

[162] Verton D.: *Virtual threat, real terror: Cyberterrorism in the 21st Century*, http://judiciary.senate.gov

[163] Према: Regional Development Glossary, http://www.emergence.nu/toolkit/glossary.php

до сада произведеног у људској историји. Милиони рачунара су део тог система, међусобно су повезани најразличитијим начинима, а сваки је у међусобној и екстерној интеракцији са десетином програма. Осим тога, као што је већ поменуто, кибер простор се развио и тренутно се користи на начин потпуно непредвиђен за оне који су га пројектовали.[164] Другим речима, он манифестује особине које нису изворно биле сматране потенцијалом система.[165] Те нежељене особине су и рањивости и такозвани *баг* (енгл. *bug* – грешка, квар), типичне дисфункције информационих система које не производе прави прекид услуге, али које, понекад, на непоновљив и привидно необјашњив начин, наводе систем на непредвидива и штетна понашања.

Наведене карактеристике – комплексност, међусобна повезаност и испољавање нежељених особина – имају дубоке последице на безбедност кибер простора и чине задатак њеног очувања врло тешким.

2.2.4. Историјски осврт на однос технолошког развоја и могућности управљања перцепцијом током ратних сукоба

Техничко-технолошки изуми, констатовали смо, налазе своју непосредну примену у војним активностима, увећавају моћ страна у сукобу те на тај начин имају и директан утицај на исход конфликата. Други аспект утицаја нових технолошких достигнућа на исход конфликата може се пратити кроз њихов посредни утицај на друштвене сукобе – кроз омогућавање нових начина за ширење пропаганде, дезинформација и управљање перцепцијом.

Посматрано из историјске перспективе, може се констатовати да су информација и проток вести имали огроман значај током оружаних конфликата. С обзиром на то, као посебно важна питања намећу се: утицај средстава комуникације и њихов развој као и начин на који су војна пропаганда и новинарска информација утицале на јавно мњење.

---

[164] На пример: за електронску трговину, обављање финансијских трансакција, „стварање“ виртуелних комуна и томе слично.

[165] Schneier B.: *Secrets and Lies. Digital security in a networked world*, Wiley computer publishing, New York, 2000, p. 7.

На ова питања желимо да дамо одговор у овом одељку рада, имајући на уму, као што су већ многи уважени аутори истакли, да се начин представљања конфликта јавности знатно променио током времена, паралелно са еволуцијом комуникационих средстава.

У том смислу је важно истаћи да се ратови не воде само војним средствима и оружјем већ и путем информације. Ратни извештачи, фотографи и камермани директно са ратних попришта шире веома упечатљиве слике, информације и поруке, које могу бити објективне у већој или мањој мери. Ови садржаји понекад нису у складу са званичним политикама сукобљених држава.

У тоталитарним режимима, војну пропаганду као и већину информација, обично контролише директно председник владе. У демократским земљама приступ информацијама је слободнији утолико што је могуће користити разноврсне изворе информисања, па у том случају медији могу да играју улогу критичара ратне политике сопствених влада.

То се догодило током рата у Вијетнаму, када је група новинара, критичних према понашању Беле куће, објавила серију слика јаког емотивног утиска и на тај начин из корена променила став јавног мњења, утицавши тиме и на будуће одлуке владе и судбину рата.

Проучавање оваквих, појединих екстремних друштвених конфликата из различитих епоха, открива интересантне аспекте везане за улогу мас-медија, њихову еволуцију и коришћење од стране националних влада и армија.

Са аспекта анализе међусобне повезаности медија и политике током међународних конфликата те на основу коришћења инструмената комуникације, који су постајали све софистицираније и тежи за контролу, могу се издвојити два периода:

Први обухвата период од друге половине 19. века до Другог светског рата. Током овог периода, покривеност догађаја од стране медија зависила је искључиво од националних влада, које су путем пропагандних акција и цензуре покушавале да добију сагласност јавног мњења за војну интервенцију.

Нарочито је током Првог светског рата влада била та која је управљала јавним мњењем, убеђујући грађане у исправност разлога за учешће у конфликту, у потребу да се издрже жртве и, нарочито, у неопходност личног ангажмана у

конфликту. Средства информисања контролисана су од стране државе. Коришћена је пропаганда као инструмент за стварање алтернативног тока информација, али и цензура ради прикривања неподобних чињеница.

Током Другог светског рата пропагандни апарат користио се у великој мери радиом који је давао могућност интензивне активности у ширењу контраинформација са циљем утицања на понашање становништва и непријатељске војске.

Други период почиње ратом у Вијетнаму и траје до данас. Током овог периода владе нису увек успевале да контролишу и, према сопственим потребама, прилагоде информативи апарат – захваљујући присуству нових медија као што су телевизија и Интернет. Телевизија и Интернет су променили начин „конзумирања“ вести. Готово тренутно преносећи догађаје, они су пружили реципијенту конкретан осећај да је директан сведок ратних дешавања.

Тако, на пример, у Фокландском и Првом заливском рату није све ишло у правцу који су одредили владини и војни менаџери информисања, будући да су се медији почели понашати као својеврстан отуђени лоби који одбија послушност режиму.

Изумом штампе 1455. године, Гутенберг је олакшао писање и дифузију вести а накнадна средства комуникације су, без сумње, довела до еволуције традиционалних новинарских критеријума избора и селекције вести.

У првим ратовима друге половине 19. века, новинарска покривеност је била врло ограничена – постојала је само фигура извештача који одлази на место догађаја, прикупља информације и описује их у новинама. Наравно, тај процес је био врло спор јер у то време нису постојали уређаји за брз пренос вести. Открићем телеграфа, начињен је помак у преносу информација, јер је смањено време трансфера са неколико недеља на неколико секунди.

Наредне технолошке иновације попут радија (почетак XX века), телевизије (шездесетих година XX века) и, на крају, Интернета, додатно су повећале брзину преноса информација, али су и повећале могућности за манипулацију информацијама.

Телевизија је, више од радија, променила однос између војних активности и стратегија и комуникационих средстава, повећавши визибилност догађаја. Ењо

Ремондино, италијански ратни извештач из Београда током агресије НАТО на СР Југославију, износи интересантно запажање: „Наравно да телевизија није измислила рат, али је постала његова сублимација, неопходан инструмент за потврђивање или оповргавање самих разлога конфликта.“[166] Може се констатовати да је током ратних конфликата последњих деценија тријумфовала телевизија, јер је наметнула свој модел нарације и естетике. Пред фасцинантним синхронизованим током слика и звукова, гледалац добија утисак да има директан приступ стварности и истини. Бодријар, познати француски социолог и филозоф, говори о телевизији као инструменту који је у стању да произведе реалност реалнију од реалног – симулакрум, односно копију за коју никада није постојао оригинал.

Интернет је довео до револуције у „војним пословима“ омогућивши спровођење офанзивних и дефанзивних информационих операција. Осим тога, Интернет је довео и до револуције у комуникационој сфери, дозволивши сарадњу и интеракцију међу људима, без географских ограничења, и дифузију разних личних „ратних дневника“.

У наставку рада покушаћемо да илуструјемо начин на који се мењала информација, средства њеног преноса, као и њен пропагандни утицај током оружаних конфликата, почевши од Вијетнамског рата до агресије НАТО на СРЈ.

2.2.4.1. Рат у Вијетнаму – први телевизијски рат

Маршал Меклуан, један од највећих стручњака за мас-медије, сматра да је рат у Вијетнаму био први телевизијски рат. У том смислу он пише: „Сви ратови су се увек водили са најновијим технологијама које је свака култура имала на располагању.“[167] Ово запажање важи и за комуникационе технологије. Сви већи ратови XX века фаворизовали су технолошки напредак у пољу медија и обратно, били су условљени променама у начину комуникације.

На почетку Првог светског рата била је углавном заступљена радиотелеграфија јер је радиофонија била још у експерименталној фази. Први

[166] Remondino E.: *La televisione va alla guerra*, Sperling & Kupfer Editori, 2002.
[167] McLuhan M.: *Razumijevanje medija*, Golden Marketing i Tehnička knjiga, Zagreb, 2008.

светски рат је, услед потребе за брзом комуникацијом, наметнуо брзо развијање радиофоније, убрзавши технолошки скок који је водио ка радиодифузији.

Током Другог светског рата телевизија је још увек била примитивна технологија. Ратна дешавања су успорила развој телевизије, да би по окончању сукоба дошло до подстицања истраживања и унапређења на пољу електронике, која је поставила основу за послератни бум телевизије.

Током рата у Вијетнаму (1962-1975) телевизија је променила однос између војних стратегија и средстава информисања. Први пут се на телевизији рат представља у негативном контексту, кроз кратке сегменте ружних и необрађених црно-белих слика у лошој резолуцији. Произведени утисак је тежак и ефектан. Гледалац има утисак да је непосредни сведок рата. Телевизијски приказ рата идеализује сукоб и издиже на пиједастал америчког хероја. Нова технологија омогућава емитовање велике количине информација. Гледалац, примајући значајну количину визуелних и звучних стимуланса, добија потребу за сублимираним тумачењем збивања. Зато му се сервирају репортаже праћене коментарима који поједностављују разумевање. Примењује се наративни модел прича из народне традиције, где се сукобљене стране деле на хероје и антихероје. На почетку, рат је представљан као сукоб са окрутним и фанатичним непријатељем. Стварала се нека врста идентификације са америчким идеалима па су медији постали промотери званичне владине политике. Стога, у овом рату медији нису трпели никакав притисак ни цензуру. Они су били овлашћени да прате војне трупе у Вијетнаму и имали су формалну аутономију у извештавању.[168]

На почетку Вијетнамског рата реч је била о формалној аутономији с обзиром на то да је између мас-медија и политике постојао компромис – новинари су се одрекли исказивања властитог политичког става у замену за слободан приступ попришту рата.

Практично, медији су прихватали стратегију и агенду естаблишмента. Без обзира на то, нису изостајали контрасти између медија и владе, који су временом

[168] Gardner H.: „War and the media paradox“, *Cyber Conflict and Global Politics*, Routledge, Abingdon, 2009. p. 9.

постајали све јачи паралелно са гашењем ентузијазма код дела владе и појавом разних покрета отпора.

Након 1965. године штампа и телевизија извештавају са ратишта, али са прогресивним елементима критике, између осталог и захваљујући бржем преносу слика и филмова – у употребу је уведен млазни авио-транспорт, потом сателити, а након тога и нове мобилне видео-камере. Пред крај 1967. године, телевизијска информација постаје амбивалентна. Почетком године телевизијске мреже су још увек једногласно подржавале владу, све до половине године, када је Џонсонова администрација уочи председничких избора покушала да убеди јавност да се рат успешно приводи крају.

Тет офанзива у јануару 1968. остварила је важан и трајни пробој унутар америчког јавног мњења.[169] Прецизније говорећи, Тет офанзива је отворила унутрашњи рат, који је телевизија снимила, између растуће опозиције и све више пољуљаног естаблишмента, који је покушавао да се одржи захваљујући својој економској моћи. Тек кад су раздвајања и несугласице постали очигледни, телевизија је отворила врата противницима рата. Мишљење публике о сукобу полако се мењало. Чувена фотографија Ника Ута која приказује девојчицу са опекотинама по телу како гола бежи из напалма, имала је снажан одјек у јавности. Али, ова фотографија није објављена случајно, нити је била прва. Она је објављена након серије драматичних слика које су на неки начин припремиле аудиторијум. Другим речима, та фотографија је објављена у право време.

---

[169] Тет офанзива (30. јануар 1968. - 8. јун 1969.) је била серија офанзивних операција током Вијетнамског рата, координисана између Народног Ослободилачког Фронта и војске Северног Вијетнама против војске Јужног Вијетнама и војске САД и других савезника војске Јужног Вијетнама. Операције се називају Тет офанзива пошто су темпиране да почну у ноћ 30./31. јануара 1969, на дан вијетнамске лунарне Нове Године. Офанзива је спектакуларно започела током прослава Нове Године, а спорадичне операције повезане са офанзивом наставиле су се до 1969.

Тет офанзива се може сматрати великим војним поразом за комунистичке снаге, пошто ни Вијет Конг ни војска Северног Вијетнама нису постигле своје тактичке циљеве. Цена офанзиве је била висока, Вијет Конг је био практично обогаљен великим губицима које су му нанеле америчке и јужновијетнамске снаге. Ипак, офанзива се сматра прекретницом рата у Вијетнаму, пошто су Вијет Конг и северновијетнамска војска извојевале огромну психолошку и пропагандну победу. Подршка ангажовању у рату, унутар САД, почела је постепено да опада и нација је постала значајно поларизована због рата. Амерички председник Линдон Џонсон је, видевши како његова популарност нагло опада након офанзиве, повукао своју кандидатуту за изборе марта 1968. Тет офанзива се често наводи као пример вредности пропаганде, утицаја медија и јавног мишљења на извођење војних циљева.

Фотографија 1: Ник Ут*, Напалм,* 1972.

Прећутни пакт између медија и политичке моћи већ је био разрушен, а губљење поверења у институције помогло је еманципацију телевизије. Тек у периоду од 1968 до 1973. телевизија документује и износи на видело окрутну истину рата пред америчку јавност, у првом плану и у боји, проузрокујући разочарање у институције, морални колапс нације и антимилитаризам јавног мњења.

У јуну 1971. Њујорк Тајмс изазива владу да објави истину о рату садржану у тзв. „Pentagon papers“ (тајна документа Министарства одбране), укључујући и преваре током војног напада на Вијетнам. У суштини, амерички медији нису у потпуности укинули подршку естаблишменту, већ нису могли а да не прикажу пољуљавање политичког врха.

Последњих година сукоба медијско покривање се смањује и готово нестаје. Постепено повлачење америчких трупа узроковало је и смањивање заинтересованости читалаца и гледалаца за ову тему, будући да је нација била већ доведена у стање апатије према рату.

2.2.4.2. „Невидљиви ратови“ – од Фолкланда до Првог заливског рата

Осамдесетих година прошлог века директна конфронтација између медија и политике показује јасну жељу да се медијска информација контролише у корист унутрашње политичке комуникације, а у случају рата да се она чак потпуно уклони.

Америчке и енглеске конзервативне владе добро су проучиле Вијетнамску лекцију. Роналд Реган и Маргарет Тачер су закључили да се управљање информацијом мора поново засновати на принципима Првог и Другог светског рата. Они су схватили да не постоји реторичка вештина која је у стању да учини прихватљивим губитак ближњих осим у контексту тоталног сукоба, који доводи у питање опстанак самог друштва. Рат се, дакле, морао представити као тоталан и неизбежан, високо технологизован, без слика деструкције, крви и смрти. Другим речима, он је морао постати „невидљив“.[170]

Фолкландски рат (1982) је први „невидљиви“ рат у телевизијској ери. Британска влада је од самог почетка сукоба заузела став по питању информисања. Директору Асоцијације новинских издавача (Newspapers Publisher's Association – NPA) дато је овлашћење да за кратко време изабере представнике четири национална дневна листа, који би уз пратњу четири камермана били послати на фронт, заједно са војним снагама.

Дописници су, због учешћа у конфликту раме уз раме са војницима, емотивно и идеалистички доживљавали сукобе, у толикој мери да су многи од њих, по завршетку рата, били критични према својим извештајима. Чињеница да није било извештача других националности повећавала је пристрасност у извештавању.

Британски дописници су трпели дуплу цензуру – материјали су били контролисани од стране Министарства одбране пре слања и, поново, по приспећу у Лондон. Након Рата у Фолкланду велике телевизије су се боље опремиле.

У другој половини осамдесетих, телевизија је ушла у своју зрелу фазу. Развојем електронских технологија и дифузијом геостационарних сателита знатно се повећао број репортажа и директних преноса, мењајући и сам новинарски вокабулар. Телевизијски инструментаријум је довео до веће драматизације, што је основа модерног политичког телевизијског новинарства. Телевизијска камера има једну карактеристику коју филмска камера нема – у стању је да од сваког догађаја направи спектакл захваљујући могућности његовог директног преношења.

---

[170] Gardner H.: *op. cit.*, p. 9.

Први рат у Заливу започео је нападом Ирака на Кувајт. Покушај договора између представника САД и ирачког министра спољних послова 9. јануара 1991. у Женеви пропао је. Након шест сати разговора, није нађено прихватљиво решење. Тада је почело да се прича о предстојећем рату и медији су се припремили пре почетка сукоба.

Личност Садама Хусеина је, до тог тренутка, у западној јавности углавном представљана у позитивном светлу. Хусеин је уживао подршку председника Регана и Буша (старијег) као и стратешких корпорација, јер је био добар купац огромних количина оружја.

Сада је, међутим, војна обавештајна служба (DIA) добила задатак да демонизује лидера ирачке нације, за шта су ангажоване и додатне четири агенције за односе са јавношћу. Као резултат ове, прецизно вођене кампање, чак 30 земаља света укључило се у хајку на ирачки народ, под изговором да су извршили агресију на Кувајт.[171]

Један дотад невиђени догађај одиграо се током телевизијске хронике о рату у Заливу – америчко укључење у рат први је објавио дописник телевизијске станице ABC, Гери Шепард, а тек након пола сата и представник за штампу Беле куће.[172] Два сата након тога, председник САД се обратио свету са намером да оправда своју одлуку: „Пре два сата наши авиони започели су напад на војне циљеве у Кувајту и Ираку. Овај напад се наставља док причам, тренутно је у акцији и пешадија. Цела ова прича је почела када је ирачки диктатор напао малог и незаштићеног суседа, Кувајт, члана Арапске Лиге и Уједињених нација, и малтретирао његов народ. Пре пет месеци започео је овај окрутни рат против Кувајта и сад учествујемо у конфликту.“[173]

С друге стране, Садам Хусеин је наставио са политиком вођења дипломатије посредством медија (*media diplomacy*), заснованом на позивању на религиозне и културне вредности арапског народа. Његове поруке су истовремено биле упућене

---

[171] Барбуловић С., et al.: *Амнезија јавности – од пропаганде до тероризма*, Графо-комерц, Београд, 2004, стр. 195.

[172] Према: Savarese R.: *Guerre intelligenti*, Franco Angeli, 1992.

[173] *Ibid*.

ирачком народу, као и народима других арапских земаља, уз позив на свети рат против америчких агресора.

На дан када је почело бомбардовање, ирачки председник се појавио на телевизијским екранима окружен дечацима током молитве. На радију је прочитано његово писмо у којем пише: „Почела је мајка свих борби... Неверници су нас преварили, Буш, ђавољи пријатељ, нас је напао. Криминалци нису успели, Бог је са нама и са верницима, и водиће их у победу… приближава се дан спасења нације, дан када ће пасти престоли издајника засновани на корупцији, када ће бити сломљене жеље сатане из Беле куће и осињака израелских криминалаца… драга Палестина и њени синови ратници биће ослобођени.“[174] На крају говора Хусеин позива Буша да повуче своје трупе.

У овом рату, тријумф телевизије, као средства комуникације и дипломатије, послужио је укључивању новинарске комуникације у политичку комуникацију. Телевизија је преносила поруку засновану на драматизацији. Другим речима, порука је била заснована на режирању догађаја и изградњи ликова као и симбола преводивих у телевизијски ефикасна лица и слике.

Media diplomacy је симболичан конфликт између Буша и Садама каналима масовне комуникације, у којима обе стране смењују претње и обећања како би остварile подршку унутар земље и пред страним јавним мњењем.

Да би избегла опасан утицај новинара на јавно мњење, америчка Војна команда се послужила двама традиционалним инструментима: цензуром и производњом алтернативног тока информација.[175] Дакле, дошло је до повратка на ону контролу информација која је са Вијетнамом готово нестала.

Прва бомбардовања Багдада започела су 16. јануара 1991. Тада су уништени ирачки комуникациони центри. Тих дана ирачки радио се могао чути само у одређеним сатима. Једине вести које су стизале биле су са фронта Саудијске Арабије и, наравно, биле су филтриране од стране Америке. Улога западних дописника је била да оду што ближе граници између Јордана и Ирака и да интервјуишу избеглице

---

[174] *Ibid*.

[175] Чомски Н.: *Контрола медија*, Рубикон, Нови Сад, 2008, стр. 49.

које су пристизале, те да на тај начин учествују у информационој слагалици која је режирана у западним земљама.

Нажалост, заташкани су многи догађаји, што је овај рат учинило најневидљивијим ратом двадесетог века. Не постоји ни једна фотографија великог масакра над ирачким народом у моменту повлачења америчких трупа које су, претпоставља се, том приликом користиле ново оружје – бомбе које сагоревају кисеоник, дакле тела, док предмети остају нетакнути. Хиљаде жртава овог масакра никада није фотографисано нити снимљено јер је новинарима забрањен приступ све док локација није потпуно очишћена.

Пентагон је затражио да се сви чланци подвргну „безбедносној ревизији". Никоме није дозвољено да разговара о логистичким детаљима операције. Ни један новинар није смео да опише ишта везано за војнике, тенкове или кретање било којег возила у току операције. Циљ Пентагона је био да уклони све репортере из ратне зоне. Велики број независних медија био је потпуно искључен из информационог конзорцијума Пентагона. Апсолутна контрола над информацијама је дозволила Пентагону да конструише и пропагира један такорећи безболан, високотехнолошки рат без слика разарања, крви и смрти. Рат у коме су доминирале слике сукоба између „зле" и „добре" стране која увек побеђује.[176]

Једино се CNN успротивила директиви америчке владе, објавивши једине слике разарања и смрти током целог рата – слике бомбардовања бункера у Ал-Хамариаху где је живот изгубило око 300 цивила. То не значи да је CNN заузела антиамерички став већ да је успела да се избори за минималну независност од Пентагона.

И у овом рату манипулација информацијама није била новост. У Америци се ипак подигло много прашине око чланка Њујорк Тајмса под насловом „Сећаш ли се Nayrah?".[177] Nayrah је била петнаестогодишња девојчица из Кувајта која је сведочила пред америчким посланицима да је видела ирачке војнике како у болници извлаче новорођенчад из инкубатора и бацају их на земљу. Њено сведочење је обишло цео

[176] Барбуловић С., et al., *op. cit*., стр. 196.

[177] Према: Sciolino E.: „Following Attacks, Spain's Governing Party Is Beaten", *The New York Times*, March 15, 2004.

свет и постало синоним за бруталност Садама Хусеина. Ипак, испоставило се да је сведочење било лажно. Намерно организована превара од стране кувајтске амбасаде и агенције за маркетинг Hill & Knowlton. Nayrah је била ћерка кувајтског амбасадора у Америци и у време измишљеног догађаја налазила се у Вашингтону.

Контрола информација у западним земљама већином је резултат политичких договора, пре него обичне ауторитативне цензуре. 13. фебруара 1991. савезничка авијација је уништила склониште за цивиле у центру Багдада. Сутрадан ујутро BBC шаље у етар телефонски позив њиховог репортера који их обавештава да је склониште било пуно цивила. Одмах након тога Одељење за односе са јавношћу захтева од BBC-ја да одвоји телефонски извештај од снимака разрушеног Багдада.

Експерти на пољу медија и комуникација сматрају да је током Првог рата у Заливу оријентација западне штампе пројектовала позицију целокупне коалиције приморане да прати САД. На почетку Другог заливског рата, одређени европски новинари успротивили су се конфликту са много више јачине и изразили неслагање са тим да се сви подреде политичкој вољи Америке.

Како би разбили монопол над контролом информација, појединци, организације, земље у развоју, као и развијене земље, покушавали су да развију своје алтернативне информативне сервисе и медије, као и могућности сателитског извиђања. Европски *Ariane* ракетни програм био је развијен, барем делимично, како би се лансирали европски сателити који би били алтернатива америчкој контроли над сателитским снимцима током првог Заливског рата.[178]

2.2.4.3. Место и улога информационо-комуникационе технологије у Другом заливском рату

Савремена историја придаје посебан значај терористичком нападу на САД 11. септембра 2001. Овај напад многи теоретичари узимају као прекретницу и са политичке и са војне тачке гледишта. Највећа светска сила је са падом Кула

[178] Занимљив је податак да први лет у свемир *Ariane 5* 1996. није успео због рачунарске грешке која је довела до квара у његовом контролном софтверу. Поред Европљана, Кина, Индија, и Јапан такође су развили своје ракетне и сателитске програме, како би проширили своју националну контролу над информацијама. Осим њих, развојем сателитских и лансирних програма баве се и Украјина, Израел, Јужна Кореја, Бразил, Иран, Малезија, Пакистан, Турска и Тајван. Према: Gardner H., *op. cit*., p. 8.

близнакиња претрпела најјачи ударац у својој историји. Америчка реакција на нападе, међутим, заснивала се на политичко-стратешком плану, сачињеном да успостави другачије односе према азијским државама и Европи. У новој геополитичкој констелацији, САД поново успевају да услове европске силе да уђу са њима у рат у Авганистану. Али, када су САД, у оквиру ове стратегије, напале Ирак са оправдањем неутрализације оружја за масовно уништавање, већ постојеће разлике између европских сила избиле су још више на површину. Неколико земаља старог континента не само да се дистанцирало од САД већ се са одлучношћу успротивило оружаној интервенцији Џорџа Буша, сматрајући је нелегитимном с обзиром на то да није под покрићем УН. Тада је настао раскол између европских држава. Са једне стране биле су земље које су подржавале француско-немачки став, док су Енглеска, Шпанија и Италија биле на страни САД. Русија је дала подршку Француској и Немачкој док се Индија и Кина нису изјашњавале. Наравно, ове поделе одразиле су се и на начин извештавања мас-медија о овом рату.

Презентација рата коју су припремили амерички медији била је пречишћена верзија конфликта. Кадрови које су телевизије преносиле углавном су били снимани са висине или из даљине – ватрено небо над Багдадом или раван пејзаж пустиње дуж којег се крећу обриси тенкова и блиндираних возила, више налик на видео-игру него на рат.

Амерички ратни извештачи, нови протагонисти ратног новинарства, заштићени и потпомогнути војском, постали су једно од најјачих америчких оружја за добијање наклоности домаћег јавног мњења.

У овом другом америчком рату на Блиском истоку забележен је тријумф патриотског новинарства, који је започела телевизија Фокс Њуз (*Fox News*), отварањем новог сателитског канала Ол Њуз (*All News*). Према подацима института Нилсен (*Nielsen*), највећи профитер у смислу гледаности била је управо Фокс Њуз, која је од интегралистичког патриотизма и безусловне подршке другом ирачком конфликту направила своју марку, промовишући агресиван и сензационалистички стил, који је свакако имао јак утицај на јавност.[179]

[179] Према: Nielsenwire, http://blog.nielsen.com/nielsenwire/category/media_entertainment/

Нови канал информисања, путем кабла, био је само врх леденог брега Њуз Корпорејшн (*News Corporation*), гигантске издавачке империје којом председава Руперт Мардок. Програм ове корпорације, захваљујући куповини сателитског канала Дајрект ТВ(*Direct TV*), може да прати 120 милиона претплатника у 52 земље.[180]

Ипак, без обзира на безусловну подршку медијске гарде Мардока и већине великих америчких информативних мрежа, међународно јавно мњење је остало прилично скептично у вези са неопходношћу војне интервенције. И унутар америчке силе било је значајних иступања против рата: Мајами Хералд (*Miami Herald*) је писао о томе како амерички медији причају о „трупама коалиције" или о „трупама које предводе САД", док је већина иностране штампе писала о „рату Америке" или „рату Царства". Мајами Хералд између осталог пише и како су у иностранству убеђени да се Буш упустио у неоимперијалистичку ратну кампању како би се домогао блискоисточне нафте. Америчке дневне новине *Alternet* су прикупиле десет најцензурисанијих вести године: међу њима, најважнија је свакако тајни амерички план за доминацију планетом назван „Pnac".[181] Према овом пројекту, рат у Ираку и Авганистану испланиран је много пре терористичких напада на САД 2001. године.[182]

Још један скандал је пратио рат у Ираку – Бушова администрација је елиминисала 8.000 од 11.800 страница извештаја који је ирачка влада предала Савету безбедности УН и Међународној Агенцији за Атомску Енергију (AIEA). На тим страницама су били детаљи о томе како су САД снабделе Ирак хемијским и бактериолошким оружјем и основним компонентама за оружје за масовно уништење. Ова документа не само да би дискредитовале Реганову и Бушову администрацију, Министарство енергије и пољопривреде САД, већ и поједине америчке привредне гиганте.

Њујоркер (*The New Yorker*) је водио исцрпно истраживање на ову тему и открио како је Пентагон створио тајну службу задужену за прикупљање

---

[180] Херман Е., Мекчесни Р.: *Глобални медији – нови мисионари корпоративног капитализма*, Клио, Београд, 2004, стр. 60.

[181] Према: *The Sunday Herald*, 15 September 2002; Harper's Magazine, October 2002; Mothers Jones, March 2003, Pilger.com, December 12, 2002.

[182] *Project for the New American Century*, http://www.newamericancentury.org/

информација о Ирачком оружју и о односима Садама са терористима, у циљу оправдавања рата.

У једном другом чланку, поменути лист покушава да открије зашто су Вашингтон и Лондон ширили лажне информације о тајној трговини уранијумом између Ирака и Нигера. Док се 24. септембра 2002. Конгрес спремао да изгласа резолуцију која је требало да овласти председника Буша да нападне Ирак, једна група високих функционера тајне службе, међу којима и директор CIA-е Џорџ Тенет, пронашли су одређену количину високоотпорних алуминијумских цеви које су путовале ка Ираку. Цеви су, наводно, могле да послуже за изградњу центрифуга за производњу обогаћеног уранијума. Ово откриће послужило је као оправдање за претпоставку да Ирак спроводи нуклеарни програм.

Осим сведочења Тенета, и влада Тонија Блера и Гардијан (*The Guardian*) су допринели учвршћивању ове претпоставке. И као да то није било довољно, државни секретар Колин Пауел, износи у јавност причу о покушају Ирака да купи уранијум од Нигера. Све је то допринело да се председнику да овлашћење да започне војни напад на Ирак. Након тога, 7. марта 2003. директор Међународне агенције за атомску енергију (AIEA), Мохамед ел Барадеј, изјавио је пред Саветом безбедности Уједињених нација да су документи у вези са продајом уранијума Ираку лажни. И још један изасланик AIEA тврдио је: „Ови документи су толико лоше фалсификовани да је непојмљиво да су стигли из једне озбиљне тајне службе. На нивоу на коме се дискутовало о документима, очекивао сам мало бољу контролу.”[183]

Чак је и *Њујорк Тајмс* заузимао критичку позицију према администрацији. Многа европска штампа такође је критиковала Бушов учинак. У интервјуу са Полом Вирилиом, познатим теоричарем брзине и специјалисте за нове технологије, Монд (*Le Monde*) цитира: „Претходни конфликти били су другачије природе због једноставне чињенице да телевизије нису имале могућност директног преноса, у данашњој брзини и конфузији слика налази се прави проблем.“ О одбијању да се прикажу ужаси рата, он каже: „Задржавање анонимности жртава је театрално, то је један начин глуме, нова врста псеудохуманитарне камуфлаже… присуствујемо рату лажи, изгубљене перцепције истинитог и лажног. Блеф је светских размера и у

[183] *The New Yorker*, March 27, 2003.

директном преносу". На питање како препознати кључне тачке, одговара: „по мом мишљењу све ће се одиграти, односно све се одиграва на штампаном папиру. Враћа се снага текста. Мора се читати. Једини позитиван пример америчке стране је *Њујорк Тајмс,* који је заузео антиратну позицију. На неки начин, спасао је част америчке штампе."[184]

И енглески *Гардијан* је критичан према начину на који се шире информације износећи тезу да су границе између чињеница и пропаганде све мање дефинисане. Глад за информацијама у директном преносу претвара се у тренутан пренос војних изјава широм целог света. Вести стижу без провере и потврде.[185]

Италијанска штампа се поделила као што су се поделиле и политичке силе њене земље. Коријере дела сера (*Corriere della Sera*), који је у првом рату у заливу подржао западну коалицију, први пут се јасно супротставља рату 9. фебруара 2003.[186]

Ирачки лист *Ath Thawra*, у чланку под насловом „Морамо да се одбранимо!"[187], апелује на све земље да изврше притисак како би се омогућило повлачење агресора из Ирака, позивајући и на свету одбрану арапа и муслимана. *Al Dustur,* Јорданске новине, пишу: „Није више психолошки рат, нити скуп једноставних грешака, у овом случају ради се о организованој лажи... о глобалном систему доминирања народима. Оно што нам западни медији приказују нису анализе ситуације већ сценске поставке вредне Холивуда."[188]

Међу различитим изворима информација, апсолутну новост представљао је Интернет. Он није обична рачунарска мрежа већ планетарни дифузор информација и, у исто време, начин за стварање сарадње и интеракције између индивидуа без географских ограничења.

Током првог рата у Заливу, Интернет је био још слабо развијен. Деценију касније, он је одиграо врло важну улогу. Огромни пораст посета сајтовима главних

---

[184] *Le Monde*, April 4, 2003.
[185] *The Guardian*, April 4, 2003.
[186] Према: www.caffeeuropa.it.
[187] Gardner H., *op. cit*., p. 9.
[188] *Ibid*.

информационих агенција региструје се од 20. марта 2003, првог дана англо-америчког рата у Ираку. У то време феномен блога долази у први план.[189]

Познат је случај младића из Багдада који је у свом онлајн дневнику описао рат у Ираку. Под псеудонимом „Salam Pax“, 29-годишњи дипломирани архитекта из Багдада, комуницирао је путем блога са својим другом Раедом у Јордану. Салам је на блогу објављивао своје белешке како би Раед могао да их прочита. Током прва два месеца, у свом дневнику под називом „*Where is Raed?*“ писао је само вести о свом животу да би, затим, сусревши се са осталим блогерима почео да описује потешкоће живота под Садамовим режимом, знајући ризике којима се излаже. Писао је о страшној инфлацији, о доласку паравојске странке Baath, која је на зграђавање комшија постављала артиљеријску станицу у једној напуштеној згради у његовој улици. Временом, новине у Великој Британији и Америци, почеле су да објављују чланке који су писали о његовом блогу. У то време, већ 20.000 људи је свакодневно читало Саламове белешке. Десетак дана након ових дешавања, Ирак је потпуно укинуо приступ Интернету.[190] Иако није могао јавно да објављује своје текстове, Салам је наставио да води дневник у свом рачунару следећих осам месеци, описујући бомбардовање Багдада. Касније је успео да их мејлом пошаље Дијани Мун, блогерки из Њујорка, која их је објавила.

---

[189] Блог или веблог (скраћено блог, од *енгл*. web log, blog) чини низ хронолошки организованих уноса текстова, који се приказују на веб-страницама.

Типови уноса могу варирати не само по својој теми и обиму већ и по формату. Тако постоји велики број блогова чији су уноси у текстуалном формату (попут вести, белешке, расправе). Такође, постоји велики број блогова који садрже фотографије, скице или неке друге графичке форме, адресе ка неком занимљивом садржају на Интернету итд.

Велики део блогова омогућава својим посетиоцима да оставе коментаре на постојеће садржаје, на тај начин стварајући мале заједнице које дискутују на теме којима се блог бави. Због тога су се блогови временом развили у широко распрострањен начин комуникације на Интернету, између аутора (или групе аутора) и посетилаца блога. Блог омогућава комуникацију на лакши начин него на форумима или путем е-поште. Он омогућава да свако на једноставан начин искаже своје мишљење на Интернету, без посебних техничких знања.

[190] Током рата у Ираку, средства која су имала утицаја на формирање јавног мњења, поред традиционалних медија, била су: Интернет, мобилни телефони и дигиталне камере. Рестрикција Интернета није непозната метода. Њој су прибегавале владе многих држава током кризних ситуација. У Кини су, на пример, мало пре гушења демонстрација на Тијенанмену јуна 1989, радио апарати омогућавали да се чују гледишта опозиције. Након гушења демонстрација на Тијенанмену, кинеске власти развиле су најосетљивији систем за филтрирање садржаја на Интернету на свету, чак и у поређењу са онима које имају Иран, Саудијска арабија, Вијетнам и Бурма. Према: Berkman Center for Internet & Society, *Replacement of Google with Alternative Search Systems in China Documentation and Screen Shots*, Harvard Law School, September 2002

На адреси http://dear_raed.blogspot.com сакупљени су многобројни Саламови чланци. Један од њих уверљиво описује окрутност рата: „Пре пола сата, запаљени су ровови напуњени нафтом. Фотографисао сам све са најближег могућег места... Данас је трећи дан рата, имали смо доста напада током дана. Неке без сирена упозорења. Можда су само одустали од ажурности. Синоћ, нису стизали ни да пусте сирену за прекид опасности између два напада. Данас су мој отац и брат изашли да виде шта се дешава у граду, кажу да су напади изгледа били врло прецизни, али да када експлодирају бомбе праве хаос и изазивају панику у крају где падну. Кућама у близини зграде Al Salam (где је министар Sahaf водио новинаре) су поломљени сви прозори, изваљена су врата а на једној је пао кров. Претпостављам да је то оно што називају колатералном штетом".[191] Девет дана након тријумфалног обарања статуе Садама, уместо бацања цвећа америчким војницима, хиљаде људи изашло је на улице Багдада да протестује против америчке окупације.

Истовремено, арапска сателитска телевизија Ал Џазира (*Al Jazeera*) преносила је сирове и бруталне слике које су у драстичном контрасту са умирујућом визијом рата коју су нудили западни медији. Посматрајући снимке арапских сателитских телевизија, гледалац је имао осећај да присуствује неком другом рату, знатно другачијем од оног хиперпатриотског који је на таласима америчких медија.

Арапске репортаже приказивале су свакодневно насиље над ненаоружаним цивилима, док су на каналима телевизије CNN и осталих западних телевизија непрестано пуштани снимци обарања статуе Садама Хусеина.

Телевизија Ал Џазира је, у том периоду, постигла невероватан успех. Ова телевизија, која је покушала да се супротстави америчкој контроли над информацијама током ратова у Авганистану и Ираку, доспела је до ширег аудиторијума као компанија коју субвенционише држава, емитујући програм и на арапском и на енглеском језику. У медијском контексту који се традиционално карактерише сервилношћу и конформизмом као што је блискоисточни, нова сателитска телевизија, активна 24 часа, постала је светски позната јер је без предрасуда пуштала поруке Осаме Бин Ладена након трагичних атентата из

[191] Према: www.http//dear_raed.blogspot.com, (Saturday, 22 March, 16.30).

септембра 2001. Ова станица, основана 1996. године, данас има око 45 милиона претплатника широм света.[192]

Неколико дана након англо-америчког напада, *Google* и *Lycos*, највећи Интернет претраживачи, регистровали су да је „Ал Џазира“ био најтраженији термин. Захтев за претрагом овог термина био је три пута чешће уношен него реч „секс“.[193]

2.2.4.4. Информационе операције Војске Југославије током агресије НАТО на СР Југославију

Ваздушне и поморске снаге Северноатланске алијансе започеле су 24. марта 1999. године агресију против Савезне Републике Југославије. Интензивна ваздушна кампања, највећа офанзивна операција у историји НАТО, требало је да примора југословенску владу да прихвати услове споразума предложеног у Рамбујеу. Споразум је предвиђао повлачење српских војних и полицијских снага са Косова и Метохије и распоређивање међународних мировних снага у ратом разореној Покрајини. После 78 дана константних ваздушних операција и интезивног дипломатског притиска, влада СР Југославије је пристала на услове сличне онима из Рамбујеа, и изгледало је да је Алијанса, под вођством САД, постигла победу, превасходно захваљујући ваздушним ударима.

Паралелно са ваздушним нападима водио се други, суптилнији рат. Неспособна да војно одговори на ваздушне нападе, СР Југославија се окренула асиметричним средствима како би се супротставила Алијанси. Током агресије, Србија је активно користила властите медије, стране новинаре и утицај Интернета да широм света утиче на јавно мњење како би постигла свој политички циљ – очување државног суверенитета и територијалног интегритета.

Недуго по окончању агресије, експерти НАТО су објавили детаљна истраживања о информационом аспекту овог конфликта. Они су сагласни у ставу да

---

[192] Gardner H.: *op. cit*., p. 8.

[193] “*Al Jazeera* Tops Net Search Requests”, *Associated Press*, Aprile 11, 2003.

је Војска Југославије победила у информационом рату, будући да је успела да оствари информациону супериорност током конфликта.[194]

На први поглед, можда је тешко сагледати манипулацију медијима и експлоатацију Интернета као кохерентну кампању информационих операција Војске Југославије. Џулијану Менјону, новинару британске редакције ITN, који је пратио рат из Београда, чинио се смешан НАТО приказ „београдске застрашујуће пропагандне машине".[195] Заиста, напори југословенске владе да обликује домаће и међународно јавно мњење изгледали су примитивни у поређењу са могућностима савремених информационих операција заснованих на кибер оружју и нападима на рачунарске мреже. Па ипак, ови напори су били делотворни. Информационе операције Војске Југославије нису превасходно биле усмерене на компјутерско и електронско ратовање. Оне су се базирале на свеобухватној стратегији која је обједињавала употребу информационих инструмената заједно са традиционалним војним борбеним активностима.

Када су преговори у Рамбујеу пропали почетком 1999. год. постало је јасно да је рат са НАТО-ом неизбежан. Југословенски естаблишмент није губио време у покретању кампање информационих операција. Први циљ кампање био је спречавање поделе државе, тј. стварања аутономне републике Косово. Други циљ је био консолидација српске власти на Косову што је захтевало слом паравојне организације, тзв. Ослободилачке војске Косова. У намери да реализује ове задатке, естаблишмент СР Југославије морао је да постигне три оперативна циља: 1) Одржавање домаће подршке акцијама безбедносних снага на Косову и Метохији и пркоса НАТО нападима; 2) Стварање несагласности између чланица НАТО и утицање на њихову одлучност за вођење рата; 3) Задобијање подршке јавности у иностранству – укључујући НАТО земље и Русију. Да би испунила ове циљеве, Војска Југославије је применила офанзивне и дефанзивне информационе операције.

Дефанзивне информационе операције. У циљу постизања „сигурности информација", југословенски естаблишмент је прибегао стратегији цензурисања

---

[194] Larsen A. W.: *Serbian Information Operations During Operation Allied Force*, Air Command and Staff College, Air University, Maxwell Air Force Base, Alabama, 2000.

[195] Peter, et al.: *The Kosovo News and Propaganda War*, International Press Institute, Vienna, 2000, http://www.freemedia.at/ KosovoB_Manyon.htm.

медија и вођења контрапропаганде. Примењујући Закон о јавном информисању, усвојен непосредно пред бомбардовање, влада је угушила неколицину независних медија који су деловали у Србији.[196]

Поред „сламања“ домаћих новинара, влада Србије се трудила да својим грађанима онемогући приступ информацијама из спољних извора. На самом почетку рата власти су прекинуле емитовање програма западних телевизијских станица. Будући да није могао да спречи пријем ових програма преко сателита и Интернета, режим је покренуо жестоку контрапропагандну кампању како би дискредитовао њихов кредибилитет. Стране агенције, као што су BBC, CNN, Скај Њуз (Sky News) и други, представљани су као „агресорско оруђе“ и заговорници идеологије ОВК.

Постизање „сигурности информација“ омогућило је режиму да изврши следећу фазу дефанзивне кампање информационих операција – спровођење контра-пропаганде која је имала за циљ демонизацију НАТО уз истовремено задобијање јавног мњења за наставак подршке отпору Алијанси. Распламсавање осећања националног идентитета и националистичког расположења постизано је стварањем слике о Србији као вечитој жртви. Сукоб на Косову представљан је као битка за национални опстанак. У првим данима НАТО бомбардовања, државна телевизија је почела са емитовањем филмова из периода НОБ-а. Након емитовања оваквих садржаја, Слободан Милошевић се обратио јавности, тврдећи да је прави циљ агресора окупација целе државе. Наредне емисије су представљале Косово као колевку српског народа. Ове слике су додатно учврстиле подршку становништва режиму. Током рата, домаћи медији су пажљиво контролисали ток информација до локалног становништва. Медији су извештавали о цивилним жртвама док војни губици нису спомињани. Уместо тога, константно су извештавали о губицима НАТО авијације.

Офанзивне информационе операције. Пошто је постигао информациону супериорност на домаћем терену, режим СР Југославије је фокусирао информационе

[196] Полиција је 28. марта затворила радио станицу Б92. Ни новински листови нису боље прошли. Издавачи пет независних новина били су ухапшени, а они који су остали на слободи нису смели да штампају издања без претходне сагласности владиних цензора. Поред тога, Министарство информисања је издало директиву којом се од свих новинара захтевало да о НАТО-у извештавају у негативном контексту. Према: Erlanger S.: “Televised Defiance Lost Amid Sirens, Blasts, and Fireballs”, *New York Times*, March 25, 1999, p. A12.

инструменте на међународну публику. Користећи тактику сличну дефанзивној стратегији, режим је користио контролу медија и пропагандне технике како би спровео психолошке операције усмерене на међународно јавно мњење са циљем ускраћивања подршке Алијанси.

Југословенске безбедносне службе биле су ангажоване на контроли иностраних новинара који су из Београда извештавали о рату. Полиција је предузела акцију хапшења неколицине телевизијских и новинских репортера под оптужбом за шпијунажу.[197]

Југословенска влада је такође распарчала корпус стране штампе да би њоме лакше управљала: до краја друге недеље рата, више од 20 новинара је било приморано да напусти земљу у року од 24 часа, због тога што је њихово извештавање сматрано пристрасним. Другим репортерима, око стотину њих, одбијено је продужење визе, дакле они су протерани на „љубазан“ начин.[198]

Новинарима који су остали наметнута су ограничења на оне слике и извештаје који могу да се емитују из Београда. У почетку, као у „Пустињској олуји“, новинари су емитовали слике ваздушних удара НАТО авијације са кровова својих хотела. Међутим, службе безбедности су убрзо притвориле више од 40 новинара и конфисковале њихову опрему. Након овог догађаја, власти су забраниле употребу мобилних емисионих предајника и приморале стране извештаче да користе технику РТС-а, где су њихове траке и извештаји били пажљиво надзирани од стране Војске Југославије. Репортери су такође били приморани да се региструју у владином прес-центру и нису могли да напусте Београд без пратње.[199]

Као резултат медијске контроле, западни новинари су постали оружје офанзивних информационих операција Војске Југославије. Њима је било дозвољено да виде само губитке НАТО-а. Локације на којима им је био дозвољен приступ су

---

[197] Hanspeter Schnitzler, извештач немачке телевизије SAT1, наводно је био ухапшен, претучен и држан у самици 26 дана. Репортери који нису ухапшени били су предмет честих узнемиравања. Детаље о овом случају и искуствима ратних извештача током НАТО бомбардовања могуће је прочитати на: Schniztler H.: *A Never Ending Story in Cell 13*, http://www.freemedia.at/ KosovoB_Schnitzler.htm.

[198] Manyon J.: *The Kosovo News and Propaganda War*, http://www.freemedia.at/KosovoB_Manyon.htm

[199] Erlanger S.: “Support for Homeland up as Sirens Wail and News is Censored”, *New York Times*, March 29, 1999, p. A1.

пажљиво одабране за постизање максималног ефекта пропаганде – на пример, место пада авиона Ф-117.[200] Снимке оборених авиона, као и друге губитке југословенске војске, није било дозвољено прикупљати. Уместо тога, новинари су били одвођени на места где је НАТО учинио тзв. колатералну штету, одакле су слали у свет слике српских цивилних жртава.[201]

Југословенски режим је, такође, користио иностране новинаре за преношење властитог гледишта спољном аудиторијуму. Режим је знао да су код западних медија интервјуи уживо боље прихваћени од монтираних изјава, те се радило на томе да појединци буду интервјуисани од стране заробљеног корпуса штампе.[202] Појединци, попут вође паравојних снага Аркана, и југословенског амбасадора у УН, свакодневно су се појављивали на највећим америчким каналима, као што су BBC, MSNBC, Фокс Њуз (Fox News), и Скај.

Поред манипулације страном штампом, режим је користио сопствене медијске изворе да иностраном аудиторијуму презентује југословенску перспективу у односу на рат. Преко закупљеног комуникационог линка EUSat, РТС је био у стању да медијски покрије целу Европу и да програм државне телевизије буде реемитован у САД на CSPAN.[203] Користећи овај форум, режим је настојао да поткопа морални и правни ауторитет НАТО путем пажљиво одабраних порука. Прво, Радио Телевизија Србије је, у више наврата, оспорила тврдње званичника НАТО о „прецизним ударима“ извештавајући о „варварским и криминалним“ нападима на цивилну индустрију, о ускраћивању основних услуга неопходних за живот народа уз визуелни приказ смрти и оскудице. Друго, српски коментатори су у информативним емисијама, у више наврата, дискредитовали наводну легалност НАТО акција, подсећајући међународну публику да Србија само спроводи своје право на сузбијање тероризма и спречавање сецесије у оквиру своје суверене територије. Дакле, коментатори су тврдили да је Алијанса, нападајући Југославију,

---

[200] *Ibid*.

[201] Erlanger S.: “Small Serbian Town Is Striken By a Deadly Accident of War”, *New York Times*, April 7, 1999, pp. A1, 10.

[202] Manyon J., *op. cit*.

[203] Ramirez A.: “Heroes vs. Intruders and Terrorists”, *New York Time*s, March 29, 1999, p. A12.

починила агресију која је у супротности са властитим оснивачким принципима, будући да је основана као одбрамбени савез.[204]

Србија је такође користила пропагандно оружје да дискредитује основни разлог ангажовања НАТО – наводно етничко чишћење на Косову и Метохији. Контролишући медије и њихове емисије, режим је негирао намеру НАТО стратега да оправдање за напад аргументују злочинима унутар територије коју контролишу Срби. Ово је омогућило српским медијима да пласирају контраоптужбе – огромне колоне избеглица које су бежале са Косова представљене су као бег од „хуманитарног бомбардовања". Поред тога, јавни сервис је емитовао слике југословенских трупа како помажу расељеним Албанцима и Милошевићев пријатељски разговор са Ибрахимом Руговом. Кредибилитет Алијансе је додатно нарушен изједначавањем НАТО са ОВК, указивањем на подршку коју је терористичка организација ОВК добијала од САД. У том смислу, српски медији су неколико пута пуштали архивске снимке западних дипломата и експерата из Немачке, Француске и Швајцарске који су повезивали ОВК са међународним организованим криминалом и европским тржиштем кокаина и хероина, као и осуде ОВК од стране представника за односе са јавношћу америчког Стејт Дипартмента, Џејмса Џолија, који је једном приликом изјавио да је „присуство српских трупа на Косову било легално и легитимно".[205]

Други аспект кампање информационих операција усмерених на дискредитовање НАТО била је експлоатација инцидената „колатералне штете". Користећи контролу над западном штампом, слике цивилних жртава су биле приказиване међународној публици истовремено са ваздушним ударима. Те слике, уз изјаве очевидаца, распрострањене преко западних и српских медија, пратиле су тврдње режима да су напади на цивиле били намерни. Те слике су побуђивале просрпске и антиратне активисте широм Европе и Русије, што је довело до протеста и демонстрација против САД и НАТО. Ово јавно незадовољство резултовало је

---

[204] Larsen A. W., *op. cit*., p. 16.

[205] Према: Karadjis M.: *Chossudosky's Frame-up of the KLA*, http://jinx.sistm.unsw.edu.au/~greenlft/1999/360/360p21/htm; Craig L.: *The Kosovo Liberation Army: Does Clinton Policy Support Group with Terror, Drug Ties?*, US Senate Republican Committee Report, March 31, 1999, www.fas.org/irp/world/para/docs/fr033199.htm

политизацијом и продужењем процеса избора циљева унутар Алијансе, а у неким случајевима и до уклањања читавих категорија цивилних мета са листе предвиђених мета.[206]

Страх од „колатералне штете“, пласиран југословенском пропагандом довео је и до ограничења употребе појединог оружја из арсенала НАТО.[207]

Активност Војске Југославије на ширењу пропаганде била је потпомогнута западним телевизијама и новинским агенцијама, које су користиле српске медије као извор у својим извештајима. Југословенска пропаганда је стопљена у извештаје веома либералних и конзервативних медијских форума критичних према НАТО-у. У настојању да дође до ширег аудиторијума, естаблишмент се окренуо новом медијуму за своје офанзивне операције – Интернету.

Током прве две недеље рата, на Интернету се појавило десет прорежимски оријентисаних сајтова на енглеском језику. Док су неки од ових сајтова били у приватном власништву, већину су водили Савезно министарство за информисање, Војска Југославије и Београдски универзитет. Поред тога, безбедносне службе су у потаји присвојиле веб адресу Б92, који је од 1997. био познат као „извор независног извештавања у Југославији“. Због тога ни путем Интернета није било могуће добити објективну информацију о сукобу већ само тенденциозну, пристрасну слику.

Министарство информисања је предузело мере којима је задобило контролу и над садржајем веб сајтова. Министар информација Никола Марковић је издао серију „сугестија“ администраторима сајтова. Конкретно, он је апеловао на кориснике Интернета да „поштују Интернет етику слањем кратких порука, без увредљивих речи. Поруке морају да се пошаљу циљаним групама са што је могуће више слика почињених злочина, додајући да су странци највише заинтересовани за аматерске видео снимке, јер они представљају аутентични снимак са терена. Истина

---

[206] Priest D.: “Bombing by Committee”, *Washington Post*, September 20, 1999, p.A1.

[207] На пример, 8. маја 1999. отказала је касетна бомба бачена са намером да погоди аеродром, и, уместо аеродрома, оштетила је болницу и пијацу. НАТО се поново суочио са сликама убијених цивила и извештајима о невиним жртвама. Негодовање због овог инцидента довело је до забране употребе касетне муниције до краја рата, која је била иницирана са председничког нивоа. Извор: Конференција за штампу НАТО, http://www.nato.int/kosovo/ pres /p990508b.htm

мора да дође до утицајних људи, политичара и пословних људи. Зато морају поруке бити послате преко имејла.“[208]

Будући да је НАТО успео постепено да прекине српске радио и телевизијске комуникације са иностранством, Интернет сајтови су постали примарни инструменти режимске пропаганде. Ови сајтови су понављали исте поруке достављене домаћој телевизијској публици – акција НАТО-а је била нелегална и неморална; НАТО агресори су намерно и неправедно циљали југословенске цивиле; српске безбедносне мере на Косову су једино одвраћале албанске терористе, а креатори политике НАТО-а били су разједињени и „погубљени“.

Ови сајтови су такође садржали дечје цртеже са приказом живота под НАТО бомбама и видео снимке разорених градова са звуком сирене за ваздушни напад. Осим тога, администратори су на сајтове постављали чланке и уводнике угледних западних новинара, интелектуалаца и политичара који су критиковали бомбардовање. Српски лидери су такође користили „кибер етар“, појављујући се у онлајн „чет румовима“ и одговарајући на имејлове. У неким случајевима, овај медиј је обезбедио нападнутој страни да оствари већи утицај на светску јавност од телевизијских интервјуа.[209]

Државне службе и појединци у Србији користили су имејл да обавесте иностране медије и светску јавност о случајевима тзв. колатералне штете. На пример, у року од 15 минута од бомбардовања кинеске амбасаде, Стратфорд, приватна обавештајна компанија, примила је пет имејлова са описом напада од људи који живе у близини амабасаде.[210]

Имејл је такође постао саставни део мреже раног упозорења. У моменту узлетања НАТО авијације из Авијана и са других локација, сарадници југословенске војске стационирани у околини ваздушних база имејлом би слали податке о врсти авиона, њиховом броју, количини наоружања и репној нумерацији авиона. Ове

---

[208] Larsen A. W., *op. cit*., p. 18, према: “Tanjug Notes New Internet Sites Against NATO Strikes”, Belgrade Tanjug News Service, 1439 GMT, 13 April 1999, FBIS, Document ID FTS19940413001460.

[209] Harmon A.: “War Waged on Web: Killers Without Context”, *New York Times*, 5 April 1999, p. 8.

[210] Интервју Џорџа Фридмана, званичника агенције Стратфорд, у емисији „Добро јутро, Америко“, 15. јун 1999, http://www.stratfor.com/media/ television/990615.asp

информације обезбедиле су благовремена упозорења југословенској противваздушној одбрани.[211]

Поред коришћења Интернета за односе са јавношћу и у пропагандне сврхе, грађани Србије су га такође користили и за вођење информационих напада против НАТО држава. У првој недељи бомбардовања је, у једном дану, послато више од 2.000 имејлова инфицираних вирусом на адресе НАТО.[212] Веб странице Алијансе су такође претрпеле кибер нападе током друге недеље рата. Тада су домаћи хактивисти[213] успели да привремено онеспособе сајт бомбардујући га ping нападима.[214] Напади су приморали НАТО да обезбеди материјалне и људске ресурсе за побољшање безбедности рачунарских система. Осим тога, ови напади су утицали на Министарство одбране САД да донесе уредбу о забрани приступа српским сајтовима како би се спречило тзв. „мапирање“ то јест идентификација америчких официјелних сајтова.[215]

2.3. Утицај нових технологија на савремено ратовање

Перманентно коришћење савремених технологија и најмодерније ратне технике карактерише све међудржавне ратове у којима су ангажоване оружане снаге најразвијенијих држава света. Оне у највећој мери располажу најмодернијим оружјем и другом ратном техником. Најсавременија оружја и друга ратна техника, заснована превасходно на информационо-комуникационим технологијама, употребљавани су у рату у Заливу, у НАТО-југословенском и у рату у Авганистану (2001. године). До изражаја су дошла оружја најновије технолошке генерације у којима преовлађује електронска компонента за откривање, идентификацију, праћење и погађање циља.

---

[211] Wall R.: “USAF Expands Infowar Arsenal”, *Aviation Week and Space Technology*, November 15, 1999, Vol. 151, Issue 20, New York, p.102.

[212] Hubbard Z.: “Information Warfare in Kosovo”, *Journal of Electronic Defense*, November 1999, Vol. 22, No. 11, p.11.

[213] О појму „хактивизма“ биће више речи у одељку 4.3.2. Хактивизам.

[214] Ping напад (или жаргонски „пинговање“) састоји се од излагања сервера великом броју упита у кратком временском периоду. Будући да је систем „преплављен“ са више упита него што његови капацитети предвиђају, долази до „загушења“ сервера те његовог „испада“ из мреже.

[215] Harmon A.: “Serbs’ Revenge: NATO Web Site Zapped”, *New York Times*, April 1, 1999, p. A14.

Оружане снаге западних сила, предвођене САД-ом, користиле су у поменутим сукобима најсавременија, „софистицирана“ оружја. Међу таква оружја могу се убројати: крстареће ракете, беспилотне летилице, ракетна зрна, авио-бомбе, електромагнетне, графитне бомбе и друга средства која спадају у оружја која су забрањена међународним конвенцијама (која спадају у категорију нехуманих и оружја за масовно уништавање, на пример касетне бомбе, запаљива средства и сл.). Водеће војне силе су у регионалним ратовима користиле и авионе најсавременије технологије. Употребљавани су сателити и многа друга средства за електронска дејства.

Најсавременија оружја и ратна техника омогућавају брже и поузданије откривање и праћење циљева, сигурније вођење, велику прецизност погађања и веће ефекте дејства. Осим тога, та оружја се теже откривају и уништавају, одбрана од њих је сложенија и мање ефикасна. Највећи број држава у свету није у могућности да поседује та оружја, најпре због високе производне цене, а потом и због тога што водеће војне силе не желе да се реше предности поседовања тих оружја у рату.

Сви видови и родови оружаних снага поседују нека од средстава врхунске ратне технике. Највише средстава последње генерације ратне технике налази се у наоружању ваздухолловства, ракетних јединица, ратне морнарице и јединица за електронска дејства.[216] Многа од тих средстава употребљавале су у регионалним ратовима оружане снаге САД и других водећих држава НАТО-а, поготово у току НАТО-југословенског рата.[217]

---

[216] Микић С., *op. cit*., стр. 266.

[217] Снаге НАТО-а тада су први пут користиле специјална борбена средства за дејство по електроенергетском систему СР Југославије. Употребљаване су „графитне бомбе“ за избацивање електропривредних постројења и преносне мреже из функције. Упоредо са њима, коришћена су и ракетна зрна и пројектили ваздух-земља. На тај начин био је паралисан електро-привредни систем земље и онемогућено је нормално функционисање државе. Да би се омогућило успешно дејство авијације и у неповољним временским условима, снаге НАТО-а су користиле бомбе за разбијање облака и термо-светлеће бомбе. Масовна примена тих бомби условљавала је и промену микроклиме у тим рејонима. Неки научници сматрају да је суша, која је погодила СР Југославију 1999. године, била последица НАТО бомбардовања. Снаге НАТО-а су у великој мери употребљавале борбена средства која су забрањена међународним ратним и хуманитарним правом. То се односи на касетне бомбе, муницију с осиромашеним уранијумом и хемијско оружје. Касетне бомбе су употребљаване и по цивилним објектима и насељеним местима. Ради повећања ефикасности дејства по оклопним возилима и фортификацијским објектима, авијација САД је користила пројектиле с осиромашеним уранијумом који, осим тренутних, ствара и дуготрајне штетне последице по здравље људи и животну средину. Према: *Ibid*., стр. 267.

У савременим ратовима мале су могућности за постизање стратегијског изненађења. У веома повезаном свету развијени средства, снаге и методи за праћење и сагледавање кризних ситуација и припрема за могуће сукобе. Све то ограничава могућности за постизање стратегијског изненађења при евентуалном избијању рата. Свака држава која има добро организован систем одбране и одговарајуће обавештајне службе може избећи ситуацију да буде стратегијски изненађена.

Оперативна, поготово тактичка изненађења, у савременим ратовима су могућа. Пре свега, то се тиче планова и одлука о ангажовању снага, маневара у току извођења борбених дејстава, мера и поступака оперативног и тактичког ма скирања, разних лукавстава, дезинформација противника, изненађења, промена начина борбених дејстава и друго.

У односу на предмет нашег истраживања посебну пажњу је потребно посветити карактеристикама савремених ратова које су настале као последица употребе савремених технологија у војној сфери. Поједине особености савремених ратова је неопходно подробније објаснити у циљу разумевања новог облика савремених друштвених конфликата - кибер ратовања. Међу особености које су од посебног значаја за разумевање, анализу и категоризацију феномена кибер ратовања можемо уврстити: *професионализацију састава оружаних снага и повећану улогу „специјалних дејстава“, непосредно и посредно учешће паравојних формација и цивила у ратним сукобима, медијско „препарирање“ јаног мњења и краће трајање ратова*, *промена улоге и значаја времена* и *измењена улога простора (копно, ваздух, вода, космос и кибер простор)*

2.3.1. Професионализација састава оружаних снага и повећана улога „специјалних дејстава“

Повећање броја професионалаца у саставима оружаних снага је данас општи тренд у свету. Савремена ратна техника, знатно сложенији садржаји и начини борбених дејстава, скраћено време за обављање функционалних задатака у рату, истакли су у први план потребу за све већом професионализацијом састава оружаних снага, поготово великих сила, јер оне располажу најмодернијом ратном техником и имају одговарајућа финансијска средства за подмиривање трошкова професионализације. Савремена ратна техника је сложена за руковање, а уз то и врло скупа. Потребно је много времена и финансијских средстава за обуку

руковалаца савременом ратном техником. Отуда и оријентација савремених армија да у своје редове укључе све више професионалаца.

Стручњаци за извођење специјалних дејстава имају врло значајну улогу у савременим ратовима уз тенденцију увећања њиховог ангажмана у будућности. Не постоје неке устаљене норме и обрасци за образовање и ангажовање јединица и састава који изводе специјална дејства. Свака држава има своје специфичности када је реч о намени, опремању и ангажовању специјалних јединица и начинима извођења специјалних дејстава. У категорију специјалних дејстава спадају обавештајна, психолошка, диверзантска, пропагандна, противдиверзантска, противтерористичка и друга дејства, посебно опремљених, организованих и обучених састава.

Специјална дејства се изводе на територији противника, а по потреби и у властитој позадини, када се укаже потреба за борбу против обавештајних, диверзантских, терористичких група и састава противника. Специјална дејства извршавају специјалне јединице, састављене од врхунски обучених професионалаца.

Специјалне јединице поседују посебну опрему и наоружање за извиђање, позиционирање, везу, дејство и маневар. У многим армијама постоје и посебне команде специјалних снага.

Услед професионализације војног кадра, ангажовања специјалиста у свим видовима војне активности као и савремене технологије, развијене државе су у могућности да у рату учествују са ограниченим снагама и потенцијалима, често и далеко од своје матичне територије. Отуда за њих рат, најчешће, не представља неки већи терет и није тоталан по обухвату, већ строго селективан, дозиран према потребама за реализацију постављеног циља агресије. Ангажују се само неопходна средства и снаге које, пак, дају потребне ефекте.

2.3.2. Непосредно и посредно учешће паравојних формација и цивила у ратним сукобима

У савременим ратовима, осим регуларних, учествују различити незаконити војни састави. То могу да буду групе, скупине, различите оријентације, јачипе, организације, наоружања, порекла, понашања, начипа ангажовања и борбених вредности. Негде су то страни плаћеници, другде групе верских фанатика, терористичке групе итд.

Незаконити и нерегуларни војни састави се, по правилу, јављају у свим грађанским ратовима. Најчешће они чине и основну снагу појединих страна у сукобу у почетном периоду грађанских ратова. Служе као језгро за формирање оружаних састава који се ангажују у грађанском рату (то поготово важи за ону страну која се ангажује против званичних државних институција и регуларне војске). Сваки рат има своје специфичности, што важи и за нерегуларне саставе који у њему учествују. Негде се ти састави укључују у регуларне јединице оружаних снага, другде имају одређени степен самосталности са већим или мањим усклађивањем са дејствима регуларних снага, док се понекад догађа да ти нерегуларни састави остају ван сваке контроле званичних структура власти и руковођења, те се понашају као праве криминалне дружине.

Осим организованих легитимних и нелегитимних паравојних формација, у рату све чешће посредно учествује и цивилно становништво. Чест је случај да се у пропагандну борбу, која је пратилац конвенционалног рата, укључују и цивили – појединачно и организовано у скупине. Ова могућност утицања на „слику“ о рату, тј. ширења информација и дезинформација омогућена је лакоћом приступа и доступношћу Интернета као средства масовне комуникације. Данас сваки појединац може преко глобалне рачунарске мреже послати у свет властито виђење ситуације на терену. Осим тога, уколико влада информатичким технологијама, он се може активно укључити у борбу − нападати војне и цивилне информационе системе непријатељске државе.

2.3.3. Медијско „препарирање“ јавног мњења и краће трајање ратова

Медијско „препарирање“ јавног мњења и прикривање правих циљева агресије једна је од кључних карактеристика савремених ратова. Пропагандне активности добиле су значајно место у савременим ратовима захваљујући енормном утицају електронских медија и других средстава јавног информисања на јавно мњење. Пропагандним средствима нападач настоји да по сваку цену оправда ступање у рат и ангажовање у сукобу. При томе се не бирају средства и методи да би се агресија оправдала. У државама агресора сви значајни медији се стављају под контролу владајућих политичких структура и државе, да би могли да остваре планирани пропагандни ефекат на јавно мњење. Грађани су изложени таквом

пропагандном и политичком притиску да често и несвесно прихватају оне представе које нису у складу са њиховим моралом и системом вредности.

Савремени, пре свих међудржавни, ратови краће трају. То је нарочито изражено код регионалних ратова. Локални ратови трају нешто дуже, а грађански најдуже. Краће трајање међудржавиих ратова условљено је, највише, њиховом производном ценом и брзим трошењем људских и материјалних потенцијала страна у сукобу.[218]

Осим тога, велике силе настоје да рат што пре окончају и због јавног мњења, које и поред медијског „препарирања“ све теже прихвата рат што он дуже траје. Уколико се рат одужи, показало се, владе агресорских држава губе ауторитет те им слаби утицај и позиција, што није у њиховом политичком интересу.

Са друге стране, у савременим условима истина о рату се, захваљујући информационо-комуникационим технологијама, теже скрива и поред покушаја медијске блокаде од стране агресора. Велики утицај у овом смислу имају невладине организације, грађани и новинари, који на својим веб порталима „откривају праву истину“, документујући је фотографијама, документима и описом ситуације на терену. Под ову врсту активности може се сврстати и деловање Џулијана Асанжа, оснивача сајта „Викиликс“, који је током 2010. године објављивао поверљиву дипломатску преписку као и строго поверљива документа америчке војске.

2.3.4. Промена улоге и значаја времена

Променили су се улога и значај времена у савременом рату. Све активности, борбене радње и дејства изводе се у знатно краћем времену. Скраћено је време припрема за борбена дејства, рад команди, доношење одлука, логистичке задатке. Томе су највише допринели савремена технологија, техника, карактеристике и могућности оружја, поготово информатичке технике. Отуда је и повећан значај школовања и обуке кадрова, а нарочито специјалиста који рукују техником, јер треба брзо и ефикасно обављати функционалне задатке у тако скраћеном времену и уз интензивна борбена дејства.

---

[218] Микић С., *op. cit*., стр. 263.

Време је, као климатски и метеоролошки фактор, такође претрпело одређене промене улога. Наиме, савремена ратна техника и оружје мање зависе од тих елемената времена. Савремена авијација успешно изводи борбена дејства и у лошим метеоролошким условима. Она је опремљена одговарајућим уређајима и средствима за дејство у тим условима. Ракетна борбена средства су понајмање зависна од временских услова (климатских, метеоролошких и услова видљивости).

2.3.5. Измењена улога простора (копно, ваздух, вода, космос и кибер простор)

Простор је попримио знатно измењену улогу у савременом рату. Ратни сукоби су некада отпочињали објавом, а тек потом и сударом копнених снага супротстављених армија. Међутим, перманентни развој ратне технике је радикално изменио и начин самог ратовања. Сламање отпора непријатељске стране данас се ретко врши уз помоћ пешадије. Борбени простор савременог рата не укључује само оперативни простор оружаних снага, већ мање-више обухвата читаво друштво непријатеља. Услед тога што модерна друштва зависе од нафте, електричне енергије, технолошке опреме и комуникација, она постају веома рањива на различите видове напада.

У савременом периоду противник најчешће бива поражен дејством оружја са великих висина или дистанце. Савремена наука, техника, комуникације, информатика и друга достигнућа омогућавају да се многи садржаји рата могу успешно реализовати са велике удаљености од противника, на ма којем делу Земље се он налазио. То нарочито важи за пропагандна, психолошка, политичка, информатичка дејства и економске мере и активности у рату.

Посебна карактеристика савремених међудржавних ратова су дејства делова оружаних снага са великих одстојања и висина, када међу противницима није успостављен непосредни борбени додир на копненом делу ратишта. Савремена авијација, ракете и сателити то омогућавају. Таквим дејствима нарочито прибегавају најмоћније војне силе, поготово када изводе операције против малих и војно инфериорнијих држава, избегавајући на тај начин властите губитке.

С обзиром на техничке могућности савременог наоружања, простор се лакше и брже савлађује. То се тиче свих основних врста и димензија простора.

Рељеф, хидрографски елементи и климатски услови добили су измењен значај у рату. Они и даље испољавају утицај и представљају услове за борбена дејства, али је њихов утицај нешто мањи у односу на ранији период. Авијација, хеликоптери и сателити омогућавају савлађивање простора без обзира на рељеф земљишта, реке, језера и друге природне и вештачке препреке.

Космос се последњих деценија у знатној мери користи за ратна дејства због чега се често назива и „четвртом димензијом простора“ (поред копна, мора и ваздуха). То се, пре свега, тиче оружаних снага најмоћнијих држава. Најпре је космос истраживан и коришћен за потребе телекомуникација, снимања, разних мерења и у друге сврхе. У савременим ратовима космос се све више користи за извођење борбених дејстава, најчешће за извиђање, везу, командовање, противваздушну и противракетну одбрану. Основна средства за те задатке су сателити различитих намена и могућности. Космички простор и космичка техника користе се најчешће за следеће војне потребе: фото-извиђање; одржавање веза; извиђање и осматрање океанских пространстава; електронско извиђање; навигацију; праћење метеоролошке ситуације; научноистраживачку делатност; постављање орбиталних станица; лансирање орбиталних бомбардерских сателита; противракетна дејства и противсателитска дејства.

Рат у Заливу је био први случај да су коришћени сателити за одржавање веза командовања у рату, затим за потребе припремања и доношења одлука. Коалиционе снаге су, том приликом, користиле око шездесет сателита.[219] Сателитарна технологија је, такође, у великој мери коришћена током агресије НАТО-а на СРЈ, као и у рату у Авганистану 2001. године.

У Заливском рату 1991. године је свега 8% бомби имало ласерско навођење. До интервенције у Авганистану (2001-2002) отприлике 60% свих бомби било је или са ласерским навођењем или са комерцијалним глобалним сателитским навођењем. Штавише, током Заливског рата 1991. укупан опсег неопходан за размену информација био је 100 мегабита у секунди (Mbps). Рат у Авганистану захтевао је више него удвостручен опсег, или 250 Mbps. Иронија је да су, управо комерцијални сателити чије су орбите 23,000 миља изнад земљине површине омогућили Пентагону

[219] Тофлер А., Тофлер Х.: *Рат и антират,* Paideia, Београд, 1998, стр. 113.

скоро целокупан опсег. Војна потреба за сателитским комуникационим системима може се видети и на следећем примеру: само једна беспилотна летелица Global Hawk (која опскрбљује Ратно ваздухопловство и команданте на ратишту обавештајним, надзорним и извиђачким снимцима високе резолуције у скоро реалном времену) употребљава 50 Mbps.[220]

Ипак, зависност Америке од сателита није ограничена само на навођење ракета. Америчка војска у великом степену зависи од сателита захваљујући свом ослањању на рачунаре и информације. У суштини, сателити представљају „летеће рачунаре", према речима Данијела Хејстингса (Daniel Hastings), и тако представљају најбољи пример напредних ИТ система за разновсрну употребу који се могу користити у разним видовима комерцијалних трансакција као и у војним акцијама.[221] Чињеница да „свемирска" материјална имовина истовремено може бити и нематеријална, информациона имовина – јер сакупља, обрађује и преноси информације – чини свимирско ратовање и информационо ратовање узајамно повезанима.

На пример GPS (глобални сателити за навигацију) постављени су у свемиру како би имали вишеструку комерцијалну и војну употребу, док се GMTI (радарски систем за лоцирање покретних објеката на тлу) може користити за надзор саобраћаја и контролу градова, као и у војне сврхе. Мање уочљиви, и много осетљивији, нано-сателити (минијатурни сателити) почињу да замењују функције великих сателита. Чињеница да се снижавају трошкови лансирања и да сателити постају мањи значи да ће и комерцијалне фирме, као и сиромашније земље моћи да створе сопствене сателитске системе. Истовремено, комерцијални сателитски снимци имају резолуцију све ближу оној коју су имали тајни извиђачки сателити САД и бившег Совјетског Савеза током Хладног рата, што значи да је свакој држави или екстремистичкој групи омогућено да приступи визуелним информацијама. Сателитске карте доступне на претраживачу Google.com већ изазивају забринутост у безебедносним круговима.

---

[220] Gardner H.: "War and the media paradox", *Cyber Conflict and Global Politics, Routledge*, Abingdon, 2009. p. 30.

[221] *Ibid*.

Питање безбедности покреће се јер су комерцијални системи јефтинији, што значи и да Пентагон губи контролу над њима. Истовремено, цивилни власници сателита очекују војну заштиту. Ово ствара непрекидну тензију између војне безбедности и приватних интереса која, затим, почиње да ствара захтеве да се војне способности прошире у свемир како би се заштитили приватни сателити. Хејстингс је описао војну ситуацију у свемиру следећим речима због мешања одбрамбених и комерцијалних сателита: „Свемирско ратовање водиће се у присуству неборачког (цивилног) кадра: као ратовање са герилама у урбаном подручју".[222]

Због ових чињеница америчка војска у великој мери зависи од имовине која се налази у свемиру. Али чињеница да сателити представљају „летеће рачунаре" чини их потенцијално рањивим, јер могу претрпети удар кибер напада. Развој нано-сателита који се могу као паразити закачити на веће сателите, ствара додатну забринутост, у смислу да они могу касније експлодирати или прекинути комуникацију. Остале претње укључују могућност нуклеарног удара на великој висини; ова претња би захтевала много редундантних сателита како би се очувале могућности комуникације. Сами војни корисници ће, стога, морати да заштите своје информације „високим степеном разноврсности" или ће на други начин морати да „очврсну" комуникационе и сателитске системе.[223] Док су амерички војни званичници предлагали оснивање Команде за неконвенционално ратовање, како би се изборили са кибер саботажом и другим екстремистичким активностима, Сенат САД је размотрио нови закон (Акт о заштити критичне информационе инфраструктуре) како би се решило питање заштите како владиних, тако и приватних рачунарских и информационих система.[224]

Поред истицања важности сателитских комуникација за вишеструке војне и комерцијалне сврхе, глобална тржишта настала, бар делимично, Интернет маркетингом почела су да оправдавају проширену улогу Ратне морнарице САД-а. У овом случају, аргумент да терористичке групе, пирати или државе могу покушати да

---

[222] *Ibid*.

[223] *Strategic Plan,* DARPA, 2007, http://www.darpa.mil/body/news/2007/2007StrategicPlan.pdf

[224] Boot M.: *Statement Before The House Armed Services Subcommittee on Terrorism, Unconventional Threats, and Capabilities*, CFR, June 29, 2006, http://www.cfr.org/publication/11027/statement_before_the_house_armed_services_subcommittee_on_terrorism_unconventional_threats_and_capabilitieshtml

прекину глобалну трговину и нападну подводне оптичке каблове, на пример, постало је главно питање за заштиту глобалне економије. Даље се наводи да производи који се продају преко Интернета обично путују бродовима, те је зато потребна морнаричка заштита. Због тога Америка планира да и даље развија капацитете своје морнарице како би заштитила процват глобалне трговине засноване на информационо-комуникационој технологији од тероризма и пиратерије, и како би спречила шверц оружја, наркотика и друге недозвољене активности.

У савременим војним доктринама, међутим, и виртуелни, нееуклидовски простор - кибер простор - је стекао статус петог борбеног простора уз копно, воду, ваздух и космос. Све више аутора сматра да је „виртуелни простор" место где би се могле водити примарне борбе у будућности, а поједине државе се увелико припремају за такав концепт вођења ратова.[225] Кибер простор не само да је погодан амбијент за спровођење пропагандних активности већ се путем њега може причинити и конкретна физичка штета – нападом на информационе инфраструктуре одређене државе – што може резултовати људским и материјалним жртвама, као и нарушавањем суверенитета нападнуте државе. Због тога је кибер простор данас постао не само мета напада већ и моћно средство (оружје напада) у арсеналу технолошки развијених армија и њихових специјализованих „информатичара ратника".

Први „Интернет рат" одиграо се априла 2007., између руских и естонских хакера. Руска влада је била оптужена за иницирање конфликта, али није у потпуности јасно ко, заправо, стоји иза њега.[226] Током 2005. десило се око 1300 успешних упада у рачунаре Пентагона (од више него 79000 покушаја). У септембру 2007., Кинеска народно-ослободилачка армија (ПЛА) била је оптужена за хакерски упад у рачунаре Пентагона, Велике Британије, и Немачке (ове оптужбе негирао је Пекинг). Један од кинеских војних циљева је, наводно, стицање „електронске доминације" над САД-ом, Британијом, Русијом и Јужном Корејом до 2050. године.[227] У јануару 2007., Пекинг је тестирао ракету која има способност да уништи сателите у орбити. Ако се узме у обзир да примирје које би заиста зауставило даље

---

[225] *L' Armement*, No. 60, XII., Paris, 1997 - I. 1998.; *From cybercrime to cyberwarfare*, "Défense nationale et sécurité collective", No 6, The Committee for National Defence Studies, Paris, 2008.

[226] Ifrah L.: "Europe Confronted by Digital Crime", *European Issues*, No. 70, 2007.

[227] Gardner H., *op. cit*., p. 30.

тестове или употрбу анти-сателитског наоружања (ASAT) не може бити скоро склопљено, кинески анти-сателитски тест би могао изазвати обнављање наоружања како у свемиру, тако и на тлу, и то у комбинацији са новим формама информационо-комуникационог ривалитета.[228]

Висок ступањ зависности Пентагона од комуникационих линкова и информационих операција чини ова подручја „Ахиловом петом“ за потенцијална ометања, прекиде функционисања и нападе. Поред реалних претњи које кибер-саботажа представља за кључне комуникационе системе, сателити, као „летећи компјутери“, могли би представљати једну од првих мета у рату за стицање надмоћи, јер су и Кина и Русија почеле да прете – делимично како би се супротставиле развоју америчких балистичких ракета за против-ваздушну одбрану које зависе од сателитских комуникација.[229]

---

[228] *Ibid*.

[229] Gardner H.: *Averting Global War: Regional Challenges, Overextension and Options for American Strategy*, Palgrave, New York, 2007.

3. ПОЈАМ И КАРАКТЕРИСТИКЕ КИБЕР РАТОВАЊА

У претходном поглављу указано је на то да у научној литератури не постоји јединствен приступ феномену рата. Различити теоретичари на различите начине дефинишу комплексни појам *рат*. Неслагања су изражена не само у дефиницији ратног сукоба већ и у приступима класификацији ратова.

Класификација ратова се може извршити на основу бројних критеријума. Разумљиво је да поједини аутори наглашавају одређене критеријуме, у складу са својим вредносним и идеолошким оријентацијама.

Међутим, из досадашњег излагања може се закључити да се у свим приступима класификацији, техничко-технолошком фактору придаје посебан значај. Важност овог фактора је несумњива јер је технологија одиграла кључну улогу у промени начина ратовања у другој половини XX века те утицала на карактеристике савременог ратовања.

Наглашени утицај технологије на начин вођења рата изнедрио је и плуралитет појмова који се користе да опишу овај феномен. У семантичком смислу данас се, осим појма „савремени рат“ често употребљавају и појмови „постмодерни рат“[230], „рат четврте генерације“[231], „рат идеја и емоција“ или „рат у коме противник уопште не поштује правила ратовања“.[232]

Можемо дакле констатовати да се свет данас суочава са феноменом рата који још није у потпуности дефинисан, класификован и садржајно одређен.

Нова обележја савремених ратова попут: професионализације састава оружаних снага и повећане улога „специјалних дејстава“, учешћа паравојних формација и цивила у ратним сукобима, медијског „препарирања“ јавног мњења и краћег трајања ратова, промењене улоге и значаја времена и измењене улога простора, у највећој мери последице су примене нових технологија у војне сврхе као и информатизације друштва у целини.

---

[230] Møller B.: “The Faces of war“, у: Реформа сектора безбедности, зборник радова, прир. Мирослав Хаџић, Г 17 Институт и Центар за цивилно-војне односе, Београд, 2003, стр. 307.

[231] Lind W., et al., *op. cit*., pp. 22-26.

[232] Арсић С.: „Нова теорија ратовања – против људског ума“, *Одбрана*, 1. фебруар 2008, стр. 40.

Доминантну улогу у савременом друштву, као и у војним активностима, заузела је информационо-комуникациона технологија. Развој информатичких наука у другој половини прошлог века и примена информационо-комуникационих технологија у свим сферама друштвеног живота у последњој деценији прошлог века произвели су ефекат информатизације друштва и најавили епоху „дигиталног доба".

Револуција медија и информационих технологија суштински мења начин интеракције у друштву – као и начин на који државе (и паравојне, анти-државне формације) воде ратове. Војно-технолошком терминологијом речено, јасно је да су непрекидном фузијом револуционарних достигнућа на пољу рачунара, сателитских комуникација и медија радикално „унапређене" могућности ратовања, чак иако информационо-комуникациона револуција није суштински изменила геостратешке и политичко-економске циљеве самог рата.[233]

Донедавно се у борбу није ишло а да се претходно не обезбеди довољан број обавештења о снази противника, сопственим снагама, простору и времену. Специфична сазнања о снази противника, просторним и временским карактеристикама неопходна су за успешно вођење рата. Међутим, она нису и довољна. Данас треба најпре обавестити јавно мњење о разлозима за борбу и резултатима борбе. За остваривање постављеног циља такође је неопходно противника лишити преимућстава које му пружају његове информације, уз истовремено обезбеђење потребних информација за сопствене потребе, што значи остварити осетну предност у реализацији циља на одређеном простору и за одређено време, уз минимално ангажовање снага и минималне губитке. Савремене оружане снаге се у овим активностима изузетно много ослањају на најновија технолошка достигнућа на пољу информационо-комуникационих технологија.

Информациона револуција је значајно трансформисала начин на који се воде ратови у информационом добу – изазвала је промене у томе како друштва долазе у конфликт, како њихове оружане снаге воде оружани сукоб итд. Више се не сукобљавају масовне, укопане војске у крвавим исцрпљујућим борбама. Уместо тога, мале и изузетно мобилне снаге, „наоружане" информацијама у реалном времену

---

[233] Gardner H.: *Averting Global War: Regional Challenges, Overextension and Options for American Strategy*, Palgrave, New York, 2007.

добијених са сателитâ и сензорâ, ударају великом брзином на неочекиваним местима. Победник је она страна која може да брже експлоатише информације, односно она страна која брже анализира, процењује ситуацију и реагује. Велике промене су видљиве у начину прикупљања, чувања, обрађивања, прослеђивања и приказивања информација, и у степену организованости организација за искоришћавање повећаног обима информација. Информација је постала стратегијски ресурс. Доминација у информационом спектру представља, дакле, неопходан услов за успех и победу у сукобу.[234]

Постизање доминације у информационом спектру омогућено је различитим техникама за манипулисање садржајем информационих система – информацијом која се преноси и њеним „паковањем“ – оруђем потребним да се та информација обликује и упути до корисника. То је могућност да се потпора информације и сама информација контролишу преко надмоћи у понуди у области рачунарских мрежа, машина и рачунарских програма (примењена логистика као подршка саме информације, намењене за решавање проблема корисника). У прилог овој тврдњи Владимир Волков износи запажање да је рат у Заливу представљао више тријумф информације него наоружања, стратегије или морала трупа: „Веома развијена техничка средства Американаца и коришћење сателита омогућили су да се информација користи у реалном времену, тј. тренутно и непосредно, тако да су савезници знали све што је Ирак чинио, док се сâм Ирак играо ћораве баке.“[235]

Посебну прекретницу у сфери војних активности али и поимања националне, регионалне и глобалне безбедности представљао је настанак кибер простора. Нови „простор“ пружио је енормне могућности за спровођење специјалних пропагандних дејстава али и извођење напада посредством рачунарских мрежа на противничке информационе системе. Ови напади у виртуелном простору, наоко неприметни, могу у реалном, физичком, свету резултовати људским жртвама и материјалним разарањима.

Због тога је кибер ратовање данас у жижи интересовања теоретичара и научника из области војних, информатичких, правних и безбедносних наука.

---

[234] Вулетић Д., *op. cit*., стр. 492.

[235] Волков В.: *Дезинформација – од тројанског коња до интернета*, Наш дом, Београд, 2005, стр. 209.

3.1. Генеза појма кибер ратовање

Паралелно са активностима на развијању и усавршавању могућности и средстава за вођење конвенционалних сукоба кинетичким оружјем, високо развијене земље су, у хладноратовском периоду, користиле своју технолошку предност за унапређивање способности вођења специјалног рата. У уводу рада смо констатовали да је распрострањена употреба телевизијске и сателитарне технологије већ од шездесетих година XX века отворила нове могућности за вођење информационог рата.

Историјски посматрано, информационо ратовање није нова појава. Историја људске цивилизације сведочи о бројним примерима информационог ратовања који указују на значај информације у постизању информационе супериорности у односу на противника.

Да подсетимо, израз *информација у рату* претходио је изразу *информационо ратовање*. Данас се у војним доктринама већине Западних земаља синонимно употребљава и израз *информационе операције*. Алвин и Хајди Тофлер су, пак, употребили појам *доктори за ефекат* (*енгл.* spin doctors) како би именовали стручњаке за информациони рат, тј. оне који стварају жељени ефекат помоћу информације, проналазећи и измишљајући начине да се она уверљиво представи. Без обзира на плуралитет израза и непостојање консензуса по питању њихове употребе, можемо констатовати да сви они истичу војни аспект пропагандних активности те да реферирају на офанзивну и дефанзивну употребу информација и средстава информисања у смислу искоришћавања, поткупљивања, кварења и уништења противничких информација и система који их преносе, уз истовремену заштиту властитих информација и система. У складу са овим одређењем, може се тврдити да се вођење информационог рата, тј. информационих операција заснива на три принципа: сазнати, спречити другога да дође до сазнања, навести друге да дођу до неистинитог сазнања. У том смислу, нагласили смо да Међународна асоцијација савета одбране (International Association of Defense Counsel - IADC) разликује три вида информационог рата: рат *за* информацију; рат *кроз* информацију (помоћу дезинформације) и рат *против* информације.

Француски часопис *Наоружање* посветио је један тематски број питањима о улози информације односно дезинформације у савременом рату. Информациони рат,

тј. рат помоћу информације, за њу и против ње, том приликом је оквалификован као оружје без којег се више не може. Савремена војна операција не може се ни замислити без „информационог покрића“, као што се не може замислити ни без „ваздушног покрића“. У поментом часопису Давид Буден пише да се „инфосфера од данас сматра петом димензијом борбе у рату – уз копнену, поморску, ваздушну и свемирску димензију“.[236]

У свом чланку под називом „Информационо ратовање: шта и како?“ Брнс дефинише информационо ратовање као „категорију техника, укључујући прикупљање, пренос, заштиту, манипулацију, прекид и уништење информација којима се одржава предност пред противницима“.[237]

Крај осамдесетих и почетак деведесетих година двадесетог века обележио је настанак савремених информационих система чију основу чине персонални рачунари и рачунарске мреже. Распрострањена употреба рачунара и рачунарских мрежа у последњој декади XX века отворила је енормне могућности за вођење информационог рата. Нови борбени фронт информационог рата препознат је у тзв. кибернетском простору, тј. Интернету као његовом најексплоатисанијем репрезенту.

С крајем „стабилности“ биполарног света, нови ризици и претње, често не-војног карактера, као што су миграциони таласи, тероризам и ширење оружја за масовно уништење, нашли су место у агенди безбедносних политика западних држава. Ако многи од ових елемената нису били непознати безбедносним сценаријима, оно што их сигурно карактерише и разликује у односу на прошлост била је изражена перцепција западних земаља о високом степену несигурности који може потицати од субјеката који би за достизање својих циљева користили не-војна, тј. асиметрична средства. На списку могућих „средстава повреде“, тј. начина за супротстављање западној војној надмоћи, нашао се, осим оружја за масовно уништење и терористичких активности, и широк спектар инструмената које нуде информационе технологије.

---

[236] L’Armement, No. 60, Paris, XII.1997–I.1998.

[237] Burns M.: *Information Warfare: What and How?*, http://www-2.cs.cmu.edu/~burnsm/Info Warfare.html

Услед растуће зависности друштва од ИКТ и ниских трошкова приступа кибер оружју, страх од рањивости се, историјски посматрано, прво појавио у САД.[238] За неколико година се страх од могућег асиметричног сукоба проширио и на остале технолошки високо развијене државе света, попримивши следећу форму – непријатељ који није у стању да уђе у традиционалну врсту сукоба могао би да нападне виталне тачке кибер простора.

Због значаја који је кибер простор попримио за вођење информационог рата, последњих је година све чешће у употреби и термин *кибер ратовање* (*енгл.* cyber warfare). Изрази *информационо ратовање* и *кибер ратовање* се у научној и стручној литератури често синонимно употребљавају. Други појам је, међутим, ужи по обиму јер снажно наглашава рачунарске и мрежне аспекте информационог ратовања.[239]

У том смислу, можемо констатовати, да се под прихватљивом дефиницијом кибер ратовања може подразумевати свака дефиниција информационог ратовања која садржи рачунарску мрежу као просторну одредницу дефиниендума, тј. у којој се активност информационог ратовања одвија посредством рачунарске мреже.

Поједини аутори, пак, праве разлику између *информационог ратовања* и *кибер ратовања* а, осим ових појмова, користе и појам *мрежног ратовања* (*енгл.* netwar), сматрајући да су све су три концепције у сагласности с парадигмом „трансформације ратовања“.[240]

Тако, на пример, Анита Перешин сматра да се највеће разлике између информационог ратовања, кибер ратовања и мрежног ратовања огледају у следећем:

- Информациони рат подразумева широко примењивање деструктивне силе против информационих система, рачунарских система и система који подржавају четири кључна инфраструктурна подручја: енергетику, комуникације, финансије и транспорт.

---

[238] Не смемо заборавити улогу лидера, коју су САД одувек имале у пољу напредних технологија и њиховој цивилној и војној примени.

[239] Према: Knapp K., Boulton W.: “Ten Information Warfare Trends“, in Janczewski L., Colarik A.: *Cyber Warfare and Cyber Terrorism*, Information Science Reference (an imprint of IGI Global), Hershey, 2008, p. 25.

[240] Ван Кревелд М.: *Трансформација рата*, Јавно предузеће Службени Гласник и Факултет безбедности, Београд, 2010.

- Концепција кибер ратовања односи се на информационо усмерен војни сукоб, углавном високог интензитета, док се концепција мрежног ратовања односи на друштвени сукоб ниског интензитета и невојних операција.
- Док се у кибер рату супротстављају војне снаге, у мрежном рату су супротстављене недржавне снаге, паравојне и нерегуларне, као у тероризму.
- Ниједна се од наведених концепција не односи само на технолошки аспект, него их треба сагледавати са аспекта доктрине, тактике и стратегије те са технолошког аспекта примене иновација при одбрани и нападу. [241]

Иако заступа став да међу наведеним појмовима треба правити разлику, Перешин се у наставку текста, након дате дистинкције, од ње ограђује следећим ставом: „треба нагласити да због комплексности подручја информационог ратовања не постоји јединствена, свеобухватна и општеприхваћена дефиниција тог појма“.[242]

У истом смислу Мартин Либицки, у својој књизи „Шта је информационо ратовање?“ наводи да је „поимање проблема информационог ратовања исто као дати слепцу да препозна слона: ако му дотакне ногу каже да је дрво, ако га ухвати за реп каже да је уже итд.“, те на тај сликовити начин показује бројне аспекте информационог ратовања.[243]

Са друге стране Бони Еткинс, истраживач војног Универзитета у Алабами, у књизи *Спектрум кибер конфликата* прави разлику између кибер ратовања и појмова са сродним значењем. Међу појмове са сродним значењем он сврстава: кибер криминал, хактивизам, кибер шпијунажу и кибер тероризам.[244]

Према овом аутору кибер ратовање и информационо ратовање су појмови који се могу синонимно употребљавати. Кибер ратовање је дефинисано као: „коришћење компјутерских техника упада и других могућности против противничке инфраструктуре базиране на информационо-комуникационим технологијама, са намером

---

[241] Perešin A.: „Paradigma novoga terorizma informacijskoga doba“, *Politička misao*, Vol. XLIV, br. 2, Zagreb, 2007, str. 93–112.

[242] *Ibid*., стр. 98.

[243] Према: Burns M., *op. cit*.

[244] Adkins N. B.: *The Spectrum of Cyber Conflict From Hacking to Information Warfare: What is Law Enforcement's Role?*, Air Command and Staff College, Air University, Alabama, 2001.

угрожавања националне безбедности или припреме за будуће операције против националне безбедности.“[245]

Рејмонд Паркс и Дејвид Даген дефинишу кибер ратовање као „подскуп информационог ратовања који укључује акције предузете у кибер свету“, док је кибер свет „било која виртуелна реалност која се састоји од збира рачунара и рачунарских мрежа. Постоји много кибер светова али најрелевантнији за кибер ратовање јесте Интернет и са њим повезане мреже које деле садржаје са Интернетом.“[246] Осим ове, по обиму шире дефиниције, поменути аутори дефинишу кибер ратовање и у ужем, војном смислу. Прецизније говорећи, они прихватају дефиницију кибер ратовања која је дата у Доктрини информационих операција Министрства одбране САД, која гласи: „кибер ратовање је комбиновање напада на рачунарске мреже и одговора на такве нападе уз примењивање, по могућству, специјалних информационих операција.“[247]

Друга група аутора, пак, не прави разлику између кибер ратовања и појмова са сродним значењем већ појам кибер ратовање употребљава као збирни назив за свеукупност поменутих активности и тенденција. У битно обележје кибер ратовања они сврставају и тенденцију његовог померања изван војних граница на индивидуалну, друштвену и комерцијалну раван.[248] Док је појмовно одређење информационог ратовања истицало његову војну димензију данас, можемо констатовати, већи део литературе о кибер ратовању истиче аспект његовог проширења ван војних области.

Термин кибер ратовање се, дакле, најчешће употребљава да опише широк распон активности на индивидуалном, друштвено-социјеталном, корпоративно-економском и војном нивоу.

---

[245] *Ibid*., стр. 13.

[246] Parks, R., Duggan, D.: *Principles of Cyber-warfare*, Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001, p. 122.

[247] *Joint Publication 3-13*, Joint Doctrine for Information Operations, Department of Defense, 1998.

[248] Cronin B., Crawford H.: “Information warfare: Its applications in military and civilian contexts”, *Information Society*, 15(4), 1999.; Hutchinson W.: “Concepts in information warfare”, *Logistics Information Management*, 15(5/6), 2002.

У намери да феномену кибер ратовања приступимо холистички, у његовој анализи поћи ћемо од претпоставке да је овај појам најшири по обиму, тј. да обухвата и оне активности које поједини теоретичари подводе под појмове са сродним значењем. Другим речима, под овим појмом подразумеваћемо и оне активности које се подводе под војни аспект као и оне активности које се приписују недржавним актерима (паравојним и нерегуларним формацијама и индивидуалним корисницима глобалне рачунарске мреже). У наставку рада покушаћемо да подробније анализирамо оправданост овакве хипотезе, тј. да размотримо садржинске, семантичке и логичке проблеме из терминолошког корпуса ове области.

3.2. Терминолошки и семантички проблеми у одређењу појма кибер ратовање

Проблем несигурности кибер простора и његових експлицитних и имплицитних утицаја на рањивост информатизованог друштва постао је, почетком XXI века, једна од важних тема научне, стручне али и шире јавности у свим технолошки развијеним земљама.

Скоро свакодневно умножавање броја и врста претњи у кибер простору[249] и повећање учесталости напада на рачунарске и мрежне системе, уз раст свести о могућим последицама за све аспекте друштвеног живота, утицали су на то да безбедносне претње у кибер простору постану предмет изучавања различитих научних дисциплина. Безбедносне претње информационим системима, дакле, почињу да се изучавају са многих аспеката – са позиција информационих и математичких наука и њихових посебних дисциплина (као што су криптографија и криптоанализа), безбедносних, војних, правних, криминалистичких и криминолошких.

Са семантичког аспекта, пак, увођење (преузимање) туђица из области информационо-комуникационих технологија у српски језик додатно отежава анализу, тумачење, класификацију и разјашњење нових безбедносних феномена.

[249] О врстама и субјектима претњи у кибер простору видети више у: Путник, Н.: *Сајбер простор и безбедносни изазови*, Факултет безбедности, Београд, 2009.

Један од посебно значајних проблема јесте и оправданост употребе појма *кибер рат*, тј. подвођење ове групације активности под категорију ратних сукоба.

У том смислу, може се рећи да су спорна и садржинска одређења појединих појмова који су ушли у употребу услед технолошког развоја друштва. За време Првог и Другог светског рата, на пример, појавиле су се групе нових термина за облике борби који су превазишли концепте рата из 19. века. Као четири главна облика међународне борбе, јављају се: психолошко, политичко или економско ратовање и ратовање у смислу оружане борбе, понекад називано и „војно ратовање".

После Другог светског рата појављују се термини који у себи садрже реч рат, или су по садржини слични рату, што ствара нејасноће код објашњења рата као појаве. Могли су се наћи у новинарству, публицизму, политици, науци и војној теорији. Такве појаве су: агресија, хладни рат, специјални рат, психолошки рат, геофизички рат, метеоролошки рат, сукоб ниског интезитета, тероризам итд.

О овом проблему у научној теорији постоје опречна мишљења те је неопходно детаљније разматрање ове проблематике како би се дошло до разјашњења појмовног и терминолошког корпуса ове специфичне области.

Како је претходно показано, термин кибер ратовање се у англосаксонском говорном подручју употребљава да опише широк распон активности на индивидуалном, друштвено-социјеталном, корпоративно-економском и војном нивоу.

Употреба израза кибер ратовање за описивање савремених сукоба у кибер простору може се чинити непримереном у односу на традиционално поимање рата као организованог, интензивног конфликта између држава, савеза држава, етничких и верских група или класа средствима оружане борбе у циљу остваривања одређене политичке, војне и друге добити. Такво становиште заступа и Слободан Микић, наш реномирани стручњак у области војних наука.

Овај аутор сматра да се у савременом добу врло често употребљавају термини који садрже реч *рат* а који, при томе, не осликавају право значење тог појма. Због њихове широке употребе и одређених сличности са појмом рат, неки се од њих, чешће употребљавани, разматрају и упоређују са ратом, као појмом и појавом: „Много је термина који означавају појаве које се често изједначавају са ратом, чиме настаје доста проблема у схватању праве суштине рата. Стиче се утисак

да просто влада неко помодарство у измишљању неких нових врста ′ратова′, који у суштини то нису.“[250]

Међу појаве које су сличне рату, а које то по својој суштини нису, Микић сврстава: агресију, хладни рат, пропагандни рат, специјални рат, психолошки рат, геофизички рат, информатички рат, метеоролошки рат, неокортикални рат, сукобе ниског интензитета и тероризам.

Ове појаве се, сматра Микић, не могу подводити под категорију рата јер не садрже оружану борбу а суштинска одлика рата је, управо, оружана борба. Наведене појаве блиске рату пре треба називати врстама борбених дејстава, које се могу спроводити самостално или у оквиру рата, него врстама рата по себи.[251]

Заиста је тешко говорити о стварном рату, када наведене појаве немају конкретне последице у смислу физичке штете или губитка људских живота.

И са аспекта парадигме *кибер рата* могу се наћи аргументи у прилог овој перспективи. Чињеница је да хакинг банке има само ограничен економски учинак. Модификација web странице неке институције тек изазива љутњу или губитак пословног угледа. Што се тиче терористичких група, оне употребљавају Интернет за комуникацију, регрутовање, припремање и финансирање операција. У том смислу, оправдана је констатација да се терористички напади још увек спроводе помоћу експлозива а не помоћу информатичких кодова. Традиционални начин је јефтинији и има више утицаја на јавно мњење.

И поред тога, претња од кибер рата, тј. од информатичких борбених дејстава је присутна, а ризик од ескалације ове врсте конфликта се увећава те га не би требало подцењивати. На ову чињеницу указао је Први информатички рат вођен током априла и маја 2007. године.[252] Природно, тип напада (*дистрибуирано*

---

[250] Микић С.: *О рату*, Прометеј, Нови Сад, 2006, стр. 83.

[251] *Ibid*., стр. 65.

[252] Напад је почео 9. маја 2007. године, био је усмерен на опструкцију званичних Интернет сајтова Естоније, једне од најинформатизованијих земаља на свету. Током неколико недеља, колико је напад трајао, Естонија се носила са по обиму најширим нападом ове врсте до сада. Услед напада, сајтови естонске владе (Министарства иностраних послова и Министарства правде), медија и банака били су блокирани**.** Овај напад дистрибуираног лишавања услуге подстакао је интензивне расправе о безбедности кибер простора на међународном нивоу. Према: *BBC NEWS*, Published: 2007/05/02, http://news.bbc.co.uk/go/pr/fr/-/2/hi/europe/6614273.stm; *The economist*, Published: May 10, 2007, http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598; *Telegraph*, Published: 19/05/2007, http://www.telegraph.co.uk

лишавање услуге - DDoS) био је релативно конвенционалан и од почетка се чинило да је резултат хактивизма. Ово је био први случај да су политички, медијски и економски елементи унутар земље били истовремено на мети, доводећи до привремене паралисаности државе. Ово је такође био први случај да је конфликт у кибер простору попримио политичку димензију која је могла да ескалира у ратни сукоб: неколико дана након напада, естонски министар спољних послова је као виновника напада оптужио руску владу захтевајући примену члана 5 НАТО-а који предвиђа колективну одбрану нападнуте земље.[253] Ово је, стога, био и први пут да је суверенитет државе био директно угрожен рачунарским нападом, који је био спроведен од стране недодирљивог непријатеља.

Гледано из историјске перспективе, преокрет у перцепцији претње кибер ратовања наступио је оног тренутка када су рачунарски напади погодили системе контроле који су „срца“ критичне инфраструктуре.[254] Системи контроле пружају повезаност између реалног и виртуелног света. Било који хакерски напад на DCS и SCADA системе могао би имати драматичне последице. На срећу, за сада имамо само неколико примера успешних напада против ових система. Али њихова растућа међуповезаност унутар Интернета и употреба стандардних протокола из економских разлога и из разлога повећања узајмне оперативности знатно повећавају ризик. Кибер ратовање је стога, у дословном значењу термина, постало реалност.

Поред тога, треба имати у виду да се према савременим теоретским елаборацијама и лексиколошким одредницама феномен рата не своди само на оружану борбу.[255] У семантичком смислу, дакле, допуштена је узајамна употреба термина конфликт и ратовање.

---

[253] Да подсетимо, први и једини пут Алијанса је активирала члан 5 Северноатлантске повеље, 12. септембра 2001. године, као одговор на терористичке нападе на САД од претходног дана.

[254] Међу системима контроле, два су посебно битна за безбедност критичних инфраструктура: контролни системи за дистрибуцију (Distributed Control Systems – DCS), који се користе у појединачним структурама или малим географским областима, и системи супервизије, контроле и преузимања података (SCADA) који се користе за дистрибуцију великог обима и у пространим географским областима. DCS се, на пример, може користити у току производње електричне енергије у једном систему, док се систем SCADA користи за контролу енергије произведене и дистрибуиране на широком простору.

[255] Тако, на пример, познати Вебстеров речник дефинише ратовање као: 1) поступак вођења рата; оружани сукоб, али и као 2) конфликт или борбу било које врсте, док конфликт дефинише као: 1) борбу или рат, и као 2) оштро неслагање. Видети: *Merriam-Webster Collegiate Dictionary of English*, Tenth Edition, Springfield, Ma.: Merriam-Webster Inc. 1998, s.v. warfare, conflict.

Појам рата је свакако шири и сложенији од појма „оружана борба“ јер осим милитаристичке, укључује и друге активности и облике борбе (политичке, економске итд.) које имају велики значај не само за припрему, ток и исход „ковенционалног рата“ већ и за разумевање природе друштвених односа у ери глобализације. Мишљења смо да је, стога, употреба израза *кибер ратовање* примерена јер имплицира на управо овакве, специјализоване, активности у новом, виртуелном, простору.

Прихватање оваквог семантичког одређења кибер ратовања представља први корак у нормирању денотације других појмова са сродним значењем. Овај корак је неопходан ако желимо да постигнемо доследност у истраживању опсега врста кофликата који покривају не само војне већ и политичке, економске, криминолошке, безбедносне и цивилне димензије.

3.3. Појмовно одређење кибер претње и кибер напада

Експанзија кибер ратовања, дакле, почиње у последњој деценији XX века са развојем савремених информационо-комуникационих технологија или, прецизније речено, са пуштањем Интернета у комерцијалну употребу.

Основна специфичност кибер ратовања јесте да бојиште није физички, већ виртуелни свет. Кибер ратовање се, према томе, може дефинисати као подврста информационог ратовања, којој није потребно традиционално бојно поље, већ се напади одвијају у кибернетском простору и усмерени су ка противничким информацијама и информационо-комуникационим инфраструктурама.

Кибер ратовање, у том смислу, представља релативно нов феномен за који би се могло рећи да спада у категорију савремених војних, али и не-војних, транснационалних и асиметричних безбедносних претњи.

Због тога је нужно дати одговор на питање о каквој је, заправо, претњи реч?

Претња је, по природи, апстрактан концепт – она је нешто што има потенцијал да стави једну организацију, особу или друштво у ризичну ситуацију. Претња је могућност да се оствари нежељени догађај. Када се ова могућност актуализује, она престаје да буде претња и постаје догађај попут других. У тренутку када је претњу уочио надлежни ауторитет или менаџмент она постаје део ризика, те

као таква предмет расподеле њиховог времена и расположивих ресурса (људских, техничких, финансијских итд.) ради супротстављања.

Према дефиницији групе домаћих аутора, претња у области рачунарских система могла би се одредити као: „противник, ситуација или сплет околности с могућношћу и/или намерама да се експлоатише рањивост“.[256] Данас је раширен велики број различитих претњи што искоришћавају широки спектар рањивости, које су саставни део свих рачунарских система.

У најопштијем смислу, анализа претњи претпостављаављење разлике између претњи према њиховом узроку – претње чији је узрочник људски фактор и оне чији је узрочник „виша сила“ (природне непогоде, нестабилност напајања електричном енергијом, ратно стање итд).[257] Прецизније говорећи, под појмом „виша сила“ могу се подразумевати кварови и инциденти, иако ове категорије не би требало сматрати ригидним.

Кварови су потенцијално штетни догађаји, изазвани унутрашњим дефектима система или дефектима спољашњих елемената неопходних за његово функционисање. Они могу бити и последица грешака у пројектовању софтвера, или последица кварова хардвера, људских грешака или корупције података. Категорија *инцидената* укључује све случајне догађаје, попут природних акцидената (поплаве, земљотреси, пожари итд). За разлику од кварова, инциденти су догађаји чији се узрок налази ван система.

Претње чији је узрочник људски фактор даље се разврставају на основу постојања односно непостојања намере субјекта претње. У том смислу се, на пољу кибер безбедности, говори о категорији злонамерних претњи (претњи са умишљајем) и о категорији људских грешака. Постоји сагласност експерата о томе да су ненамерне претње најраширенији облик претњи рачунарској безбедности, док се за злонамерне претње тврди да представљају највећи безбедносни изазов. Свакодневно повећање њиховог броја и врста представља тешкоћу у изналажењу адекватних мера за заштиту информационих система.

---

[256] Плескоњић Д., Мачек Н., Ђорђевић Б., Царић М.: *Сигурност рачунарских система и мрежа*, Микро књига, Београд, 2007, стр. 12.

[257] Петровић С.: *Компјутерски криминал*, МУП Србије, Београд, 2001, стр. 14.

Злонамерна претња се може изразити као сума различитих атрибута. Да би један догађај био оквалификован као злонамерна претња, неопходно је да постоји способност, намера и могућност или погодна прилика да се он оствари. Другим речима:

Злонамерна претња = Способност + Намера + Могућност

У пољу кибер безбедности злонамерне претње се поистовећују са нападима на умрежене информационе системе, тј. информационе инфраструктуре. Напади на информационе системе могу се дефинисати као директне акције против мрежа или информационих система са циљем да прекину операције, преузму контролу и униште, промене или корумпирају њихове податке (који су у обради или меморисани). Другим речима, реч је о акцијама које имају циљ да компромитују резервисаност, интегритет и расположивост информација и система у којима су оне ускладиштене.

Методи за спровођење напада могу бити разноврсни, у зависности од одређених слабости система који се напада. Исто толико разноврсна могу бити и оружја, односно инструменти који се користе за напад. На основу ефеката које ови инструменти остварују можемо издвојити три основна метода напада:

- *Физички напад* – подразумева употребу конвенционалног оружја против инфраструктуре у којој се налазе информациони системи или против линија преноса информација.[258] Ова врста напада усмерена је на расположивост нападнутог система.
- *Електронски напад* – подразумева коришћење енергетског оружја (Directed energy weapons – DEW), које је у стању да емитује електромагнетну енергију концентрисану у снопове атомских или субатомских честица. Електронски напад може бити извршен и оружјем које испушта електромагнетни импулс (Electromagnetic pulse – EMP), са циљем да преоптерети и онеспособи електричне спојеве система. Још усавршеније оружје подразумева директно убризгавање деструктивних информатичких програма у линије преноса система који користе радио-

[258] Након напада на Светски трговински центар и Пентагон 11. септембра 2001. важне банке података и више информационих система и линија цивилних и војних комуникација били су уништени или прекинути. Губитак информација и прекид комуникација повећали су ефекат напада. Према: Marlin S., Garvey M.: "Disaster-Recovery Spending on the Rise", *Information Week*, August 9, 2004, p. 26.

канале (радио-мостове). Електронски напад, генерално, има за циљ да доведе у питање расположивост система.

- *Кибер напад* – обично има као циљ један од захтева информационе безбедности. Ова врста напада уперена је против рачунара у мрежи, или саме мреже која се користи за приступ системима које напад циља. Инструменти кибер напада, тзв. кибер оружје (енгл. *cyber weapon*), обухватају велики број злонамерних или малициозних (енгл. *malware*)[259] информатичких програма, чији је задатак да заразе информациони систем противника са циљем да га оштете или украду разноврсне, а нарочито поверљиве или осетљиве информације (на пример, лозинке – *password[s]*, бројеве кредитних картица итд). Остали облици кибер напада искоришћавају протоколе које користе системи (нпр. TCP/IP) и њихове рањивости (грешке или слабости софтвера, неправилну конфигурацију хардвера и софтвера система или грешке настале у пројектним решењима), те на тај начин успевају да приступе информационом систему. Приступ систему често олакшавају и сами корисници система, у оним ситуацијама када несвесно бивају наведени да открију информације које су нападачу потребне, помоћу техника које се заснивају на рањивости „људског фактора".

Физички напади, иако усмерени против новог циља – кибер инфраструктуре[260] – не представљају новост међу претњама са којима се суочава друштво. Електронски напади, пак, представљају новину у развоју такозваног „не-смртоносног" оружја (осим EMP, које је познато од почетка нуклеарног доба). Електронски напад, неоспорно, има деструктиван потенцијал. Међутим, ефекти оваквог напада на кибер простор тренутно представљају непознаницу. Из расположивих извора података може се сазнати једино то да је електронско оружје за сада под сталном контролом државе (највероватније само једне – САД), која би га вероватно употребила (или га је користила)[261] само у случају отвореног конфликта.

Оружје кибер напада је, напротив, доступно свима – и развијеним земљама и земљама у развоју (Табела 3). У табели су дати подаци за други и трећи квартал 2008. године и трећи и четврти квартал 2009. године, који се односе на земље одакле

---

[259] Енглеска реч *malware* јесте кованица настала од појма malicious software (малициозни софтверски програм).

[260] Кибер инфраструктура, као што смо видели, може се сматрати синонимом кибер простора.

[261] Према непотврђеним изворима САД су га највероватније користиле током борбених дејстава на Косову 1999. године. Према: Hoffmann L.: "U.S. Opened Cyber-War During Kosovo Fight", *Washington Times*, October 24, 1999.

потиче највећи број безбедносних инцидената. Видимо да се редослед мења током времена. У другом кварталу 2009. године највећи број напада потицао је из Кине а затим из САД. Ако би за Кину рекли да се бави тим активностима из политичких разлога, слично објашњење може да се примени и на САД као и на Јапан који је у другом кварталу 2008. био највећи извор напада. Таква слика се донекле мења ако се погледа 2009. година у којој је Јапан тек на деветом месту али се у врху појављују земље као што су Јужна Кореја и Индија. Поред политичких разлога за извођење напада, један од најчешћих разлога је и директно прибављање финансијске користи као и индустријска шпијунажа.

Оружје кибер напада је економски приступачно и има потенцијално разарајући ефект на сва технолошки развијена друштва чије се благостање заснива на исправном функционисању кибер инфраструктуре и на уверењу да ће њен потенцијал, и у будућности, моћи да буде експлоатисан.[262]

Табела бр. 3*: Статистички преглед учесталости кибер напада по државама порекла*

	Country	% Traffic	Q2 08 %
1	China	26.85	8.90
2	United States	19.68	21.52
3	South Korea	9.37	2.25
4	Sweden	3.86	0.48
5	Japan	3.13	30.07
6	Brazil	2.64	1.53
7	Taiwan	2.54	2.21
8	Hong Kong	2.26	0.46
9	Germany	2.20	5.56
10	Russia	1.94	1.64
–	OTHER	25.53	–

Трећи и четврти квартал 2008. г.

	Country	% Traffic	Q1 09 %
1	China	31.35%	27.59%
2	United States	14.63%	22.15%
3	South Korea	6.83%	7.53%
4	India	3.93%	1.60%
5	Taiwan	2.32%	2.22%
6	Brazil	2.29%	2.60%
7	Netherlands	2.06%	1.16%
8	Mexico	1.96%	1.21%
9	Japan	1.95%	1.79%
10	Germany	1.93%	2.95%
–	OTHER	30.75%	–

Први и други квартал 2009. г.

Извор: "The State of the Internet – 3rd Quarter 2008", Akamai, http://www.akamai.com/stateoftheinternet, "The State of the Internet – 2nd Quarter 2009", Akamai, http://www.akamai.com/stateoftheinternet

[262] Слободан Петровић, у изјави датој 2001. за *Вести*, тврди: „Током НАТО агресије, Американци су планирали да отпочну кибер-напад на Србију, али им то није пошло за руком само због тога што информатичка технологија код нас (присутна у банкарству, полицији, војсци...) није у знатној мери међусобно повезана, па тако и није подложна овој врсти ратовања.“

У пракси је готово увек тешко утврдити да ли је одређени штетни догађај проузрокован намерним нападом, нехотичном људском грешком или кваром унутрашње компоненте система. Са гледишта управљача сервиса, разликовање између квара, инцидента или напада често је мање битно од изазване штете, барем гледано на „кратке стазе“. Другим речима, основни проблем управљача састоји се не толико у тражењу узрокâ догађаја, колико у оспособљавању система. Дистрибутивна мрежа електричне енергије може се прекинути због прозаичне људске грешке, тј. без било каквог спољашњег утицаја или, пак, због софистицираног кибер напада од стране непријатељске армије. У оба случаја резултат је исти: „угаснуће“ и последично нефункционисање сервиса или прекид свих система који су међусобно повезани и реципрочно међусобно зависни.

Информациони системи су данас изложени свим класичним претњама, као што су ватра, вода, експлозија и друге, али и специфичним, новим претњама, попут електронских и кибер напада.

Један број нових претњи или, прецизније речено, оне претње за чије је манифестовање неопходно постојање рачунарске мреже називају се кибер претњама, тј. безбедносним претњама у кибер простору. Под појмом „кибер претња“ експлицитно се подразумева „злонамерна употреба технологија које припадају кибер простору као инструмената претње, али и као циљева од стране великог броја актера – криминалаца, терориста, организација и држава“.[263]

Дакле, постоји једна специфична категорија претњи са префиксоидом „кибер“. Оне су, као и традиционалне претње, усмерене против ИК система и информација које су садржане у њима, али су извори ових претњи и средства неопходна за њихову експликацију везани за кибер простор. Другим речима, њихово манифестовање омогућено је стварањем глобалне рачунарске мреже. То је, дакле, њихово дистинктивно обележје.

У најопштијем смислу, кибер претња може се рашчланити на две компоненте: начин изазивања (средства и технике) и субјект (актер) претње. Начин

---

[263] Fischer E.: *CRS Report for Congress, Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, http://csrc.nist.gov

изазивања претње представља прави механизам претње, док је субјект претње особа или организација која иницира настанак претње или извршава акцију.

3.4. Средства и технике кибер ратовања

И поред тога што велике државе-нације данас у својим арсеналима имају наоружање велике разорне моћи, оне истовремено развијају и оружје за вођење кибер рата.

Дигитално оружје из арсенала кибер рата, са друге стране, доступно је и актерима са знатно мањим ресурсима од супер сила. Стратегијски посматрано, они могу да представљају претњу подједнаке разорне моћи. У том смислу Џејмс Адамс истиче: „Сједињене Америчке Државе су можда непоражена војна супер сила, али ова држава остаје без одбране када је у питању нов облик напада - кибер ратовање“.[264]

Николас Негропонте исто тако истиче да се природа наших средстава деструкције мења од физичких ка виртуелним.[265]

Кибер ратовање представља активност која се заснива на употреби широког спектра техника и инструмената за извршење напада на противничке ИК системе као и за манипулацију информацијама у офанзивне и дефанзивне сврхе.

У досадашњим истраживањима у подручју кибер безбедности највише се пажње посвећивало кибер нападима техничког типа и оним нападима у кибер простору који се заснивају на обмањивању других корисника кибер простора и злоупотреби њиховог поверења.

Осим различитих врста кибер напада, који, свакако, представљају један вид злоупотребе кибер простора, под методе и средства кибер ратовања можемо сврстати и покушаје зоупотребе кибер простора у односу на његову функцију средства за масовну комуникацију. У том смислу, спектру техника и иструмената који се користе у кибер ратовању, осим већ поменута два аспекта кибер напада, приписујемо и „пропаганду као чинилац кибер рата“, као посебну врсту претњи, с обзиром на њен деструктивни потенцијал у односу на државе, њихове грађане и

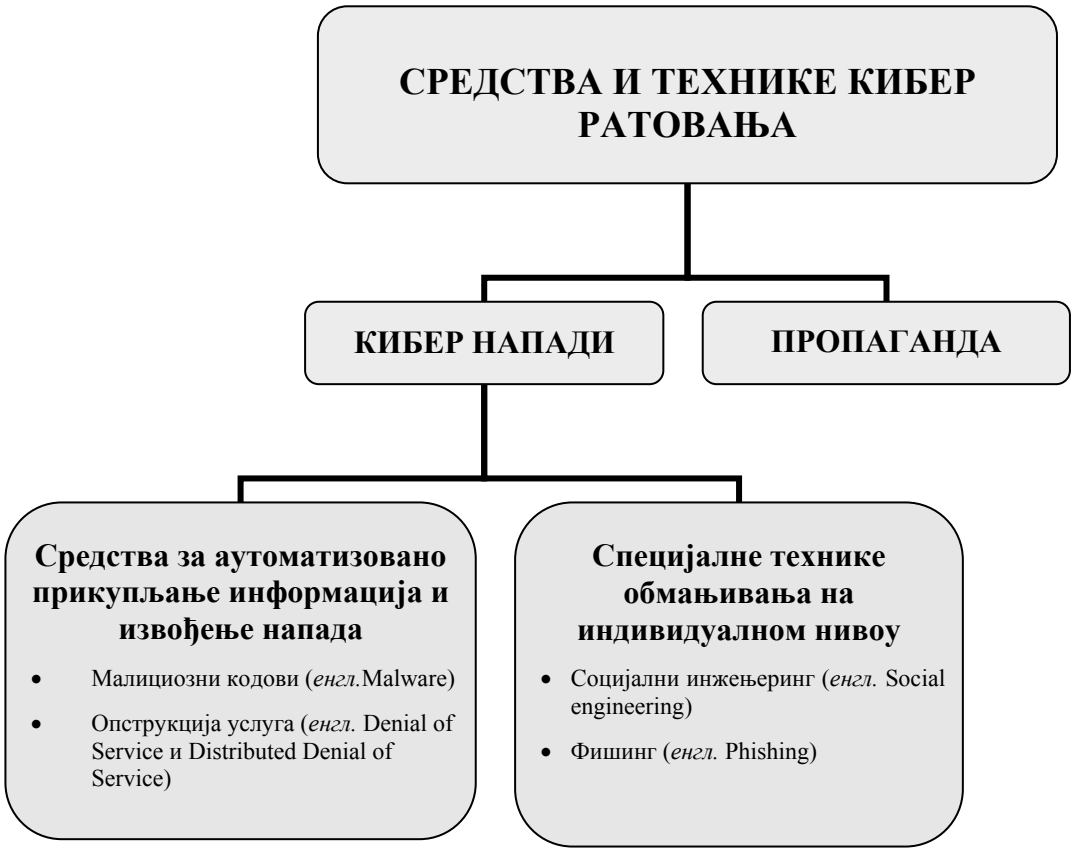
---

[264] Adams J.: “Virtual defense“, *Foreign Affairs*, May 2007, http://www.foreignaffairs.com/articles/57037/james-adams/virtual-defense

[265] Negroponte N.: *Being Digital*, Alfred A. Knopf Inc., New York, 2005, p. 11.

друштво у целини. У следећем схематском приказу покушали смо да, на основу увида у досадашња истраживања, али и властитих запажања, графички представимо једну, по нашем мишљењу систематичнију класификацију средстава и техника кибер ратовања.

Схема бр. 3: *Класификација средстава и техника кибер ратовања*



Ради бољег разумевања ризика од последица кибер ратовања, неопходно је описати најраспрострањеније врсте напада, оне који се заснивају на коришћењу обмане и оне аутоматизованог типа, али и пропагандне активности којима се кибер простор злоупотребљава као средство масовне комуникације.

3.4.1. Средства за аутоматизовано прикупљање информација и извођење напада

Уопште узев, можемо тврдити да кибер напади користе било који облик слабости или рањивости (техничке или људске) система жртве. Када су фаворизовани техничким рањивостима, улазе у категорију „средстава за аутоматизовано прикупљање информација и извођење напада“. Ако се ослањају на људски фактор, сврставамо их у категорију „специјалних техника обмањивања на индивидуалном нивоу“.

Тешко је набројати све могуће нападе базиране на техничким рањивостима противника, с обзиром на то да су њихов квалитет и квантитет ограничени једино инвентивношћу нападача. Осим тога, реални напади се често изводе комбинацијом различитих техника, што отежава њихову класификацију. Једна од могућих категоризација садржала би следеће технике: *interception*, *man in the middle attack*, *replay*, *spoofing*, *buffer overflow*, *saturation and delay*, *embedded attack*.[266] Опис свих наведених техника које се користе за извођење ове врсте кибер напада захтевао би врло специјализовано техничко знање. Из тог разлога су у раду обрађени само *embedded attack* и *saturation and delay attack*, будући да су најзаступљенији у последњих неколико година. У прву категорију спадају напади који се изводе помоћу тзв. малициозних кодова (*енгл*. malware attack), а у другу напади усмерени на опструкцију услуга циљаног рачунарског система (*енгл*. denial of service attack – DoS) или, у најновијем облику, дистрибуирани напади усмерени на опструкцију услуга (*енгл*. distributed denial of service attack – DDoS).

3.4.1.1. Малициозни кодови

Термин *малвер* (*енгл.* malware)[267] означава посебну категорију информатичких програма чији је циљ да оштете рачунарски систем корисника. Малициозни кôд инфицира рачунарски систем путем неауторизованих и за корисника неочекиваних процеса. Постоје различите врсте малициозних кодова, али њихова композиција[268] и константна еволуција отежавају кохерентну класификацију. У ову групу могу се сврстати следећи информатички програми: *вируси* (*енгл.* virus), *црви* (*енгл.* worm), *тројански коњи* (*енгл.* trojan horse), *споредна врата* (*енгл.* backdoor)*, програми за неауторизовано праћење активности корисника* (*енгл.* spyware), *програми за праћење и снимање оперативног рада корисника рачунара на нивоу микрооперација* (*енгл.* keylogger) и *отмичари* (*енгл.* hijacker).

---

[266] Berg C.: "High-Assurance Design: Architecting Secure and Reliable Enterprise Applications", *Methods of Computer System Attacks*, http://www.awprofessional.com

[267] Термин потиче од споја *енгл*еских речи „malicious" и „software", тако да је његов дословни превод „малициозни програм" или „малициозни кôд".

[268] Најчешће су сачињени од више модуларних и међусобно зависних делова.

Вирус

Вирус је део сложенијег кода који се шири унутар једног рачунара или рачунарске мреже, копирајући се унутар других програма или у одређеном делу хард-диска рачунара, тако да се може активирати отварањем инфицираног фајла. Вирус је у стању да, након инсталирања софтвера, саморепликацијом зарази остале фајлове у рачунару или мрежи, најчешће без знања корисника. Вирус обично садржи неколико „инструкција“ и има циљ да изврши минималан број једноставних операција а да при том остане невидљив.

Назив „вирус“ потиче од евидентних сличности са његовим биолошким имењаком. Вирус, сâм по себи, није програм који се аутономно инсталира, као што и биолошки вирус није сâм по себи облик живота. За разлику од ћелије, он не може да се репродукује, тј. није жив, већ је један фрагмент ДНК. Да би се репродуковао, вирус мора да уђе у живу ћелију и да искористи њен функционални апарат. На исти начин информатички вирус, да би се активирао, мора заразити програм или редослед шифре, која се аутоматски активира током информатичког процеса. Аналогно биолошком вирусу, и информатички вирус користи технику убацивања своје копије у инсталациони програм. На овај начин, када корисник активира програм, прво се, неприметно, активира вирус, а затим и програм. Корисник најчешће, посматрајући рад програма, није у могућности да примети присуство вируса нити његову активност у смислу извршавања операција које се налазе у његовој шифри. Вирус, пратећи „инструкције“, обично производи сопствене копије, ширећи на тај начин епидемију, али може имати и много штетније задатке (брисање или уништавање фајлова, форматизовање хард-диска, отварање *споредних врата* и слично).

Термин „вирус“ је у информатичком смислу први употребио Фред Коен (Fred Cohen), студент Универзитета Јужне Калифорније, у чланку објављеном 1984. године под насловом „Експерименти са рачунарским вирусима“ (“Experiments with Computer Viruses”).[269]

Први рачунарски вирус који се појавио у свету био је програм звани „Elk Cloner“. Створен је 1982. године, а инфекција овим вирусом ширила се разменом

[269] “Computer viruses now 20 years old”, *BBC on line*, November 10, 2003, http://news.bbc.co.uk

дискета. Овај начин заразе био је најчешћи током осамдесетих и почетком деведесетих година XX века.

Половином деведесетих година, због ширења Интернета, основни начин преношења заразе постала је размена фајлова путем глобалне информационо-комуникационе мреже (и-мејл и остали програми за комуникацију и размену фајлова међу корисницима). У овом периоду су се појавили и такозвани макровируси, чије су „инструкције“ написане речником скриптинг-програма (*енгл.* scripting program), као што су „MS-Word“ и „Outlook“. Ови вируси су усмерени, посебно, на инфицирање различитих верзија „Мајкрософтових“ (“Microsoft”) програма путем размене докумената.

Сматра се да сваки оперативни систем на који се дозволи инсталација неауторизованих програма постаје потенцијална мета вируса али, битно је нагласити, нису ни сви оперативни системи једнако рањиви. Оперативни системи „Мајкрософта“ највише су погођени вирусима, зато што су и најраспрострањенији међу такозваним „нестручним“ корисницима. У сваком случају, чињеница је да не постоје системи који су потпуно, или теоријски, имуни на вирусе.

У погледу структуре може се рећи да је сваки вирус састављен из најмање две компоненте, које су довољне да осигурају његову саморепликацију. Прва компонента подразумева функцију претраге фајла-домаћина, у циљу откривања да ли он већ садржи једну копију вируса, како би се избегло поновно инфицирање истог фајла. Друга компонента подразумева функцију инфицирања, са задатком да копира шифру вируса унутар сваког фајла селектованог претходном функцијом претраге. На тај начин се вирус активира сваки пут када се отвори инфицирани фајл.

Многи вируси су пројектовани тако да извршавају и друге активности осим сопствене репродукције. У том случају они садрже још две компоненте:

- функцију активације, која садржи основне критеријуме на основу којих вирус „одлучује“ да ли да изврши напад (нпр. датум или достизање одређеног задатог броја инфицираних фајлова);
- једну или више додатних функција (тзв. *payload*), које се састоје од редоследа инструкција за наношење штете систему у виду брисања

датотека или диска, приказивања нежељених порука на екрану, крађе података итсл.[270]

Неки вируси могу да буду криптовани[271] и могу да промене алгоритме или кључ шифровања сваки пут када се покрену. Овакви вируси најчешће садрже:

- функције дешифровања, са инструкцијама за дешифровање кода вируса;
- функцију шифровања – обично је она сама криптована тако да садржи процес којим се шифрује свака копија вируса;
- функцију мутације, која мења функцију шифровања и дешифровања за сваку нову копију вируса.

На основу карактеристика које имају, вируси се могу поделити на: полиморфне вирусе, *exe*-вирусе, *com*-вирусе, *companion*-вирусе, *boot*-вирусе, макровирусе, ретровирусе (вирус који инфицира антивирусне програме, чинећи их неефикаснима; назив потиче од биолошких ретровируса, који су у стању да нападну имунолошки систем, попут вируса AIDS-а) и мултиплатформне вирусе. Недовољно познавање механизама ширења вируса, али и начин на који мас-медији често третирају овај аргумент, фаворизују ширење како правих вируса тако и лажних – такозваних *hoax*-вируса.[272]

---

[270] *Threat Encyclopedia*, http://www.eset.com/threat-center/pedia/p.htm

[271] Криптографија је наука која се бави методима очувања тајности информација. Када се личне, финансијске, војне или информације од државног значаја преносе са места на место, оне постају рањиве на прислушкивачке тактике. Овакви проблеми се могу избећи криптовањем (шифровањем) информација које их чине неупотребљивим уколико доспеју у посед противничке стране. Шифра и дигитални потпис су најчешће криптографске технике које се користе да би се имплементирали безбедносни сервиси. Основни елемент који се користи назива се шифарски систем, или алгоритам шифровања. Сваки шифарски систем обухвата пар трансформација података, које се називају шифровање и дешифровање. Шифровање је процедура која трансформише оригиналну информацију (отворени текст) у шифроване податке (шифрат). Обратан процес, дешифровање, реконструише отворени текст на основу шифрата. Приликом шифровања, поред отвореног текста, користи се једна независна вредност, која се назива кључ шифровања. Трансформација за дешифровање користи кључ дешифровања. Број симбола који представљају кључ (дужина кључа) зависи од шифарског система. Криптоанализа је наука која се бави разбијањем шифара, декодирањем, заобилажењем система аутентификације – уопште, „проваљивањем“ криптографских протокола. Различите технике криптоанализе називају се напади. Према: Marić I.: *Sustav za privlačenje i detekciju napadača*, Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, Zagreb, 2006, str. 41.

[272] Реч је о порукама које обавештавају о ширењу новог „страшног“ вируса са катастрофалним последицама и траже да се обавештење проследи свим познатим особама. И ови, лажни аларми имају своју тежину. Иако нису штетни, они повећавају количину нежељене поште и шире неистините информације.

Анатомија Интернета дозвољава рачунарским вирусима (или другим малициозним кодовима) да се много ефикасније шире него што се то раније мислило. Поред тога, Интернету недостаје оно што Пастор-Саторас означава, по аналогији са људским окружењем, као „улаз заразе“ – чијом контролом је могуће ограничити ширење болести на веће делове популације. Управо та карактеристика Интернета, која га чини тако отпорним на случајне прекиде веза, чини га рањивим на интелигентно вођене нападе.[273]

Црв

Под називом *црв* подразумева се посебна категорија малициозних програма који се саморепродукују без било каквог учешћа корисника. Црв је сличан вирусу али, за разлику од њега, не мора да се везује за друге програме ради ширења и умножавања, већ се активира аутоматски и шири захваљујући мрежи.

Црв се најчешће активира истовремено са подизањем рачунара на радни ниво и остаје активан све док се рачунар не искључи. За дистрибуцију ове врсте инфекције најчешће се користи електронска пошта. Злонамерни програм у инфицираном рачунару сакупља меморисане адресе електронске поште и на њих шаље копију себе самог у виду прилога електронској поруци (*attachment*). Поруке које садрже црв обично користе технике *социјалног инжењеринга*[274] како би навеле примаоца да отвори прилог. У највећем броју случајева назив и екстензија приложеног фајла дозвољавају црву да се камуфлира као неизвршни програм (фајл, на пример, има екстензију слике или филма). Поједини црви искоришћавају софтверске грешке (*енгл.* bug) најпопуларнијих програма за размену електронске поште (попут програма „Microsoft Outlook Express“), тако да се аутоматски активирају у тренутку приказивања инфициране поруке.

Сви напреднији црви фалсификују адресу пошиљаоца и на тај начин стварају непријатан колатерални ефект ширења инфицираних порука – антивирусни програми инсталирани на серверу враћају заражену поруку на адресу са које је послата али, с обзиром на то да је она лажна, заражена порука стиже неком другом, а не правом пошиљаоцу поруке електронске поште. Црви могу, такође, за ширење да

[273] Barabasi A.: *Strength is weakness on the Internet*, http://physicsworld.com/cws/article/news/2806

[274] Техника социјалног инжењеринга објашњена је у одељку: 3.4.2.1. Социјални инжењеринг.

користе и датотеке које размењују корисници у локалној или глобалној рачунарској мрежи. У овом случају се малициозни програм имплементира међу фајлове које размењују корисници-жртве, приказујући се као врло тражени програм (најчешће као пиратска копија веома скупог програма), како би на тај начин навео корисника да их преузме на свој рачунар и инсталира.

Инфекција црвом најчешће има два негативна ефекта: проузрокује директну штету, активирањем на инфицираном рачунару, и индиректну штету, која произлази из техника које се користе за ширење инфекције. Једноставан црв, сачињен само од инструкција за репликацију, сâм по себи не ствара значајнију непосредну штету. Међутим, ови програми се често, у настојању да не буду откривени, сукобљавају са функционисањем софтвера за заштиту оперативних система, као што су антивирусни и фајервол[275] програми, ометајући тако нормално функционисање нападнутог рачунара. Већина црва, као и вируса, садржи *payload*, чији је једини циљ да оштети заражени систем. Често, међутим, црв функционише као преносилац скривене инсталације осталих малициозних програма, попут *споредних врата* или *keylogger* програма, који касније могу бити искоришћени од стране неког другог црва или злонамерних актера у кибер простору (најчешће *крекера*).[276]

Индиректна штета произлази из колатералних ефеката инфекције великог броја умрежених рачунара на исправно функционисање ИКТ инфраструктуре. Као што је већ поменуто, ширење црва ствара огромну количину нежељених и деструктивних електронских пошиљки. Црви који искоришћавају рањивости

---

[275] У подручју рачунарских мрежа фајервол (*енгл*. firewall) је пасивна компонента периметарске одбране, која може да обавља и функцију везе између два стабла мреже или више њих. Обично се мрежа дели на две или више подмрежа: једна, такозвана спољашња, обухвата цео Интернет, док друга, унутрашња, или LAN (Local Area Network), обухвата мању или већу секцију локалних рачунара. У неким случајевима постоји потреба за стварањем треће подмреже тзв. демилитаризоване зоне (demilitary zone – DMZ). Она садржи системе који морају бити изоловани из мреже, али и заштићени од фајеревола. Захваљујући својој стратешкој позицији, фајервол је најбоље место за мониторинг пакета у транзиту. Његова основна функција је да створи филтер за улазне и излазне конекције и да на тај начин подигне ниво безбедности мреже. Према: *Рачунарски речник Микро књиге*, http://www.mk.co.yu/pub/rmk/detalj1.php?EngOdrID=2304.

[276] Крекер је особа која се бави крековањем, тј. разбијањем заштитног кода софтвера. У питању су лозинке за улазак у заштићене информационе системе, као што су системи банака, болница, полиције и сличних институција, или кодови који штите софтвер или другу интелектуалну својину од нелегалног копирања. О активностима крекера видети више у одељку: 4.3.1. Хакеризам и крекеризам.

одређених програма узрокују њихову дисфункционалност, а тиме и нестабилност оперативног система, као и гашење или рестартовање нападнутог рачунара.[277]

Тројански коњ

Изворно су *тројанским коњем* називани програми који су били прикључивани регуларним апликацијама да би у позадини обављали одређене нерегуларне операције, најчешће злонамерне. Данас се под тројанским коњем (или чешће – тројанцем) подразумева знатно шири спектар злонамерних програма.

Неформално би се тројанац могао дефинисати као врста злонамерног програма који не може да се самореплицира. Ова врста малициозног програма углавном се састоји од кода који извршава одређене злонамерне функције. Најчешће је тројанац убачен у неку другу апликацију, што умногоме отежава његову детекцију. Тројански коњ је, стога, назив и добио по аналогији са чувеним тројанским коњем, јер се његове штетне функције крију унутар наизглед корисног програма.

Будући да тројанац нема способност саморепликације, његов кôд мора бити умишљајно послат жртви. Продор тројанца на кориснички рачунар обично се постиже на један од следећа два начина:

1) Прерушавањем – на многим сајтовима глобалне рачунарске мреже посетиоцима се нуде бесплатни програми или апликације (корисни софтвери, видео-игре, шале и слични садржаји) који, у ствари, садрже прикривеног тројанца. Корисник који преузима овакве фајлове са Интернета или их прима електронском поштом у опасности је да инфицира сопствени рачунар овом врстом малициозног програма. Понекад се преузимањем фајлова не повлачи директно сâм тројанац, већ линк ка другој *web*-страници на којој је он стациониран.

---

[277] Према Шнејеру, црв Msblast (познат и под именом Lovsan) у великој мери је допринео „испаду информационе инфраструктуре из система“ који се догодио 14. августа 2003. на целом истоку САД и трајао 24 сата, а чије су се последице осећале и наредна три дана. Посебно погођен је био град Њујорк. Црв, који је у тренутку хаварије погађао рачунаре Северне Америке, према Шнејеру, онемогућио је нормално функционисање SCADA система који управља и контролише процес производње електричне енергије. Schneier B.: *Internet Worms and Critical Infrastructure*, 2003, http://www.schneier.com

2) Груписањем са црвима и вирусима – понекад се за ширење инфекције могу користити црви или, ређе, вируси. У овом случају формира се мултикомпонентни црв, при чему је „традиционални“ тројанац један његов део, тј. независна компонента. У овом случају црв се користи само као „превозно средство“.

Инсталирањем и активирањем одређеног програма неопрезан корисник несвесно инсталира и активира скривени кôд тројанског коња, који се затим користи за неприметан улазак нападача у рачунар жртве. На тај начин агресор стиче приступ свим подацима ускладиштеним у рачунару жртве. Тројанац се, према томе, користи за прикупљање поверљивих информација са инфицираних рачунара или, једноставно, за наношење штете.

Циљеви агресора могу бити усмерени на прикупљање приватних информација и осетљивих података, поверљивих докумената, пројеката или фотографија, података о кредитним картицама, података везаних за лозинке електронске поште, *web*-услуге, адресе електронске поште. У неким случајевима агресор користи инфицирани рачунар за извршавање илегалних радњи: манипулација, скенирања или интерполирања у друге системе мреже или Интернета.

Тројански коњ се не шири аутономно као вирус и црв, већ захтева директну интервенцију нападача – најчешће слањем електронске поште. Чест је случај да жртва нехотично инсталира тројанац на сопствени рачунар, с обзиром на то да су ове „замке“ скривене у привлачним програмима, попут недозвољених копија видео-игара и осталих софтвера који су скупи у оригиналној верзији. Многи корисници тврде да никада нису отворили или „скинули“ софтвер са непознатих сајтова. Употребом техника социјалног инжењеринга, међутим, препредени хакери могу да преваре већину корисника, наводећи их да преузму опасан софтвер.[278]

Постоје многе врсте тројанаца, а они се, уопштено, сврставају у седам основних категорија. Битно је нагласити да је тешко сврстати одређени тројанац

[278] Septer.troj је пример тројанца који се ширио техникама социјалног инжењеринга. Тројанац је дистрибуиран у САД путем електронске поште током октобра 2001. године. Овај тројанац био је убачен у лажни формулар Црвеног крста за помоћ жртвама једне несреће. У пропратном писму је од прималаца формулара тражено да га попуне и упишу број кредитне картице. Тројанац би, након тога, дешифровао податке и слао их нападачу. Према: GFI white paper, http://www.gfi.com/whitepapers/network-protection-against-trojans.pdf.

само у једну групу, пошто сваки од њих има заједничке карактеристике са осталим категоријама.

Најчешће коришћени тројанци су они који омогућавају приступ са дистанце (*енгл.* remote access), јер нуде агресору комплетну контролу над нападнутим рачунаром. Основна намера нападача је, дакле, да употребом ове врсте малициозних програма добије комплетан приступ нападнутом рачунару, то јест фајловима, приватним разговорима, личним подацима итд. Остале категорије тројанаца су: тројанци за слање података (лозинки, редоследа коришћених типки на тастатури итд), деструктивни тројанци, тројанци за омогућавање напада типа *лишавање услуге*, *proxy*-тројанци, тројанци за дестабилизацију безбедносних софтвера и други.

Споредна врата

Споредна врата су програми који омогућавају неауторизовани приступ систему на којем се налазе. Најчешће се шире у комбинацији са тројанским коњем или црвом, али се понекада и намерно инсталирају на рачунар, од стране ауторизованих корисника, како би могли да буду употребљени у хитним ситуацијама за оправдан приступ систему у случају, на пример, заборављања корисничког имена или лозинке.

Споредна врата можемо упоредити са „улазом за запослене“. Она омогућавају делимично или комплетно заобилажење сигурносне процедуре у одређеном систему. Споредна врата намерно може оставити отвореним власник система ради бржег приступа и лакшег одржавања информационе инфраструктуре, али је чешћи случај да их „отварају“ крекери са намером да поремете систем. Ова врата могу аутономно створити и одређене врсте малвера (вируси, црви и тројански коњи), како би на тај начин дозволили агресору да са дистанце преузме контролу над рачунаром, без ауторизације власника.

Један од познатих примера споредних врата јесте програм *споредна рупа* (Back orifice), који активира улаз у систем на који се инсталира, дајући тако могућност контроле система било коме ко зна IP-адресу рачунара. Осим тога што су врло опасна за интегритет информација унутар система на који се инсталирају, „споредна врата“ се могу искористити и за извођење напада *дистрибуираног лишавања услуге*.

Програми за неауторизовано праћење активности корисника

Програм за неауторизовано праћење активности корисника назив је за софтвер који се користи за прикупљање информација из система на којем је инсталиран, са задатком да их пренесе заинтересованом примаоцу. На овај начин се кришом прикупљају разноврсне информације, од навика корисника у навигацији Интернетом до његових лозинки и криптографских кључева.

Шпијунски програм прикупљене информације шаље заинтересованом примаоцу, на пример комерцијалној организацији, која их користи за циљано слање рекламе надзираном кориснику. Постоје, пак, и програми за сакупљање података, који се могу инсталирати само уз дозволу корисника. Они се не могу квалификовати као *шпијуни* уколико је кориснику обзнањено који су подаци предмет прикупљања и под којим условима.

У ширем смислу, термин „шпијун“ се често користи и за дефинисање широког спектра малициозних програма различитих функција: слања нежељених реклама, мењања почетне странице или листе омиљених страница у програмима за претраживање Интернета, или илегалних активности, као што су упућивање на лажне сајтове за електронску трговину (фишинг) или инсталације апликација за позивање телефонских бројева са посебном тарифом (*енгл.* dialer). Шпијунски програми, за разлику од вирусâ и црвâ, не могу се ширити аутономно, већ захтевају интервенцију корисника да би се инсталирали.

Као и тројанац, и шпијун се уходаним техникама социјалног инжењеринга може инсталирати на рачунар без знања корисника. Многи програми који се нуде бесплатно на Интернету у ствари су малвери овог типа – софтвер, дакле, није бесплатан, већ се плаћа инвазијом на приватност корисника. У неким случајевима сама апликација која обећава чишћење од шпијуна садржи управо овај малициозни програм.

Инсталација шпијунског програма може се извршити на још подмуклији начин – посетом *web*-страницама направљеним тако да искористе евентуалне слабости претраживачког програма (*енгл.* browser) и на тај начин дозволе аутоматско инсталирање опасних апликација. Шпијунски програми могу бити део *payload*-функције малициозног програма са аутоматским умножавањем, као што је црв, мада је овај начин изазивања инфекције тренутно ређе у употреби.

Многи шпијуни се активирају само у тренутку покретања програма са којим су инсталирани, па тако гашењем програма престаје и њихова активност. Други, пак, имају инвазивније понашање, слично многим тројанцима или црвима: модификују оперативни систем рачунара тако да се активирају сваки пут када се укључи рачунар. Шпијун, на првоме месту, представља претњу за приватност корисника, с обзиром на то да без дозволе сакупља информације о његовим навикама на Интернету: просечно време посете, време конектовања, најчешће посећиване *web*-странице и коришћене и-мејл адресе. Прикупљене информације шпијунски програм одашиље рачунару нападача. Рачунар агресор након тога, у аутоматизованом процесу, шаље повратне циљане рекламе, које се заснивају на прорачуну преференција из сакупљених података. Рекламе се могу појавити у облику *banner pop up*-а[279] на *web*-сајтовима који се најчешће посећују или у програмима који садрже шпијуна или, у инвазивнијим случајевима, у виду нежељене електронске поште (*енгл*. spam).

Ова врста малициозних програма носи са собом и последице за рачунар на који су инсталирани. Штете иду од смањења брзине Интернет-конекције, окупације циклуса CPU и заузимања простора у RAM меморији, до нестабилности или блокирања система. Још један симптом тешке инфекције шпијунским програмима јесте отежано конектовање или конектовање без знања корисника. Ове последице су колатерални ефекти главног задатка шпијуна, а то је прикупљање информација. Ниједан шпијунски програм нема за циљ директно оштећење система на који је инсталиран, јер му је он неопходан за прикупљање података и њихово слање. Систем, међутим, не функционише правилно у присуству великог броја шпијуна, али овакве неправилности корисник често приписује грешкама у оперативном систему, хардверским проблемима и, нарочито, вирусима, те предузима радикалне акције реформатизовања хард-диска и поновне инсталације оперативног система, што са собом носи губитак времена и новца. Одређени шпијунски програми, чак, симулирају грешке у исправним апликацијама како би навели корисника да посумња

[279] Banner pop up је врста рекламе која има циљ да повећа доступност информација о одређеним производима. Присуство pop up-а на одређеном сајту манифестује се аутоматским отварањем нових прозора browser-а са рекламним садржајем.

у исправност заштитног [*firewall*] система рачунара, те да га уклони и шпијунском програму дозволи приступ Интернету.

Најбоље оружје против шпијуна представља сумња у сваки софтвер који се на Интернету нуди бесплатно. Као што је наглашено, најчешћи начин преноса ових малвера јесте убацивање у веома популарне програме. Такође, превентивно деловање подразумева избегавање сумњивих сајтова који нуде пиратерију, као и посете линковима издвојеним у непожељној пошти.

Додатни ниво заштите постиже се инсталацијом *firewall*-а, који онемогућава приступ сумњивим апликацијама на Интернету. Присуство антивирусних програма није довољно за заштиту од шпијуна, с обзиром на то да они нису нити вируси нити црви, већ је неопходна употреба посебних програма који омогућавају откривање њиховог присуства и брисање из система.

Програми за праћење и снимање оперативног рада корисника рачунара на нивоу микрооперација

Назив *keylogger* користи се за означавање инструмената који су у стању да прате и снимају целокупан рад корисника рачунара. Ови програми не само да меморишу сваку команду откуцану на тастатури жртвиног рачунара, већ на нападачевом рачунару израђују и слике радне површине нападнутог рачунара. Нападач је, на тај начин, у могућности да открије којим се све апликацијама корисник служи. Такође, ови програми „хватају“ и информације о жртвином кретању Интернетом и шаљу дневнике њене активности нападачу путем електронске поште.

Постоје две врсте *keylogger*-а:

1) хардверски – физички се повезују или за кабл између тастатуре и рачунара или са тастатуром рачунара. Врло су ефикасни, јер се лако инсталирају, а нападнути систем није у стању да примети њихово присуство;

2) софтверски – реч је о програмима који контролишу и меморишу редослед типки које корисник притиска, а затим их шаљу другом рачунару. Ова врста *keylogger*-а често се преноси и инсталира путем црва или тројанаца примљених

преко Интернета и њихов је циљ да украду лозинке и бројеве кредитних картица са нападнутог рачунара.[280]

Отмичар

Отмичар је збирни назив за посебну врсту програма чија је карактеристика присвајање контроле над апликацијама за навигацију у мрежи (нарочито над програмима за приступање Интернет-страницама, такозваним *browser*-програмима) и изазивање аутоматског отварања нежељених *web*-страница. Под овај назив, дакле, сврставају се малициозни програми који преузимају контролу над програмима за приступање Интернету, са циљем преправљања почетне приступне странице (*енгл*. homepage) те тренутног повезивања нападнутог рачунара са нежељеним сајтовима.

У системима „Windows“ *отмичар* најчешће делује на регистре система (што нестручним корисницима знатно отежава његову идентификацију). Овај малициозни програм може да коегзистира и да истовремено функционише са другим врстама малициозних програма. На пример, преправка система у сврху отмице може се извести употребом тројанског коња. У другом сценарију отмичар може усмерити *browser* на одређену *web*-страницу у циљу изазивања другачије врсте напада (*dialer*, вирус итд).

3.4.1.2. Опструкција услуга

Кибер напади под називом *опструкција* (*лишавање*) *услуге* (Denial of service – DoS) и *дистрибуирана опструкција услуге* (Distributed denial of service – DDoS) имају за циљ да онемогуће клијенте или организацију да користе услуге рачунарске мреже или информационих ресурса. Опструкција електронских услуга постиже се нападом на системе који омогућавају те услуге (на пример, нападом на сервер на којем су ускладиштени *web*-сајтови или на сервер електронске поште). Ефекти аналогни онима који настају услед напада DoS могу се догодити и случајно, као последица квара или лошег управљања мрежом.

Лишавање услуге и дистрибуирано лишавање услуге јесу врсте напада које циљају на доступност информација, а не на њихову поверљивост. Након ових напада

[280] Према: *Threat Encyclopedia*, http://www.eset.com/threat-center/pedia/p.htm.

најчешће нема крађе информација или осталих губитака информација поверљиве природе. Основна штета узрокована нападом DoS испољава се у времену које је потребно утрошити да би се нападнути систем поновно оспособио. У случају напада на економске организације, пак, последице се могу испољити у виду економских губитака или нарушавања имиџа организације због прекида услуга корисницима.

Најчешће коришћен метод за извођење ове врсте напада јесте излагање рачунара или рачунарских мрежа огромном броју захтева[281] концентрисаних у кратком временском периоду. У прошлости је за извођење ове врсте напада било неопходно имати на располагању велики број актера, саучесника, приправних за координиран напад уз помоћ специфичних програма. Данас је процес напада аутоматизован, тако да нема потребе за умишљајним учешћем трећих лица. Напад дистрибуираног лишавања услуге започиње тако што нападач присваја контролу над првим рачунаром, који постаје „мастер“ напада. Преко мастера се хиљаде других рачунара инфицирају црвом или *bot*-ом[282] и они постају такозвани „зомбији“.

Зомби-рачунар сада може да изврши било коју акцију предвиђену програмом црва, коју позивањем једне једине команде са дистанце иницира нападач а да, при том, легитиман корисник рачунара тога не буде свестан. Коришћењем ове изузетно једноставне операције хиљаде инфицираних рачунара (који творе компромитовану рачунарску мрежу *botnet*) могу да истовремено покрену напад DDoS против циља који је изабрао нападач. Зомби-рачунар се може испрограмирати и тако да омогући отварање *споредних врата* унутар локалне мреже организације којој припада рачунар и, на тај начин, депласира све примењене безбедносне мере организације. [283]

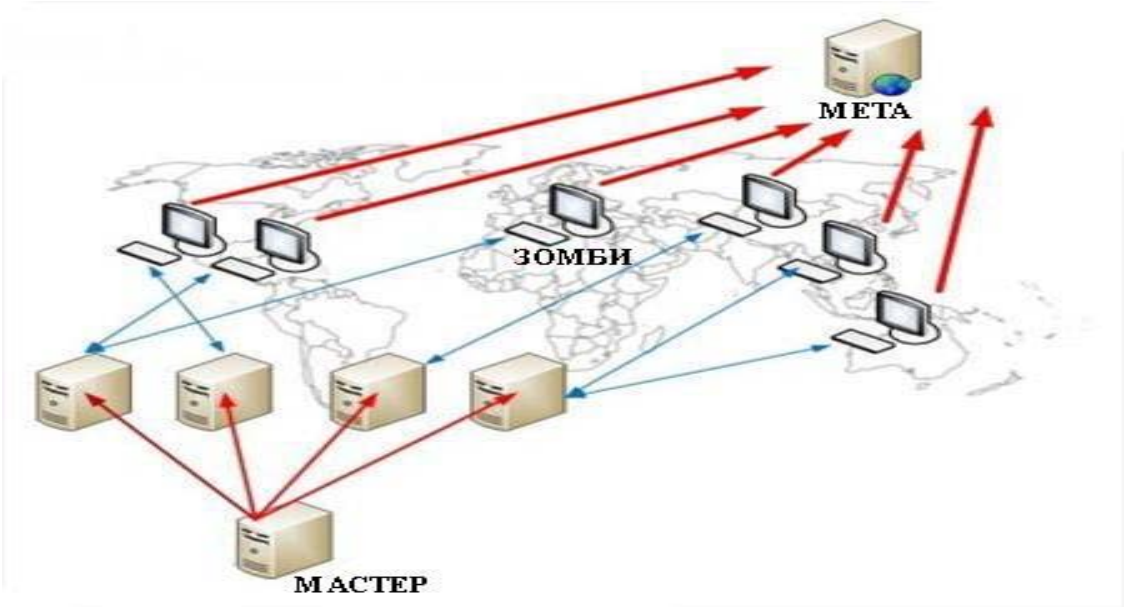
---

[281] Обично се користе поруке електронске поште, захтеви за приступ web-страницама и слично.

[282] Бот (*енгл*. bot, скраћеница од robot) јесу програми који се кришом инсталирају на рачунар жртве са циљем да неауторизованом кориснику омогуће контролу са удаљених локација (remote control). Бот-програми су пројектовани за стварање компромитованих рачунарских мрежа, такозваних bot network, или botnet, које нападач може користити за извођење координираних кибер напада.

[283] Један од скоријих случајева коришћења botnet-а за криминалне циљеве догодио се у Холандији 2005. године. Полиција је ухапсила две особе које су помоћу тројанског коња (званог „Toxbot“) успеле да створе изузетно раширен botnet, користећи га, затим, за изнуду новца од америчких предузећа.[283] У тренутку хапшења ботнет је био сачињен од око 1,5 милиона инфицираних рачунара. Парадоксално, без обзира на искључење мастер-чвора које је уследило након хапшења, постоје индиције да се исти botnet и данас шири. Проблем је у томе што bot-програми, уколико се не елиминишу са заражених рачунара, настављају да аутоматски истражују мрежу, са циљем инфицирања других рачунара. Према: Kaiser G.: *Dutch Botnet Bigger Than Expected*, 2005, http://informationweek.com

Схема бр. 4: *Модел botnet мреже*



Случај холандског *botnet*-а из 2005. године потврдио је значај који безбедносна култура индивидуалних корисника Интернета има на безбедност глобалне мреже. Распрострањеност компромитованих мрежа би била значајно мања када би корисници глобалне мреже употребљавали основне инструменте за заштиту својих рачунара, као што су антивирусни програми.

Да подсетимо, и Први кибер рат који се водио у Естонији током априла 2007. године био је заснован на нападима који су извођени техником DDoS. Овај догађај је подстакао интензивне расправе о безбедности кибер простора на међународном нивоу и означио својеврсну прекретницу у начину сагледавања савремених конфликата.

3.4.2. Специјалне технике обмањивања на индивидуалном нивоу

3.4.2.1. Социјални инжењеринг

Изразом *социјални инжењеринг* (*енгл*. social engineering) означава се врста напада при којој се нападач не служи информатичким техникама, већ покушава да путем комуникације наведе жртву да прекрши безбедносне норме или процедуре а да, при том, не примети да је изманипулисана. Могло би се рећи да је социјални инжењеринг „уметност“ искоришћавања људског понашања ради нарушавања кибер

безбедности.[284] Ова техника се не може поистоветити са техником „контроле ума“, јер се њоме угрожена особа не наводи на вршење акција које одступају од њеног уобичајеног понашања.

Социјални инжењеринг се заснива на чињеници да људски фактор, као централни елемент у информационо-комуникационој инфраструктури (не постоје рачунари или мреже који се не заснивају на учешћу човека) уједно представља и њену најслабију компоненту. Често се каже да је најсигурнији рачунар онај који је искључен или онај који није прикључен на мрежу. Чињеница да га било ко може укључити и повезати у мрежу значи да је чак и угашен рачунар рањив. С обзиром на то да је човек неопходан за рад рачунара, јасно је да слабост овог елемента кибер безбедности јесте и извор универзалне рањивости информационих система: онај ко има приступ било којем делу система, физички или електронски, представља потенцијалну претњу за безбедност тог система.

Међу различитим методима који се користе у циљу навођења једне особе да изврши одређену радњу у корист неке друге особе, основни се своди на формулисање директног и личног захтева-молбе. Иако овај метод, по правилу, има низак процент успешности, он је најједноставнији и директан: жртва тачно зна шта се од ње тражи.

Сложенији приступ укључује потенцијалну жртву у добро осмишљен сценарио. У присуству наизглед објективних разлога и морално прихватљиве мотивације, имајући на располагању више елемената у односу на једноставну молбу, нападач повећава шансе да се циљана особа понаша по његовој жељи. Коришћење оваквог приступа захтева бољу припремљеност агресора. Он готово увек мора добро познавати жртву и околности у којима се жртва налази, тј. контекст ситуације у којој напада.

Фингирана ситуација се мора заснивати на реалистичним елементима, тако да се степен неистине смањи на минимум. Уколико се одређени практични аспекти

---

[284] Социјални инжењеринг има за циљ прикупљање корисних информација за приступ мрежи или систему жртве, оних информација које нису лако доступне кибер нападима техничког типа. Нарочито се примењује у случајевима када је рачунарска мрежа (или цео систем) жртве заштићена јаким безбедносним мерама.

на прави начин уклопе у осмишљени сценарио, повећава се и могућност успеха нападача:

- жртва мора бити убеђена да одговорност за извршену радњу неће пасти искључиво на њу (тзв. „начело поделе одговорности“);
- жртва може бити убеђена како ће, уколико поступи по захтеву, моћи да оствари неки вид личне користи (на пример, да напредује у послу);
- жртва може бити убеђена како је њена морална обавеза да поступи по захтеву, тј. да ће уследити осећање гриже савести уколико не поступи тако.

Лична персуазија жртве је неопходна за успех напада социјалног инжењеринга. Жртва не сме да се осети присиљеном да реализује директиву нападача, већ њена перцепција ситуације треба да поприми перспективу „добре воље и ваљаних чинова“. Иако се жртвом управља, неопходно је да она мисли како има потпуну контролу над ситуацијом. Битно је, дакле, да жртва верује како је самостално донела одлуку да жртвује део свог времена и енергије у алтруистичке сврхе и/или за остваривање конкретних бенефиција.

Различити фактори доприносе повећању успешности сарадње између жртве и нападача – на првоме месту, постепеност приступа: нападно и ауторитарно понашање нападача према жртви код ње не подстиче жељу за сарадњом. Затим, претходно познавање нападача и жртве или њихова претходна успешна пословна сарадња у знатној мери повећавају шансе за кооперацију. И, на крају, физичка близина, лично присуство нападача, могућност опсервације нападачевог лика и гласа чине жртву расположенијом за сарадњу. Ригорозна примена техника социјалног инжењеринга не одређује сама по себи успех напада. Основни фактор успешности јесте степен учешћа жртве у активности у којој се тражи њена интервенција.

Особе врло блиске рачунарском систему који се напада (оне које управљају системом[285] или његови корисници) најчешће су жртве „социјалних инжењера“. Оне могу да пруже посебно важне информације о систему или да директно изврше модификације у њему. За остваривање успешне манипулације овим особама неопходно је да агресор добро познаје рачунарску технологију и да има уверљиве

[285] Администратор система, лица одговорна за безбедност, особље задужено за одржавање система итд.

аргументе који прате његов захтев. За особље које је „удаљено“ у односу на систем[286] технички аргументи су мање важни. Оно се најчешће одлучује за сарадњу пре услед „количине и хитности“ мотивација него због техничких основа захтева. Напади социјалног инжењеринга се ослањају на природну тежњу људи ка сарадњи, добронамерност и индивидуалну несигурност[287] у циљу добијања специфичних информација или оних података који могу бити искоришћени за извођење кибер напада у будућности.

Посебна врста напада који користи технике социјалног инжењеринга јесте такозвани *фишинг*, чији је основни, ако не и једини циљ, нелегална зарада.

3.4.2.2. Фишинг

Термин *фишинг*[288] користи се да опише поступак илегалног прикупљања осетљивих информација, добијених обманом у кибер простору, при којем се нападач представља као неко вредан поверења и ко заиста има право и потребу да оваквим информацијама располаже. Постоји неколико дефиниција фишинга, но, оне се не разликују битно. Према једној од њих фишинг подразумева „слање лажних порука електронске поште, написаних тако да делују као да су послате из банака и других легитимних институција, које имају циљ да наведу примаоца да открије личне податке осетљиве природе“.[289]

Фишинг-напади, дакле, подразумевају активности којима злонамерни актери коришћењем лажних порука електронске поште и лажних *web*-страница финансијских организација покушавају да наведу корисника на откривање поверљивих личних података. При том се првенствено мисли на податке као што су бројеви кредитних картица, корисничка имена и лозинке, PIN-кодови и слично.

---

[286] На пример: помоћно особље, портири, чувари, чистачи итд.

[287] Типичан пример био би покушај прикупљања заштићених података (попут корисничког имена и лозинке) телефоном, приликом којег се нападач представља као администратор система који покушава да реши алармантну ситуацију. Конверзација поприма тон ургентности, нападач врши константан притисак на жртву, која, услед несигурности, открива тражене информације.

[288] Реч фишинг (*енгл.* phishing) означава намерно погрешно написану реч „пецање“ (*енгл.* fishing). Највероватније проистиче из израза „password harvesting fishing“ (пецање на плантажама лозинки).

[289] *Know your enemy: phishing – Behind the scenes of phishing attacks*, The Honeynet Project & Research Alliance, http://www.honeynet.org

Напад најчешће започиње тако што нападач настоји да усмери жртву ка одређеној *web*-страници, дизајнираној тако да имитира визуелни идентитет легитимне организације. Жртва, даље, не сумњајући у аутентичност *web*-странице, на њој оставља властите поверљиве податке. У следећем кораку нападач користи прикупљене личне податке жртве, тј. преузима њен идентитет како би извршио незаконите финансијске трансакције. На овај начин жртве могу да претрпе значајне финансијске губитке или, у озбиљнијим случајевима, чак и губитак сопственог „електронског идентитета“, који бива искоришћен за криминалне циљеве. Последице крађе извршене фишингом штетне су за жртву напада, која трпи губитак не само у економском смислу већ и у смислу репутације и кредибилитета пред различитим друштвеним институцијама (финансијским, административним, осигуравајућим итд).

Криминалци су се одувек служили различитим видовима превара како би дошли до поверљивих информација. Са ширењем услуга електронских трансакција криминалци су, такорећи, почели не само да иновирају методе већ и да аутоматизују традиционалне технике у циљу извршења напада усмерених ка масовном тржишту.

Нападач започиње акцију слањем порука електронске поште великом броју корисника (неколико десетина, стотина, па и хиљада),[290] представљајући се као препознатљив и веродостојан привредни субјект (банка, осигуравајуће друштво, трговинска организација итд). Порука обично садржи захтев да се хитно посети сајт дотичне организације, парадоксално објашњен као начин заштите поверљивих података корисника од нејасно аргументованих претњи. Порука, дакле, садржи адресу (link) чијом се активацијом жртва повезује са *web*-сајтом који симулира оригинални сајт изабране организације. У следећем кораку жртва оставља личне податке на лажној (наизглед легитимној) *web*-страници.

Квалитет и квантитет „улова“ повећавају могућност крајњег успеха нападача. У ту сврху је у последње време створен криминални савез између

[290] Претпоставља се да је само у САД послато више од 35 милиона таквих порука у првој половини 2005. Извор: Bank D.: “Spear Phishing tests educate people about online scams”, *The Wall Street Journal*, August 17, 2005, http://online.wsj.com

стручњакâ за фишинг (фишера) и такозваних спемера.[291] Фишери могу да уз помоћ најновијих техника за масовно слање порука електронске поште, користећи банке података које садрже хиљаде и-мејл адреса (које су на располагању спемерима), контактирају огроман број корисника, уз минималан ризик да буду идентификовани.

Пошто прибави неопходне информације за приступ банковном рачуну жртве и изврши нелегалне финансијске трансакције, нападач се сусреће са проблемом пребацивања новца украденог електронским путем у властиту земљу, будући да већина националних финансијских и безбедносних служби прати токове новца ка иностранству. Решење се најчешће проналази у коришћењу посредника који живи у истој држави као и жртва, и који често није ни свестан сопственог саучествовања у криминалној радњи. Новац украден са банковног рачуна жртве прослеђује се на рачун посредника који подиже новац (осим једног процента који задржава на име учињене услуге), а затим га шаље фишеру поштом или користећи се различитим услугама трансфера новца.[292]

---

[291] Спеминг (*енгл*. spamming) подразумева слање великог броја незахтеваних порука електронске поште, најчешће комерцијалног карактера. Може се остварити путем било којег медија, али је најчешће коришћен Интернет, тј. и-мејл-сервис. Основни циљеви спеминга су реклама, често порнографског садржаја, трговина на берзи, дискутабилни финансијски пројекти итд. У форми личног писма користи се и за превару. Спемер (пошиљалац спема) шаље идентичне поруке на хиљаде и-мејл-адреса. Ове адресе су најчешће прикупљене аутоматски са web-страница, из база података или једноставно „погођене“ насумичним коришћењем честих личних имена. У првих шест месеци 2005. године, према статистици корпорације „Symantec“ („Symantec“ је светски лидер у производњи софтвера за заштиту рачунара и мрежа од кибер напада), „спем“ поруке су представљале 61% укупно размењених порука електронске поште у свету. Од тог броја 51% потиче из САД.

По дефиницији, спем порука се шаље без дозволе примаоца, због чега се од стране ISP-а (Internet Service Provider) и већине корисника Интернета сматра неприхватљивим понашањем. Анкете су показале да се спем сматра једном од највећих сметњи на Интернету – слање ових порука у супротности је са Уговором о прихватљивом понашању корисника (Acceptable Use Policy) већине Интернет-провајдера, те може да доведе до раскида уговора са пошиљаоцем. Спеминг се, још, дефинише и као електронски еквивалент физичкој пропагандној пошиљци. Док у случају физичке пошиљке цену штампања материјала и слања плаћа пошиљалац, у случају спема сервер примаоца сноси највеће трошкове у смислу времена утрошеног за обраду података и простора „утрошеног“ за складиштење података. Спемери најчешће користе бесплатне Интернет-налоге тако да су њихови трошкови заиста минимални. Услед изазивања поменутих трошкова на терет примаоца, многи спем сматрају крађом, тј. криминалним актом. Према калифорнијским ауторитетима спем је, 2004. године, само у САД нанео трошкове веће од 10 милијарди долара, укључујући губитак продуктивности, софтвер и радну снагу неопходну за супротстављање проблему.

[292] Пример поруке која има за циљ проналажење посредника за транзит новца: „Hello! We finding Europe persons, who can Send/Receive bank wires from our sellings, from our European clients. To not pay TAXES from international transfers in Russia. We offer 10% percent from amount u receive and pay all fees, for sending funds back. Amount from 1000 euro per day. All this activity are legal in Europe. Fill this form: http://XXX.info/index.php (before filling install yahoo! messenger please or msn), you will recieve full details very quickly.“

Апроксимативан *енгл*ески у поруци, која је доследно цитирана, већ је, сâм по себи, довољан да покаже да извор поруке није легитиман.

Званичници у САД тврде како је 1,78 милиона грађана Америке отворено признало да је преварено и да је путем електронског писма наведено да открије број платне картице, лични идентификациони број (PIN-кôд) или друге личне податке, услед чега су претрпели материјалну штету. Процене су да је тамна бројка знатно већа – око три милиона случајева. Криминалци су „на име“ недовољно опрезних Американаца зарадили скоро 1,5 милијарди долара, због чега су преваре фишингом постале уносна грана организованих криминалних група. Број оваквих напада непрекидно расте, по месечној стопи која се креће између 10 и 20%, а најчешће жртве су корисници услуга великих комерцијалних банака.[293]

Није боља ситуација ни у Великој Британији, где је, према резултатима истраживања обављеном на узорку од 2.000 корисника Интернета, 5% корисника било жртва фишинг-напада. Половина жртава није од својих банака добила никакву надокнаду.[294] У 2004. години свота губитака директно изазваних фишингом износила је 12 милиона фунти и претпоставља се да је сваке године све већи.[295]

Износ губитака не треба да изненади, јер је способност фишерâ таква да су чак и едуковани корисници изложени ризику. У експерименту који је извршен у јуну 2004. године на америчкој Војној академији у Вест Поинту више од 80% од око 500 војника наведено је да открије личне информације преко лажних порука електронске поште.[296]

Проблем фишинга ни у којем случају није ограничен само на територију САД и Велике Британије. У питању је глобални проблем, нарочито због флуидности саме мреже и података који се путем ње могу размењивати, без обзира на стварну локацију преваранта и жртве. Анализе показују да су рачунари с којих потичу напади махом лоцирани у азијским земљама – чак 20% њих налази се у Јужној Кореји, 16% у Кини, а 7% на Тајвану. Наравно, то не значи да се људи који стоје иза тих активности заиста налазе у тим земљама, али је индикативно да је Далеки исток препознат као својеврстан „рај“ за „пецароше“ наивних корисника Интернета. То се

---

[293] Kerstein P.: *How Can We Stop Phishing and Pharming Scams?*, http://www.csoonline.com

[294] Richardson T.: “Brits fall prey to phishing”, *The Register*, May 3, 2005, http://www.theregister.co.uk

[295] Leyden J.: “UK card fraud hits £505m”, *The Register*, March 8, 2005, http://www.theregister.co.uk

[296] Bank D.: “Spear Phishing tests educate people about online scams”, *The Wall Street Journal*, August 17, 2005, http://online.wsj.com

приписује језичким и временским баријерама тог региона у односу на државе западне хемисфере. Интересантно је напоменути да је број „брендова“ које фишери користе као мамац константан и да се креће у опсегу од 42 до 46. У том смислу, утврђено је да су фишингом највише погођени: сектор финансијских услуга (70%), Интернет-сервис-провајдери (15%) и трговински ланци (7%).[297]

Напади који се спроводе техником фишинга у суштини су базирани на недостатку безбедносне културе информатизованих маса. Већина корисника Интернета није спремна да се самостално и на адекватан начин суочи са претњама у кибер простору, иако свакодневно користи информационе системе. Милиони корисника свакодневно препуштају своје ресурсе, пословне и личне информације системима чији начин функционисања и рањивости не познају довољно. Другим речима, значајни лични ресурси смештени су у инструменте чијим се грешкама и аномалијама не зна да се адекватно управља.

Дакле, масовна распрострањеност финансијског пословања „из фотеље“, заједно са неискуством корисникâ у области кибер безбедности, до сада су осигурали лаке зараде „електронским криминалцима“. Извештај корпорације „Symantec“ прогнозира раст феномена фишинга у будућности.[298] Предвиђа се да ће се криминалци, с једне стране, специјализовати за извођење напада на мање пословне системе (мање банке, сајтове за онлајн трговину итд), с обзиром на то да они, уопште узев, имају слабије системе заштите, док ће, са друге стране, континуирано усавршавати методологију напада на индивидуалне кориснике кибер простора.

Фишинг се понекад погрешно третира искључиво као проблем друштава у којима постоји висок степен продора електронског пословања. Међутим, он подједнако погађа и развијене и неразвијене земље. Док се прве боре појачаним мерама интерне и екстерне контроле и ригорозним законским нормама, оне саме су немоћне да зауставе поплаву превара без помоћи оних потоњих. Сиромашније земље се често појављују као „легло“ међународног организованог криминала, што са́мо по себи има погубне последице за њихове и иначе крхке политичке системе. С друге

[297] Филип А.: *Phishing*, http://www.inet.co.yu/textview.php?file=k-phishing.html

[298] *Internet Security Threat Report – Trends for January 05–June 05*, Symantec, http://www.symantec.com

стране, ни њихови грађани и компаније нису имуни на фишинг-нападе, па је проблем самим тим у најмањој мери удвостручен. Услед заостајања у процесу усвајања законских норми из домена кибер безбедности и њихове имплементације, и наша земља се све чешће опажа као погодно место за лансирање „обмањивачких кампања“, због чега нас светска јавност наводи као пример „обећане земље“ за такве активности.[299]

3.4.3 Планирање и извршење напада

Кибер напад који има за циљ остваривање неауторизованог приступа и заузимање рачунарске мреже тим путем није једноставно спровести. Самом чину извршења напада мора претходити детаљно планирање акције. Може се рећи да је то, у суштини, дуготрајан процес, који се одвија кроз одређене фазе. Неки од ових корака већ су аутоматизовани и извршавају се коришћењем малициозних програма или других инструмената који се лако могу набавити у глобалној мрежи.[300] Професионални нападачи, међутим, користе софистициране и персонализоване инструменте, који су тешко доступни другима, а чији се ефекти не могу опазити ни од стране стручњакâ у пољу кибер безбедности нити од хардверских и софтверских безбедносних инструмената.[301]

На нивоу теорије може се разликовати пет фаза кибер напада:[302]

Прва фаза: „препознавање и преоперативни надзор“

У првој фази нападач се детаљно упознаје са информацијама које ће му олакшати приступ информационом систему организације коју намерава да нападне. Најчешће се користи метод социјалног инжењеринга, којим се од једног члана организације (инсајдер) добијају осетљиве информације (као што су бројеви телефона, органиграми организације, подаци о приступним налозима и лозинкама

---

[299] Катиловић Д.: „Пецање наивних душа“, *Свет компјутера*, децембар 2004, http://www.sk.co.yu/2004/12/skin05.html

[300] *Professional cyber arms dealers*, Defensetech, http://www.defensetech.org/archives/004142.html

[301] “How cyber crime went professional”, *The Independent*, August 13, 2008, http://www.independent.co.uk/news/business/analysis-and-features/how-cyber-crime-went-professional-892882.html

[302] Skoudis E.: *Counter Hack: A Step-By-Step Guide to Computer Attacks and Effective Defenses*, Prentice Hall, New Jersey, 2002, p. 21.

итд). Други методи укључују прегледање електронског отпада ради проналажења информација које су од важности за успешно извођење напада. Начин аутоматизовања ове фазе састоји се од инфицирања циљаног система помоћу неког од малициозних програма.

Друга фаза: „анализа (scanning)“

Када прибави осетљиве информације, нападач детаљно испитује систем мреже организације са циљем откривања њене рањивости, ради проналажења приступних улаза. Овај процес је врло спор и може да траје месецима.

Трећа фаза: „приступ“

Пошто заврши попис „рањивог инвентара“ и конфигурације мреже, нападач приступа преузимању контроле над системом и мрежом, користећи украдене лозинке и стварајући лажне корисничке налоге, или, пак, користећи рањивости, инсталира *тројанца* или *бот*, који остају „успавани“, чекајући команду за активацију из спољашње мреже (Интернета).

Четврта фаза: „одржавање приступа“

Након приступа систему нападач може да инсталира додатне малициозне програме (*споредна врата*, или *root kit*) који остају прикривени, дозвољавајући нападачу да неприметно приступи систему у било којем тренутку, са привилегијом да, по жељи, постане његов администратор. На тај начин, нападач *de facto* добија власт над системом, као и могућност да га конфигурише по сопственој жељи и елиминише претходне рањивости како би га заштитио од противнапада.

Пета фаза: „прикривање трагова“

Софистицирани нападачи и освојеном систему приступају неприметно, јер је „невидљивост“ неопходна за прикупљање што већег броја информација и повећање нанете штете. У том смислу, нападач најчешће користи програме *root kit* и *тројански коњ* који дозвољавају преправљање *log*-фајлова (дневници који евидентирају идентитет корисника који приступа систему) и тражење сакривених фајлова, како би избегао да заштитни механизми примете његово присуство.[303]

---

[303] Saita A.: “Antiforensics: The Looming Arms Race”, *Information Security*, Vol. 6, No. 5, 2003, p. 13.

3.4.4. Пропаганда као чинилац кибер рата

Осетљива информационо-комуникациона инфраструктура, како смо могли видети, најчешће је угрожена злонамерним коришћењем различитих техничких инструмената из арсенала кибер ратовања.

Кибер напади који се базирају на употреби разноврсних малициозних софтверских апликација, али и они што се користе специфичним методима обмане појединаца који опслужују информационе системе, представљају значајну претњу не само складном фунционисању информационих система већ и, посредно, целокупном друштву које се на њима темељи. Претходно поменуте врсте претњи, можемо констатовати, специфичне су по томе што су усмерене на дестабилизацију инфраструктуре која је у основи кибер простора. Другим речима, кибер напад превасходно циља на сâм кибер простор, тј. на ентитете унутар њега.

За разлику од њих, постоји и она категорија претњи информационом друштву која кибер простор злоупотребљава у једном ширем смислу – не као циљ, већ као средство. Реч је о специфичној злоупотреби кибер простора као средства за масовну комуникацију. Ова врста злоупотребе укључује пласирање дезинформација[304] и субверзивно-пропагандну активност.

У најопштијем смислу под појмом пропаганде подразумева се планска и смишљена активност, као и сама техника те активности на ширењу политичких, привредних, културних и других идеја, мишљења и поступака, са циљем утицаја на схватање и понашање људи.[305]

Пропаганда као форма ширења информација није нова. Хитлер и Стаљин ефикасно су је користили тридесетих година. Милошевићева контрола медија била је кључна за његово одржање на власти, током деведесетих година XX века. И у Руској Федерацији, током деведесетих, битка за моћ водила се у телевизијским станицама. Тако је било и у недавним сукобима у Јужној осетији где су се, заједно за оружаном

---

[304] Термин дезинформација, у контексту шпијунаже, војних обавештајних служби и пропаганде, означава намерно ширење лажних информација са циљем обмане противника у вези са сопственом позицијом или акцијом. Док пропаганда има за циљ утицање на емоционалну димензију личности, дезинформација манипулише на рационалном нивоу.

[305] Милашиновић Р., Милашиновић С., *Основи теорије конфликата*, Факултет безбедности, Београд, 2007, стр. 529.

борбом, водила и надметања на информативном и пропагандном плану, са значајним ангажовањем ПР агенција са обе стране. У новим условима више него икада, тзв. мека пропаганда може се показати делотворнијом него тврда.

Кроз историју су били заступљени различити методи ширења пропаганде. У ту сврху и данас се користе различита средства:

- писана пропаганда врши се путем књига, штампе, памфлета, летака, реклама и других публикација и писаних материјала;
- визуелна пропаганда се врши путем фотографија, телевизије, карикатура, филмова, цртежа, симбола, итд;
- усмена пропаганда се врши путем радија, путем говора, кроз непосредне контакте, предавања, манифестације, демонстрације, јавне изјаве итд.
- Пропаганда се најчешће спроводи комбинацијом ових средстава.[306]

Пропагандно-субверзивна активност, јесте посебан облик пропагандне активности која се спроводи у ратним условима али често и у мирнодопским.

Под појмом непријатељске пропаганде, односно субверзивне пропаганде, подразумева се: „планска, организована и смишљена активност према нашим грађанима у земљи и иностранству и широј светској јавности ради придобијања јавног мњења за политику и циљеве који су супротни основним вредностима одређеног друштва, за стварање неповерења код грађана у његову перспективу за подстицање дефетизма отпора, идеолошке и политичке опозиције и сл. са циљем за стварање предуслова за угрожавање или рушење Уставом утврђеног поретка.“ [307]

Пропагандно-субверзивна активност је најчешће примењивана непријатељска делатност која има своје специфичне методе изражавања и одвијања - мада је најчешће пратеће средство у односу на укупност непријатељских манифестација и главно средство преко којих се изводе. Овај вид активности не може заменити оружане снаге али може допунити њихову делотворност.

Пропагандно-субверзивна активност се увек спроводи у комбинацији са другим активностима: политичким, идеолошким, обавештајним, економским,

[306] *Ibid*., стр. 530.
[307] *Ibid*., стр. 529.

војним, психолошким итд. Она је само „формацијски" организована на самосталним основама.

Таква укупност активности, са варијацијама у конкретној садржини, у многим земљама има своје посебно терминолошко одређење. У САД су у употреби појмови „међународна политичка комуникација", „специјални рат" и „психолошки рат", у Великој Британији „политички рат" итд. Оваква терминологија се често избегава у јавности, осим у ретким изузецима када се говори о делатности противника, али је скоро одомаћена у интерној употреби и за сопствену активност. Код нас, за овакву укупност субверзивне активности, још није усвојен јединствен термин. Покушало се са преузимањем америчке кованице „специјални рат", али тај термин се више односи на војну садржину и не одржава сву ширину непријатељске активности.[308]

У англосаксонском говорном подручју, да подсетимо, од 1976. године у употреби је појам „информационо ратовање" за означавање активности уперених против знања и система вредности одређене земље или организације. Од почетка деведесетих година прошлог века све је чешћа употреба појма кибер ратовање да би се означиле пропагандне и пропагандно-субверзивне активности које се одвијају посредством глобалне рачунарске мреже – Интернета.

Иако је појам кибер ратовање релативно новијег датума, субверзивно-пропагандна активност није и нова појава. Историја људске цивилизације сведочи о бројним примерима пропагандног ратовања који указују на значај информације у постизању информационе супериорности у односу на противника.

Констатовали смо да је израз „информационо ратовање" претходио изразу „кибер ратовање". Исто тако, израз „информација у рату" претходио је изразу „информационо ратовање". Први израз се односи на тактичко и стратешко заваравање, ратну пропаганду и уништавање командних и контролних система. Пример информације у рату представља употреба пропагандних форми разгледница,

[308] *Ibid*., стр. 536.

памфлета, говора и постера, које су растурали Американци и Немци током оба светска рата.[309]

Експанзија информационог ратовања почиње у XX веку, са развојем савремених технологија. Основна специфичност информационог ратовања јесте да бојиште информационог ратовања није физички, већ виртуелни свет, а потенцијални ратници на овом бојишту могу бити државни органи, војне организације, терористи, индустријски конкуренти, хакери и други. Сваки од ових противника мотивисан је различитим циљевима, ограничен различитим нивоима ресурса, сопственим могућностима и могућностима система да се брани.

Према дефиницији Института за проучавање информационог рата (Institute for Advanced Studies on Information Warfare), информациони рат представља „офанзивну и дефанзивну употребу информације и информационих система да би се искористиле, поткупиле, искриварile и уништиле информације и системи информисања противничке стране, истовремено штитећи властите информације и системе“.[310] Према овом одређењу, вођење информационог рата заснива се на три принципа:

- сазнати;
- спречити другога да дође до сазнања;
- навести друге да дођу до неистинитог сазнања. У овом трећем аспекту реч је о дезинформацији и утицају на мишљење и ставове.

Са друге стране, „Intelco“, филијала Међународне асоцијације савета одбране (International Association of Defense Counsel – IADC), као видове информационог рата разликује:

- рат *за* информацију;
- рат *кроз* информацију (помоћу дезинформације);
- рат против информације.[311]

---

[309] О појму пропаганде, али и о терминима са сродним појмовним значењем (агитација, индоктринација, „испирање мозга“, психолошки рат, субверзија итд), видети шире у: Милашиновић Р., Милашиновић С.: *Увод у теорије конфликата*, Факултет цивилне одбране, Београд, 2004, стр. 289–314.

[310] Greenberg L., Goodman S., Soo Hoo K.: *Information Warfare and International Law*, National Defense University, Washington DC, 1998.

[311] International Association of Defense Counsel, http://www.iadclaw.org/books.cfm

Алвин и Хајди Тофлер употребили су појам „доктори за ефекте“ (енгл. *spin doctors*) како би именовали стручњаке за информациони рат, тј. оне који стварају жељени ефект помоћу информације, проналазе и измишљају начине да се она погодно представи. Тофлерови су идентификовали шест начина да се „лажима заведу духови“: оптужити супротну страну за злочине и крволочност, хиперболички „надувати“ важност збивања, извести сатанизацију или дехуманизацију противника (демонизовати непријатеља), извести поларизацију типа „они који нису са нама против су нас“, призивати Божју казну, водити метапропаганду, тј. дискредитовати противничку пропаганду.[312]

Могућности примене ових и сличних замисли данас су готово неограничене. До енормног повећања могућности за вођење информационог рата како у сфери војних активности тако и у сферама економије, политике и културе, дошло је са настанком кибер простора или, прецизније речено, појавом Интернета.

У информационом добу значај информација и свих активности које су везане за ширење и продукцију информација је, у великој мери, порастао. Као и физички простор, и кибер простор припада ономе ко га се најпре домогне. Било која стратегија за успостављање контроле над Интернетом, попришт информационог рата, морала би као императив да усвоји следеће максиме: загосподарити каналима за проток информације, што је могуће више емитовати властите погледе и ставове да би се што ефикасније наметнули и без престанка усавршавати методе и средства за обраду информације.

Џозеф Нај сматра да је све већа раширеност информација довела до тога да су оне, чак и у демократским државама, централизованије него што је то био случај у доба локалне штампе. На будуће сукобе ће, према његовом мишљењу, утицати не само то који актери поседују телевизијске мреже, радио станице или *web* сајтове – кад постоји обиље таквих извора – него и чињеница који актер поклања пажњу којим изворима информација и дезинформација. Образлажући повећан значај пропаганде у информационом добу, Нај закључује да моћ информације припада онима који је

[312] Тофлер А., Тофлер Х., *Рат и антират,* Paideia, Београд, 1998.

могу преуредити и на прави начин вредновати, како би издвојили оно што је и тачно и важно.[313]

Интернет, иако представља откриће америчких војних стручњака, увелико је превазишао своју војну функцију. Данас је Интернет постао пропагандно поприште *par excellence*. Управо због специфичности овог амбијента на којем се пропагандна активност одвија дошло је и до промена у појмовној равни. Уместо израза „информационо ратовање“ у теоријској науци све је чешћа употреба термина „кибер ратовање“ јер овај термин снажно наглашава рачунарске и мрежне аспекте информационог ратовања.

Међутим, не може се рећи да постоји општа сагласност по питању употребе овог термина. У војним доктринама западних земаља, на пример, израз „информационо ратовање“ је још увек на снази. Овај израз је у доктринарним документима националних армија усвојен, и операционализован као технички термин, те је још увек у употреби од стране војних теоретичара.

Сваки корисник глобалне информационе мреже може постати жртва различитих техника усмерених на управљање перцепцијом. Чест је случај да особа која се обавештава преко Интернета верује да су обавештења која прима објективна. Напротив, велики број обавештења је тенденциозно пристрастан, национално, религиозно, политички, социјално или пак професионално обојен. Интернет се мање ослања на квалитет информације, а више на могућност да искристалише распрострањена мишљења. Тако се уз помоћ глобалне рачунарске мреже формирају „заједнице веровања“, које карактерише некритичко прихватање онога што се нуди у информационом галиматијасу, прихватање дела истине подметнутог као целина.

Отворени политички маневар дезинформисања у кибер простору, на пример, покренуо је запатистички покрет у Мексику 11. фебруара 1995. године. Овај покрет је успео да „мобилише штампу у САД, а преко ње и међународно јавно мњење тако што је, на Интернету, лансирао апел са захтевом за помоћ у супротстављању офанзиви мексичке владе, откривајући наводне покоље у селима у зони Морелија-Гамача. Новинари, који су неколико дана касније, као и обично, дотрчали на лице

[313] Nye S. J.: *Bound to lead: The Changing Nature of American Power*, Basic Books, New York, 1990.

места, могли су констатовати само да нема никаквих покоља, да се ништа заправо није догодило. Ипак, ефект је био постигнут, било каква акција мексичке армије у тој зони постала је немогућа, јер је све било под будним очима јавности. Штавише, популарност мајора Маркоса није престајала да се даље шири и расте брижљиво развијеном психолошком акцијом у којој су веома широко коришћене могућности Интернета.“[314]

Технички су могућности дезинформисања путем кибернетике неограничене, посебно помоћу слике и звука. Такве могућности се у огромној мери већ користе у области рекламе. Својеврсну дезинформацију спроводе и развијене државе света, које промовишу властите вредности и властити стил потрошње, две области које су у међувремену постале нераскидиво повезане и измешане. Оне то чине из економских, али и политичких побуда. Идеја је једноставна – промовисањем властитих вредности извозе и властити стил потрошње, чиме повећавају продају својих производа.

Повезивање вредносног система и производа објашњава перманентно инсистирање САД на извозу америчког начина живљења у све друге делове света. Да парафразирамо Волкова – можда не постоји директна узрочно-последична веза између светског поретка и потрошње кока-коле, али је сигурно да превласт информације отвара могућност за остваривање значајних профита. Средства којима се, при том, служе транснационалне компаније под покровитељством матичних држава по дефиницији су заобилазна, посредна, будући да нико нема осећај да се потчињава Америци тиме што једе у ресторану „Мекдоналдс“.

3.5. Објекти кибер ратовања

Информационо доба донело је промене у теоријским разматрањима о елементима националне моћи и разматрањима о националној безбедности држава. Раније је војна моћ била доминантан фактор по којем се упоређивала међусобна моћ појединих земаља.

У информационом добу информације, као и инфраструктура која их преноси, постају све важније за националну безбедност уопште а посебно у

[314] Волков В., *op. cit*., стр. 211.

оружаним сукобима. Иако се још увек, гледано кроз застарелу призму, региструју само војни сукоби, свакодневно се воде информациони, технолошки, економски, обавештајни, верски, психолошки, дипломатски, спортски и други ратови, на различитим нивоима. Тиме се врши померање тежишта рата са војне на друге сфере и делатности као што су информативна и обавештајна.

3.5.1. Информација као објект кибер рата

У претходном поглављу указали смо на чињеницу да је информација постала стратегијски ресурс савременог доба. Чињеница је да се свакодневно увећава количина информација у дигиталном формату али и да се, посредством савремених технологија, увећава могућност њихове обраде у јединици времена што се свакако одражава и на њихову употребну вредност. Процене овог растућег обима складиштених информација се крећу од једног до два ексабајта нових података у години, или приближно 250 мегабајта података за сваког мушкарца, жену и дете на земљи.[315]

У том смислу можемо рећи да је информација постала средишњи потенцијал светске производње и војне моћи. Светска производња темељи се на власништву и монополу над информацијама а сукоби се темеље на геоинформацијским надметањима. Делић праве информације може да обезбеди огромну стратегијску или тактичку предност. Недостатак делића информације може да има катастрофалне ефекте, сматра Тофлер.[316]

Велики број теоретичара међународних односа анализира националну моћ првенствено из угла њене војне димензије и користи је у класификацији држава. Међутим, у ери глобализације, информационе револуције и масовног комуницирања, војна моћ постепено губи на значају. Напредак на пољу информација, учинио је да се моћ „разлије на нове изворе и нове димензије“ (*diffusion of power*) односно да

---

[315] Nugent J., Raisinghani M.: “Bits and Bytes vs. Bullets and Bombs: A New Form of Warfare“, Janczewski L., Colarik A.: *Cyber Warfare and Cyber Terrorism*, Information Science Reference (an imprint of IGI Global), Hershey, 2008, p. 27.

[316] Тофлер А., *Рат и анти рат*, Paideia, Београд, 1998.

богатство информацијама утиче на моћ актера у савременом свету.[317] Као најважнија форма моћи појављује се *мека моћ*[318], моћ која се заснива на привлачности пре него на присили.

Џозеф Нај, амерички теоретичар, указује на измењено схватање природе моћи у савременом свету. Нај истиче да је „освајање срца и умова одувек било важно, али је оно од посебног значаја у глобалном информатичком добу.“ У том смислу, он наводи да је информација увек била моћ, а да модерна информациона технологија шири информације много шире и брже него било када раније у историји. Због тога је значај информације као елемента моћи порастао. Нај истиче да се природа моћи променила у последњих педесетак година, а посебно након последње информатичке револуције која је рачунаре и Интернет учинила неопходним у свим областима живота.

У опису утицаја информационе револуције на савремене односе, Нај износи свој суд о утицају информационе револуције на суверенитет и контролу држава, поимање националне безбедности и измењену природу претњи, питање националног идентитета, повећан значај недржавних актера, улози медија и пропаганде и надметање у обавештајном раду.

По питању суверенитета и контроле домет државе је, данас, порастао у неким областима али се смањио у другим.[319] Све земље, укључујући највеће, суочавају се са повећањем проблема које је тешко контролисати унутар суверених граница, као што су трговина дрогом, избеглице, тероризам, наметање културних вредности итд. Државе, по питању суверенитета и контроле, морају позорницу да деле са актерима који могу да употребе информације за увећавање сопствене меке моћи и врше притисак на владе директно или индиректно мобилишући њихову јавност.

---

[317] Симић Д.: *Наука о безбедности, савремени приступи безбедности,* Службени лист, Београд, 2002, стр. 37.

[318] Термин мека моћ први помиње професор међународних односа на Харварду Џозеф Нај у књизи: *Bound to lead: The Changing Nature of American Power*, Basic Books, New York, 1990.

[319] Krasner S.: “Sovereignty”, *Foreign Policy*, January/Februrary 2001, p. 24; Weiss L.: *The Myth of the Powerless State*, Cornell University Press, Ithaca, NY, 1998.

Исто тако, данас национална безбедност може да буде угрожена не само оружаним снагама, већ нападачи могу да буду владе, групе, појединци и други недржавни актери. Нај истиче да ће нуклеарно одвраћање, оружане снаге у земљи и стационирање трупа у иностранству бити важне и у информатичком добу, али неће бити довољне да осигурају националну безбедност. У прилог тој тези он наводи чињеницу да је више десетина држава развило агресивне програме кибер ратовања.

Војна моћ и војне технологије, дакле, остају важан фактор у домену међународних односа. Информатичка технологија има неке ефекте на коришћење силе која користи малима а некад иде у прилог већ моћнима. Комерцијална доступност раније скупе војне технологије користи малим државама и невладиним актерима и повећава рањивост великих држава. Други трендови, међутим, ојачавају већ моћне. Информатичка технологија произвела је револуцију у војним пословима. Многе релевантне технологије доступне су на комерцијалним тржиштима, а може се очекивати да ће слабије државе купити многе од њих. Кључ, међутим, неће бити поседовање модерног хардвера или напредних система, него способност да се интегришу те технологије у један систем. Нај оцењује да ће у том погледу Сједињене Државе вероватно задржати вођство. У информатичком ратовању, чак и мала предност представља велику разлику.

По оцени Џозефа Наја, владе су увек водиле рачуна о протоку информација и контроли над њима. У савременом информационом добу, питање контроле над информацијама и комлетним информационим спектром посебно је актуелизовано. Информациона револуција се заснива на брзом технолошком напретку у области рачунара, комуникација и софтвера, који је довео до драматичног смањења трошкова обраде и преноса информација. Кључна одлика информатичке револуције није само *брзина* комуникације између богатих и моћних, већ се суштинска промена огледа у изузетном смањењу *трошкова* преноса информације. Као последица информатике револуције, количина информација које се могу пренети широм света постала је неограничена. Резултат тога је експлозија, односно „обиље информација“ које су доступне разним корисницима.

Нове информатичке технологије јачају утицај мрежних организација, новог типа заједница, као и транснационалних актера (појединаца и приватних организација, почев од корпорација преко невладиних организација до терориста)

који делују преко међудржавних граница. Сви ови актери данас су у могућности да играју непосредну улогу у светској политици.

У анализи активности неформалних група и невладиних организација у информатичком добу, Нај констатује да је информатичка технологија, нарочито Интернет, олакшала утицај спољних група на унутрашња дешавања и активности група унутар држава.

Сви поменути актери желе да у кибер рату, односно рату *за* информације, рату *кроз* информације (помоћу дезинформације) и рату *против* информација остваре своје интересе. Другим речима, информација је постала примарни објект кибер ратовања. Овладавање информацијама, успостављање контроле над њима и могућности да се креира, и јавном мњењу представи, властита представа стварности промовисале су информацију у основни објект кибер ратовања а кибер ратовање у примарни вид сукоба. Победа у рату за информације постала је предуслов за победу у традиционалном војном сукобу.

Информација је, дакле, постала основни ресурс у информационом добу и основни објект кибер ратовања. Отуда не изненађује чињеница да се данас спроводе бројне активности на националном, регионалном и глобалном нивоу, у циљу заштите овог ресурса. Ове напоре у сфери заштите информација и успостављања безбедног окружења за несметано функционисање информационог друштва су, на теоријској равни, пратила бројна коцептуална одређења.

На Светском самиту о информационом друштву (2003) донета је *Декларација о принципима*, у којој је наглашена потреба за развијањем концепта *кибер безбедности*. У одељку Декларације који је посвећен *Изградњи поверења и безбедности у коришћењу ИКТ* наводи се да је: „Јачање поверења, укључујући безбедност информација и мреже, аутентичност, приватност и заштиту корисникâ, неопходно за развој информационог друштва и стварање поверења између корисника ИКТ. Потребно је промовисати, развијати и имплементирати глобалну културу кибер безбедности кроз сарадњу свих доносилаца одлука и међународних експертских тела. Овај напор би требало да буде подржан кроз повећање међународне сарадње. У оквиру глобалне културе кибер безбедности важно је повећати безбедност и осигурати заштиту података и приватност, паралелно са повећањем могућности приступа и трговине. Такође, морају се узети у обзир и степен социјалног и економског развоја сваке земље и поштовати развојно оријентисани аспекти информационог друштва.“[320]

---

[320] *Declaration of principles building the Information Society: a global challenge in the new millennium*, 2003 World Summit on the Information Society, doc. WSIS-03/GENEVA/DOC/4-E, B5, 35, 2003, http://www.itu.int

Слична декларација, која је била предложена у резолуцији Уједињених нација из децембра 2002. године,[321] такође је одражавала убеђење да су поверење и безбедност темељ информационог друштва.[322]

Етимолошки посматрано, корени појма *кибер безбедност* сежу у шездесете године прошлог века и везују се за простор САД. У том периоду је третирана *комуникациона безбедност* (*Communication Security* – COMSEC).[323] Са појавом компјутера, седамдесетих година прошлог века, настала је *компјутерска безбедност* (*Computer Security* – COMPUSEC). Већ осамдесетих година XX века, услед инцидената као што су били *Кукавичје јаје* (Cuckoo's egg)[324] и *Морисов црв* (Morris

---

[321] У резолуцији 57/239, из децембра 2002, Генерална скупштина УН промовисала је елементе за стварање глобалне културе кибер безбедности, позивајући земље чланице и све међународне организације да узму у обзир те линије водиље у припреми Самита о информационом друштву. У децембру 2003. резолуција 58/199 још једанпут је подвукла неопходност промовисања глобалне културе кибер безбедности и заштите критичних инфраструктура.

[322] *Plan of action*, 2003 World Summit on the Information Society, doc. WSIS-03/GENEVA/DOC/5-E, 2003, http://www.itu.int

[323] Синковски С.: „Информациона безбедност – компонента националне безбедности", *Војно дело*, бр. 2/2005, ВИЗ, Београд, 2005, стр. 34.

[324] Током 1986. први пут је јавно обелодањен међународни инцидент у кибер простору. У књизи Кукавичје јаје Клифорд Стол (Clifford Stoll), астрофизичар који је радио као системски инжењер у лабораторији „Lawrence Berkeley" у Калифорнији (лабораторија је била у саставу мреже ARPANET) описује како је случајно, због грешке у једном оперативном систему Unix који је одржавао, открио непознат кориснички рачун. Након консултација с колегама утврдио је да никоме није познато ко је и зашто отворио тај рачун нити ко се њиме користи. Неколико дана касније добио је обавештење како неко са тог рачунара покушава да провали у други рачунар, што га је подстакло на даљу истрагу, која је резултовала закључком да је неко неовлашћено присвојио права над системом. Клифорд је, уместо да закључа спорни рачун и тиме онемогући даље акције нападача, одлучио да допусти нападачу да настави са својим активностима како би му ушао у траг. Иницијални контакти с органима власти (полиција, FBI) нису уродили плодом, тако да је Клифорд сâм наставио истрагу. Након неколико месеци открио је да нападач поседује информације о неколико војних пројеката (тада је био актуелан војни пројект „Рат звезда" – Star Wars, у време Хладног рата), да је провалио у неколико стотина рачунара на Интернету и у мрежу TYMNET (TYMNET је била међународна рачунарска мрежа утемељена на протоколу X.25, која је повезивала хиљаде великих компанија, образовних установа и владиних агенција, али је са порастом популарности Интернета нестала потреба за овом услугом, па је мрежа 2004. године и званично угашена). Временом се за случај заинтересовао и агент FBI-ја, што је било кључно за разоткривање нападача, који се представљао као Ловац (Hunter), а касније су се у потрагу укључили и агенти америчке Централне обавештајне агенције (Central Intelligence Agency) и Националне агенције за безбедност (National Security Agency – NSA). Како би ухватили нападача, Клифорд и остатак тима осмислили су непостојећу тајну мрежу, под називом SDINET, што је напослетку довело до хапшења нападача. Нападач је лоциран у западној Немачкој и, уз помоћ немачке полиције, ухапшен. Испоставило се да је нападач припадао удружењу Компјутерски клуб Хаос (Chaos Computer Club), чији су чланови веровали да све информације морају бити јавно доступне. Међутим, део чланова је добијене војне информације продавао и КГБ-у. Према: Marić I., *op. cit*., str. 13.

worm),[325] увидело се да мрежа састављена од великог броја рачунара[326] може бити искоришћена за злонамерне циљеве. Тада долази до интеграције комуникационе и компјутерске безбедности, те настаје појам *информациона безбедност* (*Information security* – INFOSEC). Информациона безбедност је интегрисала раније одвојене дисциплине, као што су безбедност персонала, компјутерска безбедност, комуникациона безбедност и оперативна безбедност. Већ у том тренутку информациона безбедност је постала један од четири камена темељца националне безбедности САД.[327]

Али, шта се конкретно сматра кибер безбедношћу? У овом тренутку не постоји општеприхваћена дефиниција термина, те му се често додељују различита значења. Најраспрострањеније је схватање по којем се кибер безбедност поистовећује са већ поменутом информационом безбедношћу, која се односи на „заштиту информација и информационих система од улаза, коришћења, ширења, прекида услуга, неауторизованих измена или уништавања, са циљем гаранције поверљивости, интегритета и расположивости“.[328] Акцент информационе безбедности стављен је на спречавање неауторизованог приступа информационим системима. Са овог становишта, превасходно се разматра поверљивост (*енгл.* confidentiality) информација.

Према другом, новијем, схватању (насталом деведесетих година прошлог века) термин „кибер безбедност“ се поистовећује са термином *информационо*

---

[325] Први црв, познат као Internet worm, идентификован је 1988. године на рачунару „Vax“ једног америчког универзитета. Пошто је рачунар био један од сервера у мрежи ARPANET, овај црв се самореплицирањем ширио са једног рачунара на други скоро експоненцијалним растом. Процењено је да је било инфицирано око 7.000 хостова (око 10% рачунара у саставу мреже ARPANET). Један број хостова је избачен из функције, док су код других функционалне могућности значајно деградиране. Аутор овог црва, 23-огодишњи студент са универзитета Cornell Роберт Морис (Robert Morris), искористио је слабости у три апликације TCP/IP и написао је експериментални, самореплицирајући и самопропагирајући програм, и убацио га у Интернет. Ускоро је открио да се програм реплицира и да реинфицира машине знатно брже него што је очекивао. Иако Морисов црв није био намењен за злонамерни напад, он је пример до каквих поремећаја у умреженим системима може доћи оваквим нападом. Према: Петровић С., *op. cit*., стр. 220.

[326] ARPANET је тада бројала око 88.000 рачунара.

[327] Поред дипломатије, економије и војне компоненте. Према: Синковски С., *op. cit*., стр. 34.

[328] Guideline for Identifying an Information System as a National Security System, National Institute of Standards and Technologies, http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf.

обезбеђење (*Information assurance* – IA).[329] Информационо обезбеђење дефинисано је од стране Националне агенције за безбедност САД као скуп мера за „заштиту и одбрану информација и информационих система обезбеђивањем њихове расположивости, интегритета, аутентичности, приватности и неопозивости. Оно укључује мере за бекап[330] система заштитом, откривањем и реакцијом на нападе.“[331]

У наведеном становишту термин „обезбеђење“ представља ниво поверења који је пропорционалан ефикасности додатних мера безбедности. Увођење овог термина на неки начин сведочи о промени „гранитног“ концепта безбедности, типичног за традиционалне информационе системе, који нису били повезани у мрежу, ка флексибилнијем концепту безбедности, који, са једне стране, подразумева да се природа кибер простора супротставља достизању апсолутне сигурности, а који је, са друге стране, одмерен вредношћу информације и уређаја које треба заштитити.

Напредак у рачунарској техници и начинима умрежавања рачунарских система[332] проширио је, дакле, у односу на концепт информационе безбедности, листу својстава информација пред које се постављају безбедносни захтеви. Са становишта информационог обезбеђења значајно је задовољавање следећих својстава информација (или безбедносних сервиса информација и информационих система): *приватност* или *поверљивост* (*енгл.* privacy, confidentiality), *интегритет* (*енгл.* integrity) и *расположивост* (*енгл*. availability). Њима се понекад додају још два: *аутентичност* (*енгл*. authentication) и *неопозивост* (*енгл.* non-repudiation).

Циљ *приватности* је да дозволи приступ информацији искључиво ауторизованим лицима, процесима или програмима. *Поверљивост* информације може бити везана за разлоге националне безбедности (на пример, информације о

---

[329] У српском језику не постоји адекватан превод термина information assurance. Могуће га је превести као: „информациона гаранција“, „информационо осигурање“ или, у нешто слободнијем облику, „информационо обезбеђење“. Домаћи ауторитет у овој области Стеван Синковски усваја термин информационо обезбеђење, позивајући се на идентичан превод у руским академским круговима.

[330] Бекап (*енгл*. backup) подразумева прављење резервних, сигурносних копија система, чиме се омогућава повратак система у претходно стање. Рачунарски речник Микро књиге, http://www.mk.co.yu/pub/rmk/detalj1.php?EngOdrID=446

[331] *National Information Assurance (IA) Glossary, CNSS Instruction n.* 4009, Committee on National Security Systems, National Security Agency, 2003, http://www.nstissc.gov

[332] Настанак локалних (Local Area Network – LAN) и бежичних (Wireless Area Network – WAN) мрежа а, пре свега, Интернета.

наоружању), индустријске безбедности (на пример, пројекти неког новог производа) или личне приватности корисника.

Интегритет тежи да осигура да информације и ресурси који њоме управљају (хардвер и софтвер) могу бити модификовани или уништени само уз посебну и претходно дефинисану ауторизацију.

Циљ *расположивости* се састоји у томе да информације и услуге које су са њом повезане буду одмах доступне ауторизованим корисницима. Другим речима, систем који даје такве услуге треба да функционише само када се то од њега захтева, и то у ограниченом и унапред одређеном времену. Са оперативнога гледишта, „расположивост“ се односи на прихватљиво време одговора система и прикладног нивоа услуге. Са гледишта безбедности информације, међутим, „расположивост“ представља способност заштите од штетног догађаја или могућност бекапа система у случају када се нежељени догађај већ десио. Расположивост савремених информационих система, који су у стању непрекидне активности, неопходна је како за нормално извршавање активности информационог друштва тако и за безбедност људских живота (довољно је поменути, на пример, системе који регулишу авионски саобраћај или аутоматизоване уређаје у операционој сали).

Аутентичност је мера безбедности која тежи да одреди вредност и валидност преноса, поруке или пошиљаоца. Овом мером се, такође, контролише и ауторизација корисника да прими специфичне категорије информација.

Неопозивост је мера безбедности чији је циљ да осигура ток комуникације. Њоме се постиже да пошиљалац информације има доказ о њеној испоруци, али и да прималац информације има податак о идентитету пошиљаоца, тако да ниједан од учесника у преносу касније не може негирати извршену трансакцију.

Степен важности наведених својства информација, са безбедносног становишта, варира у зависности од контекста у којем се размена информација врши. У војним системима, на пример, највећа пажња се посвећује поверљивости информација, док се у финансијским трансакцијама између банака акцент ставља на интегритет.

Иако не постоји општеприхваћена дефиниција кибер безбедности, можемо закључити да су појмови *информациона безбедност* и *информационо обезбеђење* укључени у шири концепт кибер безбедности. Према дефиницији америчког

Конгресног истраживачког сервиса (Congressional Research Service),[333] кибер безбедност се односи на:

- скуп активности, мера и техника осмишљених да заштите од напада, прекида сервиса (услуга) и осталих претњи рачунаре, мреже рачунара и информације које они садрже или размењују, као и софтвер, податке и остале елементе кибер простора; те активности могу да садрже, на пример, процену предности и рањивости хардвера и софтвера који се користе у политичкој и економској електронској инфраструктури једне земље;
- ниво безбедности и заштите од претњи који произлази из претходно цитираних мера;
- обједињене напоре и покушаје, који укључују истраживања и анализе, са циљем да се створе и побољшају активности везане за безбедност кибер простора и ниво његове заштите од претњи или кибер претњи.

Кибер безбедност се не може одвојити од општег контекста у којем функционише информационо друштво. Она обухвата широки спектар активности и мера, те представља комплексан систем, с обзиром на то да обједињава различите, подједнако важне аспекте. То значи да ниједан од њих не може бити запостављен: ако би један део система добио мање пажње, комплетан систем би престао да исправно функционише. Таква комплексност чини тешким достизање апсолутне сигурности. Није могуће потпуно елиминисати ризик од неадекватног, случајног или намерног, коришћења инструмената информационог доба. Кибер безбедност је, дакле, изнад свега управљање ризиком,[334] непрестано трагање за компромисом између вредности онога што треба заштитити, нивоа заштите и цене заштите.

3.5.2. Критична информациона инфраструктура као објект кибер рата

Концепт кибер безбедности, истакли смо, развио се као последица ширења рачунарских мрежа и стварања глобалне мреже – Интернета. Захваљујући првим безбедносним инцидентима у кибер простору увидело се у колико мери рачунарски

---

[333] Fischer E. A.: *CRS Report for Congress, Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, 2005, http://csrc.nist.gov

[334] Schneier B.: *Secrets and Lies. Digital security in a networked world*, Wiley computer publishing, New York, 2000, p. 384.

системи и мреже представљају извор ризика по информацију и, посредно, по индивидуалну, корпоративну, националну, регионалну и глобалну безбедност. Услед процеса континуиране информатизације становништва и прогресивне аутоматизације инфраструктура и сервиса неопходних за функционисање друштва, повећавао се и значај кибер безбедности. Овај концепт је данас постао централни елемент политика националне безбедности свих технолошки високоразвијених земаља, али и регионалних и глобалних безбедносних политика.

Информација је, дакле, основни ентитет који је изложен безбедносним претњама из арсенала кибер ратовања. Три аспекта информације су, најчешће, изложена ризику: приватност, интегритет и расположивост (доступност).

Осим информације ризику је изложена и целокупна инфраструктура која је задужена за пренос података и информација и њихово складиштење.

Националне безбедносне политике су, међу приоритетним задацима, одувек имале и заштиту државних инфраструктура. Непосредно по завршетку Хладног рата овај проблем је у Западним земљама, накратко, прешао у други план услед смањења директних територијалних претњи. Међутим, већ половином деведесетих година XX века питање заштите националних инфраструктура је поново заокупило пажњу креатора државних политика и постало срж расправе о унутрашњој безбедности. Сједињене Америчке Државе су поново имале улогу лидера у овим активностима.

Два догађаја су, у постхладноратовској ери, поновно иницирала интересовање САД за заштиту осетљивих информационих система: зависност америчког друштва од нових технологија која је настала као последица информационе револуције са једне стране, а са друге стране, повећана перцепција претње након атентата на Федералну зграду Алфреда П. Мураха у граду Оклахоми 1995. године.[335] Анализирајући последице атентата, амерички ауторитети су

[335] Федерална зграда Алфреда П. Мураха (*енгл*. Alfred P. Murrah Federal Building) представљала је канцеларијски комплекс америчких федералних служби смештен на адреси 200 N.W. 5th Street у пословном средишту града Оклахоме у истоименој држави. Зграда Мурах је била мета бомбашког напада изведеног 19. априла 1995. године. Том приликом је настрадало 185 људи. Све до деведесетих година прошлог века, у згради су се налазиле регионалне канцеларије Управе за социјалну безбедност, Федералног истражног бироа (FBI), Управе за сузбијање дрога (DEA) и Бироа за алкохол, дуван, ватрено оружје и експлозив (ATF). Према: "Critical infrastructure protection: a brief overview", http://chnm.gmu.edu

утврдили да је „губитак једне Федералне зграде од мање важности и удаљене од виталних ганглија нације, произвео ланчану реакцију на различите активности, које никада у нормалним условима не би биле повезане са том зградом“.[336] Осим изгубљених живота и саме инфраструктуре атентат је изазвао и прекид многих процеса и активности које су биле контролисане директно или индиректно из Федералне зграде.

Овај догађај створио је свест да међусобна зависност инфраструктура и релативно рањивих тачака представља фактор ризика за националну безбедност. Анализа последица атентата резултирала је моменталним доношењем Председничке директиве број 39 (PDD-39), којом је оформљена Радна група за критичне инфраструктуре (Critical Infrastructure Working Group), сачињена од представника различиих владиних агенција, којом је председавао тадашњи министар правде.[337] Задатак Радне групе био је да анализира ситуацију и предузме неопходне акције ради превенције сличних догађаја у будућности. Резултати анализе, објављени у фебруару 1996. године, евидентирали су, између осталог, константан мањак пажње по питању заштите кибер инфраструктуре, конституисане информатичким системима и мрежама, на које су се ослањале критичне инфраструктуре државе.[338]

На основу закључног извештаја Групе, председник Клинтон је именовао Комисију за заштиту критичних инфраструктура (Commission on Critical Infrastructure Protection – PCCIP), са задатком да врши детаљну анализу постојећих веза између критичних инфраструктура земље и националне безбедности.

Комисија је на крају свог рада дала оцену о високој рањивости (са израженим експоненцијалним растом) целокупне националне инфраструктуре због све веће, али не увек и видљиве, међусобне повезаности самих инфраструктура захваљујући којој типичне рањивости једне инфраструктуре представљају елемент ризика за цео систем. Том приликом је информационо-телекомуникациона инфраструктура (уређаји за пренос и обраду информација), заједно са још седам

---

[336] *Ibid*.

[337] U.S. Policy on Counterterrorism *PDD-39*, http://www.fas.org/irp/offdocs/pdd39.htm

[338] Дефиниција критичних инфраструктура дата је у Председничкој директиви PDD-63. Према овој дефиницији критична инфраструктура је описана као „структура међусобно повезаних мрежа и система које обухватају индустрију, институције (укључујући људе и процедуре) и способност дистрибуције која обезбеђује поуздан ток основних производа и услуга за одбрану и економску безбедност“. Према: The White House, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

других инфраструктура, проглашена за „критичну“ – названа је Критичном информационом инфраструктуром (Critical information infrastructure - CII).[339] Информациона и електроенергетска инфраструктура означене су као најосетљивије због тога што прожимају све остале, и представљају основу за нормално функционисање свих осталих инфраструкура. Реч је о оним инфраструктурама које одржавају основне секторе савременог друштва као што су здравство, економија, енергија, транспорт, телекомуникације, јавни ред, одбрана и, уопштено, јавна администрација, који су комплетно зависни од поузданог и сигурног функционисања система информационо-комуникационих технологија.

У октобру 1997. претходно поменута комисија закључила је да „безбедност, економија, животни стандард и, врло могуће, сама егзистенција индустријализованих земаља“ зависе од „електричне енергије, телекомуникација и рачунара..., који су, осим традиционалне физичке претње, изложени новим виртуелним претњама“.[340]

Закључци Комисије за заштиту критичних инфраструктура били су исте године на неки начин подржани организовањем вежби од стране америчке Агенције за националну безбедност (National Security Agency – NSA) којима је дато шифровано име „Подесни прималац“ („Eligible Receiver“). Циљ вежбе је био да се провери способност војног апарата да открије кибер напад усмерен против рачунарских мрежа важних војних команди и да му се супротстави. У вежби је учествовало 35 експерата Агенције за националну безбедност.[341]

---

[339] У осталих седам спадају инфраструктуре: банкарства и финансија, електроенергетских система, водоводних система, транспорта, хитних служби, владиних сервиса и инфраструктуре за испоруку и складиштење горива и гаса. Према: Marsh R.: *Critical Foundations: Protecting America's Infrastructures*, The George C. Marshall Institute, http://cipp.gmu.edu/clib/43_TheMarshallInstitute-CriticalFoundationsProtecting.htm

[340] *Critical Foundations: Protecting America's Infrastructures*, President's Commission on Critical Infrastructure Protection, Washington, 1997, http://www.fas.org/sgp/library/pccip.pdf

[341] Напад је био усмерен на Команду Пацифика, стационирану на Хавајима и одговорну за војне операције у пацифичком региону. Приликом напада стручњаци Агенције (који су, иначе, симулирали севернокорејске агенте) могли су да користе као средство само софтвер доступан преко Интернета и нису смели ни на који начин, нити из било којег разлога, да прекрше законе САД. Користећи се техником и инструментима који су у општој употреби од стране хакерâ, „нападачи“ су успели да приступе различитим системима Пентагона, укључујући и оне који се сматрају строго поверљивим. Другим речима, они су успели да дестабилизују нормално функционисање система и да изврше модификације мањег значаја у садржају електронске поште, укључујући и неке са информацијама осетљивим за националну безбедност а да при том не буду идентификовани од стране нападнутог система. Према: Verton D.: *Black Ice: the Invisible threat of Cyber-Terrorism*, The McGraw-Hill Companies, 2003, pp. 32–33.

Резултат вежбе је запрепастио организаторе: са релативном лакоћом агенти NSA могли су да прекину операције система команде и контроле снага САД у Пацифику. Другим речима, резултати су указали на комплетну неприпремљеност Америке да се одупре координираним нападима из кибер простора.[342] Дата сазнања су се претворила у страх да би се исте технике и исти инструменти могли применити, са још страшнијим последицама, против основних инфраструктура америчког друштва и економије, тј. против „мрежа система и независних процеса које функционишу на колаборативан и синергијски начин да би произвеле и распоредиле поуздан ток услуга и основних добара...“, чије би продужено неисправно функционисање или уништење „... имало ослабљујући утицај на безбедност и социјално и економско благостање нације“.[343] Реч је о оним инфраструктурама које одржавају основне секторе савременог друштва, као што су здравство, економија, енергија, транспорт, телекомуникације, јавни ред, одбрана и, уопштено, јавна администрација, који су комплетно зависни од поузданог и сигурног функционисања система ИКТ. „Умрежени рачунари управљају нашим критичним инфраструктурама, које су од виталне важности за одбрану нације, економску сигурност и јавно здравље.“[344]

Онемогућавање нормалног функционисања информационих система, у савременом друштву које је постало од њих зависно, може имати врло озбиљне последице на све сфере друштвеног живота. Последице могу бити чак и фаталне уколико се угрозе критичне информационе инфраструктуре као што су, на пример, системи за контролу копненог и ваздушног саобраћаја, хидро-брана, нуклеарних електрана, безбедносних и здравствених служби или, пак, системи за дистрибуцију електричне енергије.

---

[342] Према: *Cyber Security Research And Development Act*, House Of Representatives, додатак предлогу закона H.R. 3394, 2002, http://www7.nationalacademies.org/ocga/laws/PL107_305.asp

[343] Према: *Critical Foundations: Protecting America's Infrastructures*, President's Commission on Critical Infrastructure Protection, Washington, 1997 http://www.fas.org/sgp/library/pccip.pdf. Друга дефиниција је понуђена у Patriot Act-у (sect. 1016) из 2001. године и гласи: „физички и виртуелни системи од виталног значаја за САД, толико битни да би њихово нефункционисање или уништење имало за последицу слабљење безбедности, економске безбедности нације, здравља и јавне безбедности или њихову комбинацију“.

[344] *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, United States General Accounting Office, GAO-04-321, 2004, http://www.gao.gov/new.items/d04321.pdf

Након терористичких напада на Америку септембра 2001. године, у Западним земљама нарочито је актуелизовано питање безбедности кибер простора и заштите критичних информационих инфраструктура. Акцентовање ових питања, према неким аналитичарима, наступило је као последица страха америчке администрације од могућег „ефекта бумеранга“, тј. као последица сазнања да је Интернет за терористе представљао основни извор информација потребних за планирање и реализацију напада.

Повишена перцепција претње од могућности преношења тероризма у кибер простор, али и других видова кибер ратовања који могу нанети материјалну штету државама и становништву, угрозити системе одбране, нарушити здравље, права, али и сâм живот људи, пласирала је питање о могућности стварања безбедног кибер простора међу најактуелнија питања регионалних и светских организација.

Тако је, на пример, током 2006. године, у оквиру активности на супротстављању тероризму, Европски парламент упутио препоруку Савету Европе и европском Савету за заштиту критичних инфраструктура. Препорука је, између осталих, садржала и следеће ставове:

„Критичне инфраструктуре у Европској унији постале су високо повезане и међусобно зависне, што их чини посебно рањивима на поремећаје и уништење. Услед тога, постоји потреба да се сачини Европски програм за заштиту критичне инфраструктуре (European Programme for Critical Infrastructure Protection – EPCIP), који би био финансиран од стране држава чланица, и/или власника инфраструктура и оператера.

Потребна је ефикасна стратегија како би се постигла припремљеност (смањење ризика и претње) у односу на критичну инфраструктуру, повећање безбедносних мера, промовисање безбедносних стандарда и механизама за заштиту цивилног становништва. Заштита критичних инфраструктура захтева конзистентно, кооперативно партнерство између власникâ и управљачâ инфраструктуре и влада држава чланица. Анализа ризика и управљање ризиком у свакој инфраструктури морају бити базирани на стриктним стандардима ЕУ.

Морамо обезбедити да интегрална европска стратегија посебно обухвати претње критичној инфраструктури, укључујући рачунарске инсталације, поремећаје и уништење, што би имало значајне последице на здравље, безбедност и економско

благостање грађана. Убеђени смо да постоји потреба за јачањем система за заштиту рачунара кроз сарадњу националних компетентних ауторитета и европских (као што је ENISA)[345] у суочавању са све софистицираним претњама у пољу информационих технологија. ЕУ мора да утврди хармоничан метод како би државе чланице и оператери, уз помоћ заједничких стандарда организација и појединаца на пољу безбедности могли да: идентификују критичне инфраструктуре, анализирају рањивости и њихову међузависност, као и прекограничне последице евентуалне кризе, и заузму релевантан приступ према претњама; да осмисле решења за заштиту ове инфраструктуре, припреме их за све хазарде и обезбеде адекватан одговор у случају напада или катастрофе.

На пољу превенције, приправности и одговора на терористички напад уочљива је потреба за заједничким приступом Заједнице, који би, између осталог, био усмерен на: одговарајућу комуникацију надлежних са јавношћу у случају кризе, улогу Европола у примени силе против терориста у законским оквирима, механизме упозорења и институцију *Европског програма за заштиту критичних инфраструктура* (EPCIP) у истраживању безбедности.

Европска информациона мрежа за рано упозорење на плану критичне инфраструктуре (European Critical Infrastructure Early-Warning Information Network) имала би задатак да размењује информације о заједничким претњама и рањивостима и да осмисли одговарајуће мере и стратегије за смањење ризика у циљу подршке заштити критичне инфраструктуре.“ [346]

Можемо закључити да се данас већина система, операција и инфраструктура води путем дигитално контролисаних система ограничених степеном способности и безбедности. Осим тога, многи почињу да увиђају да су, услед технолошког напретка у дигиталним комуникацијама, телекомуникације подређене информационој технологији, а не обрнуто.

---

[345] ENISA је скраћеница за Европску агенцију за безбедност мрежа и информација (European Network and Information Security Agency). ENISA је основана 2004. године са седиштем на Криту. Према: http://www.enisa.europa.eu/pages/01_01.htm.

[346] Препорука са ознаком 2005/2044(INI) објављена је у *Службеном гласнику Европске уније* (Official Journal of the European Union), 25. 5. 2006, P6_TA(2005)0221.

Дакле, тренутно стање је такво да су информационе базе, контролни системи и средства комуникације међусобно повезани на глобалном нивоу. Овакво стање има своју „Ахилову пету“ јер технолошки најразвијенија страна може, у исто време, бити и најрањивија или, уколико је адекватно заштићена, може бити најопаснија.

У све бројнијим расправама о заштити критичних инфраструктура информационој инфраструктури се додељује посебна пажња. Током година су развијене различите мере за превенцију и одговор на могуће инцидентне ситуације, узроковане техничким кваровима, природним катастрофама или намерним деструктивним чиновима.[347] Растућа зависност система који омогућавају основне услуге од информационе инфраструктуре представља елемент ризика, с обзиром на то да прожима све остале и намеће им сопствене рањивости. Типичан пример прожимања може се видети у системима контроле.[348] Реч је о специјализованим рачунарима и технологијама који се користе у многим инфраструктурама услуга и индустрије за мониторинг и контролу најосетљивијих процеса. У индустрији електричне енергије, на пример, системи контроле могу да управљају и контролишу производњу, пренос и расподелу електричне енергије. У дистрибуцији гаса се мониторинг тока гаса у цевима обавља са удаљених тачака. У хидродистрибуцији они контролишу ниво воде у изворима и резервоарима, рад пумпи, степен квалитета воде и присуство хемијских адитива. Уопште узев, њихова основна функција је прикупљање оперативних података и мера са сензора, који се након обраде шаљу команди контроле и удаљеним периферним уређајима, који директно утичу на физичке компоненте инфраструктуре.

Да подсетимо, међу системима контроле два су посебно битна за безбедност критичних инфраструктура: 1) дистрибуирани систем управљања (Distributed Control Systems – DCS), који се користи у појединачним структурама или малим географским областима, и 2) систем за прикупљање, пренос и контролу података и

---

[347] Moteff J. D.: *Critical Infrastructures: Background, Policy, and Implementation*, CRS Congressional Research Service, Report for Congress, 2003, http://www.fas.org

[348] Систем контроле је дефинисан као комбинација рачунара, уређаја за контролу процеса, интерфејса и његовог софтвера, који заједнички надгледају варијабле техничких процеса и управљају различитим процесима. У подручју система контроле можемо истаћи: SCADA, DCS, системе за контролу процеса (PCS), системе за управљање енергијом и системе за контролу производње. Према: Dacey F. R.: *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO, 2004, http://www.gao.gov.

аутоматизацију и управљање индустријским процесима (SCADA),[349] који се најчешће користи у пространим географским областима.[350]

3.5.3. Системи за аутоматизацију и управљање индустријским процесима (SCADA) као објект кибер рата

SCADA системи имају широку примену у управљању и праћењу рада индустријских постројења и опреме (као што је водопривреда и хемијска индустрија) али и у телекомуникацијама, енергетици и системима управљања.

Ова врста система служи за аутоматизацију индустријских процеса, односно за прикупљање података са сензора и инструмената лоцираних на удаљеним станицама као и за пренос и приказивање тих података у централној станици у сврху надзора или управљања. Прикупљени подаци се обично посматрају на једном или више SCADA рачунара у централној станици (*енгл*. master station). SCADA систем може да прати и управља и до стотинама хиљада улазно-излазних вредности. Уобичајени аналогни сигнали које SCADA систем надзире (или управља) су нивои, температуре, притисци, протоци флуида или гаса и брзине мотора. Типични дигитални сигнали за надзор (управљање) су прекидачи нивоа, прекидачи притиска, статус генератора, статус контакта релеји итд.

Најпростији SCADA систем састоји се од неколико пари жица које на свом једном крају имају прикачене прекидаче, сонде, релеје итд. На другом крају је обичан персонални рачунар који преко аквизиционо-управљачке картице прима податке, обрађује их, формира информације о процесу и на тај начин врши надзор, а

---

[349] SCADA је акроним од Supervisory Control And Data Acquisition (прикупљање података, надзор, праћење и управљање) и подразумева цео спектар опреме, система и решења која омогућавају прикупљање података о неком процесу - удаљеном систему, обраду истих, надзор и, у појединим случајевима, реаговања на адекватан начин. Према: *Supervisory Control and Data Acquisition (SCADA) Systems*, National Communications System, 2004, p. 12, http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf

[350] DCS се, на пример, може користити у току производње електричне енергије у једном систему, док се систем SCADA користи за контролу енергије произведене и дистрибуиране на широком простору. Globalspec, http://communication-equipment.globalspec.com/LearnMore/Communications_Networking/Networking_Equipment/Distributed_Supervisory_Control_Systems_DCS_SCADA

некада чак и управљање. То је у основи централизован систем аквизиције и управљања.[351]

Комплекснији пример SCADA система је мрежа терминалских јединица којима се управља из рачунарског центра посредством неког комуникационог медија. То је дистрибуирани систем управљања (*енгл.* Distributed Control System - DCS). Стандард ISA S5.1 дефинише DCS као систем који се, иако функционално интегрисан, састоји од подсистема који могу бити физички раздвојени и удаљени један од другог.[352] DCS је првобитно развијен према потребама великих предузећа и процесних постројења који су захтевали знатну количину аналогног управљања.

Најкомплекснији пример SCADA система је мрежа SCADA система која функционише по принципу сервер-сервер, сервер-клијент. У овом случају, реч је о пројектовању великих SCADA система - географски дистрибуираних SCADA система, који се називају WASCAD системи (енгл. Wide Area SCADA). Разменом података између два или више независних SCADA система који контролишу различите сегменте истог технолошког процеса или привредног система (хетерогени WASCAD систем), стиче се целовита слика о његовом стању. Исто се подразумева и за хомогени WASCAD систем, с том разликом што се овде SCADA системи брину о истим сегментима јединственог технолошког процеса или привредног система (нпр. електроенергетски систем једне државе).[353]

Класичан SCADA систем оријентисан је ка управљању индустријским процесима или аутоматизацији лабораторија и одликује се малом дислокацијом појединих SCADA елемената, поузданијим извршењем комуникационих активности, и много већим степеном аутоматизације управљачких активности. Сложенији SCADA систем назван WASCAD орјентисан је на управљање географски дистрибуираним системима код којих се због комплексности процеса и комуникационих грешака најчешће избегава аутоматско вођење процеса како на локалном тако и на супервизорском нивоу. Последњу одлуку о промени режима

---

[351] Маринковић Д.: „Основе прикупљања података и управљања", *Микроелектроника*, Београд, бр. 1, мај 1998.

[352] *Instrumentation Symbols and Identification*: *ANSI/ISA–5.1–1984 (R1992)*, ISA – The Instrumentation, Systems, and Automation Society, North Carolina, 1992.

[353] Маринковић Д., *op. cit*.

процеса даје човек тако да је нагласак на квалитетном надзору - супервизији процеса.

3.5.3.1. Елементи SCADA и DCS система

Основне компоненте SCADA система су:

- програмабилни логички контролери (*енгл.* Programmable Logic Controller – PLC) или вишеструке удаљене терминалне јединице (*енгл*. Terminal Units – TU),
- централна станица и HMI рачунар(и)[354],
- комуникациона инфраструктура.

Иако су у архитектонском смислу SCADA и DCS системи веома слични, они се донекле разликују. Основне разлике између ових система могу се уочити у следећем:

- SCADA превасходно користи програмабилни логички контролер, док DCS користи удаљене терминалне јединице.
- PLC поседује већи ниво интелигенције од TU-а.
- За разлику од TU-а, PLC је у могућности да контролише станице без управљања од стране мастера.[355]

Терминалске јединице су електронска опрема инсталирана на местима где се врши праћење стања, догађаја или мерење величина преко сензора или праћење рада неког другог уређаја. Јединица претвара измерен сигнал или статус у форму која се може послати преко комуникационог медија према надзорно-управљачкој јединци (*енгл*. Supervisory Control Unit - SCU). Терминалска јединица, такође, прима податке

---

[354] Термин *централна станица* се односи на сервере и на софтвер за комуникацију са опремом, а онда и на HMI софтвер који се извршава на једном или више рачунара у контролној соби, или негде другде. У мањим SCADA системима, главна станица може бити само један PC, док у већим SCADA системима, главна станица се може састојати од више сервера и дистрибуираних софтверских апликација.

HMI рачунар је обично индустријски PC на коме се извршава софистицирани SCADA HMI софтвер. HMI (Human-Machine Interface – спрега између човека и рачунара) је апарат који процесне податке представља оператеру и кроз који оператер контролише процес. Основни интерфејс оператера је скуп графичких екрана који приказују репрезентацију опреме која се посматра.

[355] Bimbo S., Colaiacovo E.: *Sistemi SCADA - Supervisory control and data acquisition*, APOGEO srl, Milano, 2006, pp. 19-20.

са надзорно-управљачке јединице и претвара их у форму команди за неки извршни уређај.

Програмабилни логички контролер јесте најчешће коришћена савремена терминалска јединица. У суштини, свака терминалска јединица поседује апликациони софтвер у меморији, микропроцесор и компоненте за контролу укључивања/искључивања неког другог уређаја. Међутим, софистицираније терминалска јединица, тј. програмабилни логички контролер, представља персонални рачунар који поседује аквизиционо-управљачку картицу или проширен BUS намењен за праћење и управљање системима - другим уређајима. У зависности од природе примене терминалске јединице (тј. програмабилног логичког контролера) зависи хардверска и програмска подршка. Обрада мерних података, уочавање алармних услова и догађаја али и извршавање управљачких функција SCADA система, могу се у целости извршавати локално на самој терминалској јединици.

Прикупљање података почиње на нивоу PLC-а и укључује очитавање величина и статуса. Затим се подаци који су потребни шаљу на SCADA систем, где се преводе и форматирају на такав начин да оператер у командној сали уз помоћ интерфејса може, на основу њих, донети одговарајуће одлуке које могу бити потребне да би се подесиле нормалне функције рада PLC-а, а самим тим и процеса. Подаци се такође могу чувати у историјату, који је често подржан базом података, ради приказа трендова и других аналитичких радњи. SCADA систем типично имплементира дистрибуирану базу података, која се често зове и база тагова, која се састоји од елемената званих тачке или тагови. Таг представља једну улазну или излазну вредност која се прати или којом се управља од стране система. Тагови могу бити тврди (*енгл*. hard) или меки (*енгл*. soft). Тврди таг представља стварну вредност улазног или излазног сигнала, док је меки таг резултат логичких и математичких операција примењених на тврдом тагу. Већина интерпретација концептуално уклања ове границе називајући тврде тагове најпростијим случајем меког тага. Вредности тагова се обично чувају као комбинација вредност-време; вредност и временски

тренутак када је та вредност снимљена или израчуната. Серија вредност-време комбинација је историјат тог тага.[356]

3.5.3.2. Топологија SCADA мреже и комуникација између елемената система

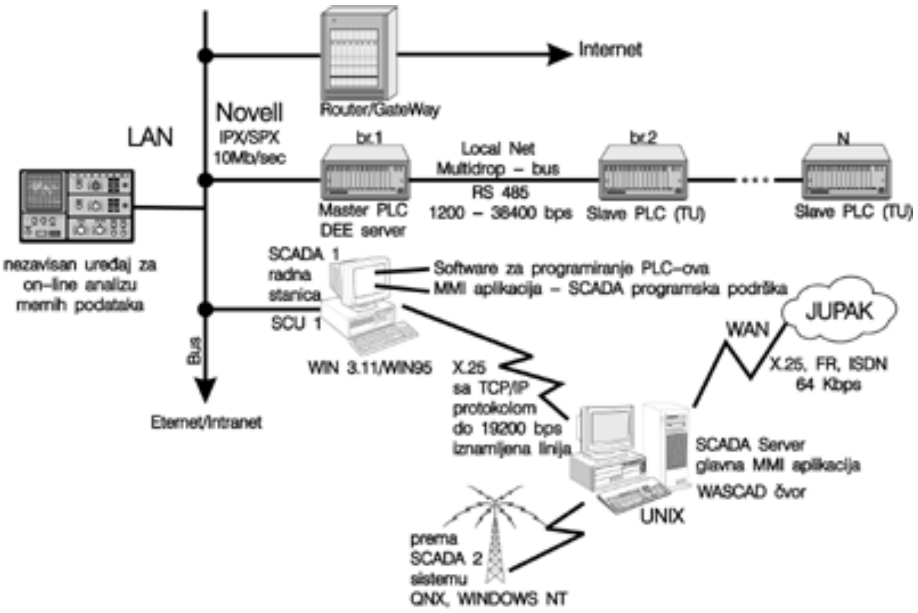
Конфигурација SCADA система је веома различита и зависи од просторног распореда технолошког процеса, управљачког задатка итд., и креће се од једнорачунарског система до поменутих WASCAD система.

Комуникација између терминалских јединица и надзорно управљачких јединица, као и међусобна комуникација између надзорно управљачких јединица, се одвија преко комуникационог медија, у зависности од могућности и захтева корисника. Тако се, на пример, пренос података може обављати преко јавне телефонске мреже, закупљених телефонских парица, осталих додељених жичних веза, двосмерних радио система, сателитских веза, фибер-оптчких веза, доступних LAN мрежа или било којег медија који омогућава пренос дигиталних података. Локалне мреже су идеалне за SCADA системе са малом дислокацијом елемената неког процеса управљања. Модерни SCADA системи, а нарочито WASCAD системи комбинују горе набројене комуникационе медије и топологије у циљу формирања снажног информатичког WASCAD чвора (схема бр. 5). У суштини оваква SCADA мрежа је дистрибуирана мрежа са разгранатом структуром (*енгл*. tree structure). Дакле једина разлика између надзорно управљачких јединица у разгранатој структури SCADA система би била у нивоу надлежности приликом одлучивања у процесу управљања.

---

[356] *SCADA aplikacija za vođenje procesa pneumo-transporta zeolita*, http://www.automatika.rs/baza-znanja/teorija-upravljanja/scada-aplikacija-za-vodjenje-procesa-pneumotransporta-zeolita.html

Схема бр. 5: *Пример SCADA хетерогене мреже*



Извор: Маринковић Д.: „Основе прикупљања података и управљања", *Микроелектроника*, Београд, бр. 1, мај 1998.

Надзорно-управљачке јединице и програмска подршка јесу централно место SCADA система. Надзорно-управљачки центри су обично опремљени PC рачунаром или неким снажним рачунарским системом. Ти рачунари су прогамски подржани апликацијом типа MMI (енгл. Man-Mashine Interface) која омогућава интерактиван дијалог са рачунаром за конкретан систем надзора и управљања. Основу за доношење одлука и управљање на овом нивоу чине подаци примљени од терминалских јединица. Сви подаци се формирањем централне базе података претварају у форму погодну за презентацију и генерисање упављачких акција (MMI апликација - SCADA програмска подршка). MMI апликација је обавезно подржана графичким интерфејсом који нуди могућност зумирања појединих делова извештаја или приказа више сигнала на једном дијаграму, скалирања сигнала али и могућношћу процесирања сигнала (дигитално филтрирање, спектрална анализа) у реалном времену (енгл. on-line processing). Додатне могућности MMI интерфејса су нпр. графичко приказивање објекта из разних перспектива, приказивање инсталација по етажама односно машинским подстаницама у облику мимик дијаграма (*енгл.* mimic diagram) са приказом статуса рада, мерних величина итд. Као што је већ речено, једна од основних карактерисика SCADA система је централизација најприоритетнијих функција на надзорно управљачкој јединици. Наиме, програмска

подршка у терминалским јединицама осигурава аквизицију података и локално управљање процесом до нивоа који се задаје са надзорно управљачке јединице, али иницирање свих контролних функција и крајња верификација њиховог извршења се врши само на надзорно управљачкој јединици.

Међутим, врло је битно нагласити разлику између програмске подршке која се користи за надгледање, контролу и синхронизацију осталих система приликом контроле процеса у реалном времену − SCADA програмска подршка, и програмске подршке за пост анализу (*енгл*. off-line processing) прикупљених података аквизицијом. Данас се на тржишту нуди програмска подршка која је већ стандардизована за процесно управљање преко рачунара. Та програмска подршка су генератори SCADA апликације за отворене рачунарске системе. Сваки захтев комитента се једноставно може реализовати бирањем опција или додавањем сегмента програмског кода у оквиру генератора апликације. Зато је данас акценат стављен на правилно пројектовање а не на развој властитих (елемената) SCADA система.

3.5.3.3. Рањивост SCADA система

Да подсетимо, прве генерације SCADA система подразумевале су тоталну централизацију процеса и коришћење WAN-а (Wide Area Network). Интеграцијом LAN-а (Local Area Network) и WAN-а омогућен је почетак децентрализације кроз дељење вођења процеса на више операторских (локалних) јединица. У данашње време, а тај тренд ће се вероватно задржати и у блиској будућности, доминира комуникациона веза заснована на TCP/IP протоколу. Овај тип комуникације омогућава креирање диспечерског центра за надгледање процеса производње на нивоу комплетног производног постројења. Већина савремених PLC-ова има инсталиран Ethernet модул који дозвољава надгледање и управљање са великих удаљености што, са друге стране, представља и значајну рањивост.

Данас је, дакле, све чешћи случај да се централна станица повезује са удаљеним контролним станицама помоћу Интернета. У том смислу, можемо закључити да су у прошлости проблеми безбедности система контроле били најчешће везани за физичку заштиту и спречавање настанка људске грешке у различитим процесима производње или дистрибуције производа. Последњих година, пак, порасла је свест о томе да су системи контроле критичних инфраструктура изложени кибер нападима, чији виновници могу бити веома различити:

непријатељске владе, терористичке групе, конкурентске компаније, различито мотивисани појединци и други.

Национални савет за истраживање САД указао је 2002. године да „могућност напада на системе контроле тражи хитну пажњу“.[357] У првој половини исте године неколико експерата кибер безбедности објавило је да је 70% произвођача енергије претрпело барем један озбиљан напад. Према подацима из фебруара 2003. године, претња од организованог кибер напада који је у стању да прекине функционисање критичних инфраструктура била је толико реална да је заштита система контроле постала национални приоритет.[358]

Међу различитим факторима који су допринели повећању ризика за системе контроле најевидентнији су:

- усвајање стандардних и врло распрострањених технологија, чије су рањивости широко познате, те се лако могу искористити;
- све распрострањенија примена повезивања тих система у шире мреже које нису директно контролисане од стране управљача инфраструктуром;
- недовољна или непостојећа заштита удаљених терминалских јединица;
- широка јавна доступност осетљивих техничких информација.

Док су у прошлости системи контроле користили мрежне протоколе и сопствене технологије хардвера и софтвера, што је неупућенима отежавало разумевање њиховог функционисања, данас привреда показује тенденцију да користи стандардне технологије и протоколе глобалне мреже, због знатно нижих цена управљања и побољшања способности система. Да ствар буде гора, и технолошки недостаци су постали општепознати, као што су општепознати и све софистицираније, а за коришћење једноставнији, инструменти неопходни за наношење штете у кибер простору. Дакле, коришћење стандардних технолошких архитектура у управљању системима контроле критичних инфраструктура довело је

[357] *Making the Nation Safer: the Role of Science and Technology in Countering Terrorism*, The National Research Council, Washington D.C., 2002, http://www.nap.edu

[358] *The National Strategy to Secure Cyberspace*, The White House, Washington D.C., 2003, http://www.whitehouse.gov

до повећања броја не само система потенцијално изложених кибер нападу, већ и актера способних да га изврше.[359]

3.6. Субјекти (актери) кибер ратовања

Из досадашњег излагања се могло увидети да кибер напади могу бити усмерени на намерно убацивање дезинформација на одређене интернетске форуме, енциклопедије, блогове и web сајтове сличног карактера или да могу бити строго усмерени према мрежној саботажи. Претходна елаборација је, такође, указала на чињеницу да на податке садржане у кибер простору, као и на елементе самог кибер простора, могу утицати било који колективни друштвени субјекти али и појединци који имају приступ умреженим рачунарским системима.

Технологије информационог доба на глобалном нивоу увећавају улогу држава, организација, мултинационалних компанија, невладиних организација, транснационалних криминалних организација и, чак, појединаца у међународној арени.[360] Може се оправдано веровати да ће се овај тренд наставити, дозвољавајући све већем броју учесника да на ефикасан начин следи сопствене интересе, што може да остави значајне последице на стратешком плану.

Савремене технологије омогућавају дистрибуцију информација, али и дезинформација, фаворизују културну и економску интеграцију (или дезинтеграцију) и дају визибилност и хитност догађајима, где год да се они дешавају у тзв. глобалном селу. Природа кибер простора таква је да се токови информација тешко могу ограничити и контролисати. Може се рећи да кибер простор не познаје политичке и географске границе. Две тачке су увек близу, без обзира на дистанцу која их раздваја, а веза између два удаљена рачунара има исте потешкоће које може имати локална рачунарска мрежа у једној згради. Природа кибер простора, са једне стране, подстиче интензивирање односâ између међународних актера, а, са друге, лаку дистрибуцију нежељених информација. Из тог разлога неке владе су, чак, одлучиле да усвоје рестриктивне политике према кибер простору или да својим

---

[359] Детаљни и ажурирани статистички извештаји о инцидентима везаним за системе контроле доступни су на адреси: US-CERT, http://www.cert-us.gov.

[360] Williams P.: "Transnational Criminal Organizations and International Security", Arquilla J., Ronfeldt D. F.: *Cyberware is coming!, in: Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, 1997, p. 329.

грађанима онемогуће приступ Интернету.[361] Прокламовани мотиви су били „заштита традиционалних вредности“, „одбрана националне безбедности“, промовисање морала, „превенција ширења субверзивног деловања“ итд. Информационе технологије, дакле, доприносе и формирању националних безбедносних политика.

Ако, уопште узев, постоји сагласност о томе да друштво пролази кроз континуирани процес информатизације, мишљења се мање слажу када се дотакну теме утицаја ове револуције на међународни безбедносни контекст. Безбедност постиндустријског друштва постаје све комплекснија, управо због његове зависности од нових технологија.

Државе које се ослањају на информационе технологије изложеније су и рањивије на било који облик штетне преправке, прекида или уништења технологија од којих зависе информациони токови, као што су, на пример, индустријска друштва рањивија од аграрних друштава у погледу континуираног снабдевања енергијом. Неједнака доступност и способност коришћења информационих технологија, са друге стране, продубљује јаз између богатих и сиромашних друштава. Јаз је присутан како на међудржавном, тако и на унутардржавном нивоу. Уколико би технолошки јаз наставио да се шири, осећај ускраћености код сиромашних популација би могао да изазове унутардржавне, али и међународне тензије.

Безбедносне претње у савременим околностима, дакле, асиметричне су. Земље са нижим нивоом зависности од нових технологија не само да су мање рањиве, већ могу да искористе рањивост развијенијих земаља за достизање својих стратешких циљева. Могућност извршавања деструктивних акција, са економскога гледишта, све је доступнија. Развијање офанзивних стратегија у кибер простору не захтева високе инвестиције, попут оних неопходних за конвенционално ратовање, а, изнад свега, ове стратегије доступне су великом броју актера. За разлику од технолошки софистицираног оружја, кибер оружје могу развијати појединци или групе, за шта су им потребни једино знање и мотивација. Државама или актерима

[361] У том смислу је најбољи пример Кина, земља са тоталитарним режимом, која је међу првима схватила и значај Интернета и важност његове контроле. Кинеска влада је једна од ретких која је успела да споји два контрадикторна аспекта – да фаворизује приступ Мрежи (тренутно има око 130 милиона корисника) и да, истовремено, спроведе контролу над информацијама, која подразумева потпуну блокаду било какве критике режима на web-у. У основи овог успеха налази се зналачко дозирање технологије (распрострањена употреба инструмената за филтрирање садржаја), репресија, цензура и обесхрабривање (у 20 провинција раде посебна полицијска одељења обучена да прате „субверзивне“ кориснике). Информација преузета из: Reporters Without Borders, http://www.rsf.org.

којима до сада није придаван значај у стратешком контексту то омогућава да теже другачијој позицији у кибер простору, где равнотежу моћи одређује пре знање него количина војног арсенала.

Осим тога, у кибер простору је мање изражена веза између безбедности и територије. Геополитичка позиција, која је одувек била централни, средишњи, елемент безбедносне политике државе, постепено губи свој значај. Данас више није неопходно физички ући у неку територију, нити је напасти кинетичким оружјем. Дакле, комплетна контрола физичких ентитета, као што су ваздушни или копнени простор, није довољна да једној држави гарантује безбедност. Војна надмоћ не значи сигурност у кибер простору, где је неопходно развити нове стратегије одбране кибер инфраструктуре, што је посебно тешко због типичног амбигвитета кибер напада. Уколико је кибер напад извршен професионално, врло је тешко одредити порекло извршиоца и мотивације, из више разлога:

- сачувати анонимност у кибер простору технички је врло лако;
- напад се може извршити из било којег дела света или, ако је неопходно, и са више тачака у исто време;
- последице напада се могу манифестовати након дужег временског периода, спречавајући тако откривање средстава и актера;
- време између откривања нове рањивости и стварања офанзивних инструмената који се могу применити за извршење напада све је краће, захваљујући усавршавању моћи рачунарâ;
- технологија која се користи за нападе релативно је једноставна за коришћење и врло је економична;
- у кибер простору се лако могу наћи инструменти и технике за извршавање напада;
- делотворност напада је све већа захваљујући аутоматизацији и софистицираности метода напада – један напад може да буде довољан да изазове тешке последице.

Као што је раније поменуто, кибер претње – за разлику од традиционалних претњи – нису одмах уочљиве нити се могу лако категоризовати. Првенствено, не постоји јасна идентификација који би актер могао да постане противник. Непријатељске државе, терористи, незадовољни радници, тинејџери, комерцијална или индустријска предузећа, политички активисти и криминалне организације само су примери могућих актера. Тешко је наћи евидентне доказе у вези са непријатељским намерама могућих нападача и њихове реалне способности да изведу напад на тако широком нивоу да угрозе безбедност државе.

Изнете потешкоће не умањују значај изучавања субјеката кибер ратовања, напротив. Уочени проблеми и израженост нових претњи у стратешком контексту

XXI века довољан су подстицај за научну тематизацију овог проблема. На првоме месту, истраживачки рад се мора усмерити на идентификацију актера, њихових различитих мотивација и циљева те анализу широког асортимана техника и инструмената („алата“) које су у стању да употребе. У табели која следи извршена је класификација најчешћих субјеката кибер ратовања на основу њихових мотивација и техника или начина изазивања претње.

Табела бр. 4: *Класификација субјеката претњи у кибер простору*

Субјекти претњи	Мотивација	Технике и инструменти
Хакери Крекери	Изазов Его Бунтовништво	Социјални инжењеринг Неауторизовани приступ Малициозни програми
Хактивисти	Пропаганда Слеђење политичких циљева	Опструкција услуга „Изобличавање“ сајта (*енгл*. web defacement)[362]
Инсајдери	Радозналост Его Обавештајна активност Материјална корист Освета	Уношење погрешних или лажних података Прислушкивање („пресретање“) Малициозни програми Саботажа Неауторизовани приступ Социјални инжењеринг
Криминалне групе	Уништавање информације Илегална дистрибуција информације Материјална корист	Напади уз коришћење обмане Крађа идентитета Упад у системе Малициозни програми
Терористи	Уцена Деструкција Пропаганда Освета Медијска промоција	Информационе операције Опструкција услуга Упад у системе Малициозни програми
Привредне корпорације	Економска шпијунажа Индустријска шпијунажа	Крађа информација Социјални инжењеринг Неауторизовани приступ
Националне армије Обавештајне службе	Стратешка предност	Информационе операције

Извор: Приликом израде табеле коришћени су документи Истраживачког одељења администрације Конгреса САД (General Accounting Office – GAO) и америчког Националног института за стандарде и технологије (National Institute of Standards and Technologies – NIST).[363]

---

[362] *Енгл*ески термин defacement (као и његов синоним defacing) могао би се дословно превести са „наруживање“, „замрљавање“. У пољу информационе безбедности овај израз се односи на недозвољено мењање почетне стране неког web сајта (његовог „лица“, home page-a) или преправљање и замењивање једне унутрашње стране или више њих. Овим недозвољеним активностима „наруживања“ сајтова баве се крекери. Мотиви вандализма могу бити различити, од идеолошких до чисте жеље за доказивањем. За добијање приступа сајту-жртви крекери најчешће искоришћавају слабости софтвера који управља сајтом или оперативних система, а ређе се служе техникама социјалног инжењеринга.

[363] *Cybersecurity for Critical Infrastructure Protection – Technology Assessment*, United States General Accounting Office, GAO-04-321, http://www.gao.gov; *Guideline for Identifying an Information System as a National Security System*, National Institute of Standards and Technologies, http://csrc.nist.gov

Субјекте кибер ратовања, тј. актере рачунарских напада можемо, у аналитичке сврхе, поделити у две различите категорије. Критеријум поделе јесте постојање односно непостојање намере код починиоца рачунарског упада. У том смислу можемо правити разлику између умишљајног кибер напада, и напада без умишљаја.[364]

Умишљајни кибер напад који се користи у кибер ратовању је сваки напад извршен помоћу кибер средстава са циљем да намерно утиче на националну безбедност или да створи услове за даље операције против националне безбедности. Умишљајни напади се могу изједначити са ратовањем - то је национална политика на нивоу ратовања. Они укључују било коју радњу која је извршена против противниковог рачунара и информационо-комуникационих система.

Неумишљајни кибер напад изводе актери, најчешће појединци, који ненамерно угрожавају националну безбедност и углавном нису свесни потенцијалних последица својих напада на међународном нивоу. У ове актере спадају сви они који почине кибер инфилтрацију, заобилазећи одбрамбене механизме система, те манипулишу, искоришћавају или уништавају информације садржане у систему односно сам систем. Ови актери имају различите мотиве и намере али, у основи, не намеравају да нанесу штету националној безбедности или даљим операцијама против националне безбедности. Ови актери најчешће се подводе под генерички појам „хакер“ и, иако чине кибер деликте, они кибер ратовање не воде намерно. Важно је напоменути да постоје случајеви да овом категоријом актера манипулишу они актери који нападе спроводе са умишљајем, искоришћавајући њихово знање и способности у кибер операцијама.[365]

Сви поменути актери користе исте основне алате за извршење напада, као што су рачунар, модем, телефон, и софтвер. Будући да су основни алати за извршење напада заједнички у целом спектру актера кибер ратовања, у пракси је тешко идентификовати нападача. У том смислу Лајонел Алфорд пише: „напад у оквиру кибер ратовања, усмерен против америчких инфраструктура, разликује се од

---

[364] Alford L. D. Jr.: “Cyber Warfare: Protecting Military Systems”, *The Journal of the Defense Acquisition University Review*, Quarterly 7, No. 2., USAF, 2000, p. 105.

[365] *Ibid*.

хакерског напада. Он се састоји од серије мањих напада, спроведених против пажљиво одабране мете, синхронизованих у времену, са циљем да оствари одређене циљеве. Противник може да комбинује кибер нападе са физичким нападима у покушају да паралише или успаничи велики сегмент друштва. Може да оштети нашу могућност да одговоримо на инциденте (на пример, искључивањем 911 система или комуникација у случају несреће), може да спута нашу способност да расподелимо конвенционалне војне снаге и на други начин ограничава слободу деловања нашег националног вођства."[366]

Другачије речено, у већини случајева једини начин да се направи разлика између хакерског напада и напада од стране армије противничке државе састоји се у анализи интензитета, организације или ефеката напада. Теоретски једина „јасна" ситуација била би она када је кибер напад спроведен заједно са другим, кинетичким, нападима у оквиру конвенционалног рата или уз објаву рата од стране државе непријатеља.

3.7. Сличности и разлике између кинетичког и кибер ратовања

Оште узев, може се рећи да кибер ратовање има другачије карактеристике и принципе од оних који су својствени традиционалном, кинетичком ратовању. Принципе традиционалног ратовања описали су, кроз историју, значајни војни теоретичари попут Сун Цуа, Клаузевица, Жоминија, Лидл Харта и других. Неки од принципа традиционално схваћеног рата применљиви су и на кибер рат, неки нису, а неки чак могу бити у потпуној супротности према кибер рату.

Кинетичко ратовање дефинишемо као ратовање у „реалном свету". Сва војна средства: тенкови, бродови, авиони, као и људство данашњих армија света, протагонисти су кинетичког ратовања. Кинетичко ратовање има историју дугу као и људски род. Многи војни теоретичари и историчари покушавали су да проникну у суштину ратовања и да издвоје његове принципе.

---

[366] *Ibid*.

Сун Цуова књига *Умеће ратовања* често се наводи у публикацијама посвећеним информационим операцијама јер су одређени Цуови принципи применљиви и у „виртуелном рату“. Такав је, на пример, Сун Цуов принцип манипулације доносиоцима одлука супарничке стране.[367]

Клаузевицева књига *О рату* изгледа да је изгубила популарност код писаца о информационим операцијама, али верујемо да је још увек релевантна, посебно у оним аспектима где се разматра *воља*, *магла рата* и *ратно трвење*.[368] Кибер ратовање, посматрано са војног аспекта, може подстаћи вољу за ратовањем код непријатеља. Стратешки напади током кибер рата, исто тако, смерају на увећање ратне магле и трвења.

Хартова *Стратегија* је применљива на кибер ратовање кроз принцип „индиректног приступа“.[369] Посматрано из позиције нападача, кибер напад је најделотворнији у оним случајевима када се одбрана нападнутог система потпуно заобиђе или поништи (уништи).

У оквирима овог рада није могуће прећи целокупну листу карактеристика кинетичког ратовања које имају одређених сличности са кибер ратовањем. Неке од њих смо разматрали у одељку „Утицај нових технологија на савремено ратовање“. Том приликом смо издвојили следеће карактеристике: *професионализација састава оружаних снага и повећана улога „специјалних дејстава“*, *непосредно и посредно учешће паравојних формација и цивила у ратним сукобима*, *медијско „препарирање“ јавног мњења и краће трајање ратова*, *промена улоге и значаја времена и измењена улога простора*. Ове карактеристикаме смо, експлицитно или имплицитно, детаљније елаборирали у претходним поглављима рада.

Осим поменутих карактеристика, важно је размотрити и остале релевантне карактеристике савремених ратова[370] у циљу утврђивања заједничких својстава кинетичког и кибер ратовања.

---

[367] Сун Цу: *Умеће ратовања*, Будућност, Нови Сад, 2004.

[368] Клаузевиц Ф. К.: *О рату*, Војна Библиотека, Београд, 1951.

[369] Харт Л.: *Стратегија посредног прилажења*, Војно дело, Београд, 1952.

[370] Видети табелу „Опште карактеристике савремених ратова“ унутар поглавља „Карактеристике савремених ратова“.

Један покушај у том правцу учињен је на америчкој војној академији Вест Поинт. Рејмонд Паркс и Дејвид Даген су у раду објављеном 2001. године истраживали применљивост појединих карактеристика савремених ратова на кибер ратовање.[371] Међу релевантне особености савремених ратних конфликата који се воде кинетичким оружјем они су уврстили следеће карактеристике: *масовно учешће људи и технике*, *офанзивност*, *могућност стратегијског изненађења*, *улога материјално-техничког фактора*, *маневарски карактер ратних дејстава*, *примарно дејство по систему руковођења и командовања – јединство команде*, *безбедност и једноставност*.

Резултати спроведеног истраживања показали су следеће:

- Кинетички принцип „масовност“ је потпуно ирелевантан за кибер ратовање изузев када оно укључује нападе опструкције услуге (Denial of Service – DoS) који има одлике кинетичког напада.
- Кинетички принцип „офанзивност“ није посебно значајан за кибер ратовање. У теорији се могу правити аналогије између кибер ратовања и подморничког ратовања и кибер ратовања и специјалних операција. Обе аналогије су сувисле. Међутим, ни у једном од претпостављених модела офанзивност није толико значајна као што је то случај у конвенционалном ратовању.
- У кибер ратовању су, исто као и у конвенционалном ратовању, прикривеност и изненађење изузетно значајни фактори. Према томе, традиционални принцип „могућност стратегијског изненађења“ применљив је и у кибер ратовању.
- На кибер ратовање применљив је и традиционални принцип „*улога материјално-техничког фактора*“. Будући да је кибер ратовање вид асиметричног ратовања, економија силе је битна.
- Кинетички принцип „*маневарски карактер ратних дејстава*“ применљив је и на кибер ратовање будући да агресор током кибер напада не помера своје трупе већ само мења тачку напада.
- Кинетички принцип „*примарно дејство по систему руковођења и командовања – јединство команде*“ применљив је на кибер ратовање у већини случајева. Принцип се не може применити на оне случајеве кибер рата када се за извођење напада злоупотребљавају несвесни корисници информатичких ресурса, који нису под командом протагониста напада –

[371] Parks R., Duggan D.: *Principles of Cyber-warfare*, Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001, pp. 122-125.

дакле, у нападима дистрибуираног лишавања услуге (Distributed Denial of Service – DDoS) .

- Кинетички принципи „безбедност“ и „једноставност“ применљиви су на кибер ратовање.

Спроведено истраживање указало је на то да су поједини принципи кинетичког ратовања применљиви и на „виртуелни рат“. Међутим, очигледно је да овај нови вид сукоба има и одређена специфична, дистинктивна, обележја. Намера нам је да на основу доступних резултата досадашњих истраживања детаљније елаборирамо оне принципе који су карактеристични за нови облик савремених конфликата – кибер ратовање. Листу принципа коју су понудили Паркс и Даген не треба прихватити као коначну, већ као почетни корак у анализи овог недовољно истраженог и сложеног феномена. Поменути аутори су издвојили следећих осам принципа кибер ратовања.

Основни, детерминишући, принцип кибер ратовања могао би да гласи: *кибер ратовање мора имати конкретне ефекте у реалном свету.*

Кибер ратовање је бесмислено уколико не погађа некога или нешто у не-кибер свету. Неко може нападати ентитете у кибер свету колико год жели, али такви напади су безначајни док немају конкретне ефекте у физичком свету.[372] Кибер ратовање у својој најпрепреденијој форми може утицати на умове доносилаца одлука у физичком свету. Претходно је аналогно кинетичком ратовању. Последње је у потпуности форма информационог ратовања, у коме је опонент снабдевен информацијом која га води лошој одлуци.

Напади, дакле, могу бити усмерени на доносиоце одлука, како тактичких тако и стратегијских. Доносиоци тактичких одлука, на пример, могу бити обманути по питању локације и бројности непријатељских и савезничких снага. На оперативном нивоу, подаци о времену снабдевања и количини набавке и појачања могу бити коришћени за манипулисање и доношење лоших процена као што су напад са недовољном количином муниције и уздржавање од напада услед страха од несташице залиха. Доносиоци стратегијских одлука, пак, могу бити увучени у

[372] Сценарији погађања ентитета у физичком свету су веома бројни. Кибер напад може погодити објект у физичком свету попут хидробране или онеспособити електричне подстанице. Замислив је сценарио по коме нападач може заузети контролу над целокупном електроенергетском мрежом што за последицу може имати отварање хидробрана и плављење градова или узроковати несреће у копненом, поморском и ваздушном саобраћају. Напади, на пример, могу онеспособити систем електронске јавне управе или све кључне инфраструктуре једне државе. Списак могућих физичких ентитета који би могли бити угрожени веома личи на листу Y2K проблема, о чему је било речи у одељку “Техничко-технолошки узроци несигурности кибер простора“.

додатне акције против држава или група које, уистину, нису актуелни нападачи. Могућност оваквих сценарија потврђена је кроз бројне симулације кибер рата које се спроводе у америчким истраживачким центрима последње две деценије.[373]

Други принцип кибер ратовања могао би се формулисати на следећи начин: *једна страна може предузимати активне кораке да се сакрије у кибер свету, али све што неко чини је видљиво – питање је само да ли ико посматра.*

Кибер свет је вештачка творевина, створен је од стране људи коришћењем хардвера и софтвера. Било која акција коју предузимају учесници у конфликту у том свету захтева манипулацију дигиталним подацима – њихово премештање или мењање. Уколико неко покушава да води кибер ратовање он мора да измени неки *бит*[374] у токовима података између рачунара – та чињеница указује на нечије присуство или акцију. Одбрана или заштита ИК система се заснива на способности откривања таквих активности. То значи да сваки од протагониста кибер ратовања мора непрекидно надзирати свој систем, што представља значајан проблем. Искуство говори да аутоматизовани детектори за откривање и спречавање напада имају одређене недостатке, те да се одбрана система не може у потпуности њима поверити. У одбрани је, дакле, пресудан људски фактор.[375]

Камуфлирање у физичком свету аналогно је скривању у кибер ратовању. Борци у физичком свету могу користити различите технике да прикрију своје присуство. У кибер свету, пак, то није случај. Протагонисти кибер ратовања морају покушати да сакрију доказе унутар постојећих токова података. Детектор кибер напада морао би да разликује bit-ове који су артефакти нападача од огромне већине bit-ова који представљају уобичајену активност. Ово је још сложеније уколико се напад изводи не-агресивним техникама када понашање нападача не одступа од понашања обичног корисника информационих ресурса. Системи за детекцију упада

---

[373] Једна од њих спроведена је у оквиру пројекта DARPA који се базирао на идеји да непријатељ покушава да подстакне рат између САД и неке друге државе путем кибер напада. Учесници који су били у улози руководства националне команде (National Command Authority - NCA) нису могли да открију идентитет правог противника. Према: Duggan R.: *Insider Adversary Model Briefing*, DARPA IASET Insider Workshop, August 2000.

[374] Бит је мерна јединица количине информација – 1 бит одговара једној цифри бинарног цифарског система. Реч бит настала је 1948. године као сраћеница од **bi**nary digi**t** (бинарна цифра).

[375] О системима за детекцију спречавање напада видети више у: Marić I., *op. cit*.

не могу правити разлику између обичног корисника базе података и противничког манипулисања базом, у ситуацији када се агресор представља као ауторизован корисник система.

Трећи принцип кибер ратовања може се дефинисати на следећи начин: *у кибер свету не важе константна правила понашања актера, нити постоје непроменљиви закони у односу на функционисање технике, изузев оних који захтевају промену у физичком свету.*

У физичком свету може се очекивати да ће се метак кретати у одређеном правцу након опаљења. Путања метка може се предвидети помоћу балистике. Сваки пут када се зрно испали оно ће се понашати исто, са незнатним одступањима од предвиђене путање, која су одређена физичким разлозима. У кибер свету, веровање у каузални след још је мање оправдано. Кибер свет, као вештачка људска конструкција, није савршен. Он се може мењати, и мења се, на неочекиван и хаотичан начин. Софтвер може изневерити, хардвер може отказати, на кориснички интерфејс могу утицати бројни фактори. Ове, и хиљде других варијација, узрокују непредвидивост кибер света.

У кибер ратовању, овај принцип реферира на нападе, будући да се они не дешавају увек на исти начин, као и на променљива окружења, те на флуктуирање перформанси система. Једини аспект кибер света који није подложан промени представљен је оним ентитетима који изискују промену у физичком свету. На пример, перформансе рачунара су физички одређене – рачунар не може повећати моћ обраде података све док особа у физичком свету то не учини уносећи измене у његов софтвер или хардвер. Ширина опсега комуникација је ограничена телекомуникационом инфраструктуром и једино може бити промењена заменом једног уређаја другим.

Четврти принцип гласи: *Поједини ентитети унутар кибер света имају овлашћење, приступ, или способност да изврше било коју акцију за коју нападач жели да буде извршена. Нападачев циљ јесте да преузме (присвоји) идентитет тог ентитета.*

Будући да је кибер свет потпуно вештачка творевина, он је изграђен и контролисан од стране људи и њиховог алата. Не постоји ниједан део кибер света који није под контролом људског фактора. За приступ рачунару најчешће су

потребна овлашћења администратора система. Некада корисник мора проћи физичко-техничку контролу до просторије у којој се рачунар налази. Али, увек постоји нешто или неко ко има ауторизацију да учини оно што кибер ратник жели да се учини. Већина корака током кибер напада је једноставно усмерена на то да се присвоји идентитет ентитета који може извести жељену акцију.

Класичан пример је експлоатисање Јуникс „корена“ (UNIX root exploit). Када неко изводи експлоатисање „корена“ он покушава да присвоји идентитет (а тиме и овлашћења) администратора Јуникс система. Бројни напади започињу експлоатисањем „корена“, а следећи кораци укључују промену конфигурације или софтвера циљаних система.

Наравно, експлоатација „корена“ није једини пример, није чак ни најчешће примењивана техника. Током многих напада, откривају се и присвајају идентитети обичних корисника рачунара, администратора база података, системских програма (као што су UNIX daemons и Windows services) и произвођача. У сваком случају, први корак напада подразумева проналажење особа са ауторизованим приступом циљаном систему а затим следи присвајање њихових идентитета, најчешће техникама социјалног инжењеринга или фишинга.

Пети принцип гласи: *инструменти кибер ратовања имају двоструку намену.*

Средства кинетичког ратовања имају појединачну намену. Опште је познато да се у рату оружје користи за напад, оклоп за одбрану а различита технолошка достигнућа и сензори за откривање непријатеља. Сасвим је разумљиво да ниједна од страна у сукобу, током његове манифестне фазе, не тестира своју одбрану тако што гађа властите трупе.

У кибер ратовању, међутим, исти инструменти користе се двојако –и од стране нападача и од стране одбране. Нападач користи аутоматизоване скенере вулнерабилности како би пронашао начин да приступи систему противника. Бранилац користи исте скенере вулнерабилности како би открио слабости властитог система. Уређај за пресретање пакета података (тзв. sniffing) је направљен како би администратор мреже могао да прати актуелни саобраћај у циљу откривања безбедносних пропуста на властитој мрежи. Откривене слабости се евидентирају од

стране администратора у циљу побољшања поузданости и безбедности властитих система. Нападач, пак, ове уређаје користи за откривање слабости противника.

Шести принцип: *и нападач и бранилац контролишу веома мали део кибер простора који користе. Онај који може да контролише противнички део кибер простора може да контролише и противника.*

Обе стране у кибер конфликту могу контролисати само хардвер и софтвер који поседују. У физичком свету, то је обим њиховог утицаја. Ретко када неки актер може контролисати нешто изван властитог интерфејса. Чак и америчко Министарство одбране, према проценама, контролише само 10% комуникационе инфраструктуре која се користи за комуникацију унутар Министарства.[376] Ово имплицира да, у било ком случају, ни нападач ни бранилац не могу контролисати 90% инфраструктуре коју користе приликом својих активности.

И поред тога што ниједна страна у кибер конфликту не контролише већи део инфраструктуре коју користи, чињеница је да су обе стране рањиве при нападу на ту инфраструктуру. Ако једна страна задобије контролу над противничким делом инфраструктуре, она стиче предност у односу на другу страну.

У пракси, најчешће се у ту сврху користе напади на противничке доменске сервисе (Domain Name Service – DNS)[377], како би се над њима задобила контрола. То се постиже или директним нападом на DNS сервер или одређеним информатичким техникама за „превару“ сервера. Једном када се задобије контрола над DNS-ом, када се успешно заобиђу безбедносни протоколи Интернета (Internet Protocol Security – IPSEC), непријатељ постаје рањив на многе врсте обмањивачких напада.

Седми принцип је предочен следећом тврдњом: *кибер простор није конзистентан, нити је поуздан.*

Последица вештачке природе кибер простора јесте та да он није постојан, а самим тим, није ни поуздан. Овај принцип је повезан са трећим принципом који

---

[376] Parks R., Duggan D., *op. cit*., p. 124.

[377] Domain Name System (DNS) је систем који дели цео Интернет у поједине домене. Сваки домен користи nameservere који познају IP адресе и имена рачунара који се налазе у подручју тог домена. Сви nameserveri су међусобно повезани у облику стабла те се могу посматрати као једна велика централна база података.

говори о непостојању непроменљивих закона у кибер свету. У кибер простору нити хардвер нити софтвер неће увек радити онако како се од њих очекује. Ово претежно важи за софтвер, али се уочава и недоследност у функционисању хардвера, најчешће услед варирања температуре или напона у електричним инсталацијама.

Последица овог принципа је да ниједан агресор у кибер рату никада не може бити сигуран да ће напад успети.

Осми принцип гласи: *физичка ограничења у односу на раздаљину и простор нису применљива на кибер свет.*

У кибер свету, физичка раздаљина није препрека за извођење напада. Кибер напад може бити изведен, са једнаком делотворношћу, са другог континента као и из суседне просторије. У кинетичком ратовању напади се спроводе пројектилима који морају прећи одређену раздаљину. Изазивање одговарајуће штете у физичком свету, дакле, има просторна ограничења. Стварање штете посредством кибер света, чини се, таква ограничења нема.

3.8. Преглед важнијих кибер напада

Досадашња елаборација проблема истраживања указала је на чињеницу да употреба информационо-комуникационих технологија у савременим сукобима добија све већи значај, не само у војној већ и у цивилној сфери. Ратовање у кибер простору пружа значајне предности – нападач се лично не излаже опасностима а притом лако и брзо може угрозити противничке циљеве. Поред тога, ова форма сукоба најчешће не дозвољава да идентитет и одговорност актера буду јасно идентификовани.

У овом одељку рада описан је и анализиран Руско-грузијски конфликт на глобалној рачунарској мрежи који је 2008. године вођен упоредо са копненом офанзивом руских снага. Овај сукоб у кибер простору многи теоретичари сматрају Другим кибер ратом.

Осим тога, у овом одељку рада дали смо увид у хронологију кибер инцидената након Руско-грузијског конфликта, у намери да сагледамо правце ширења овог феномена. Размотрена су питања идентитета нападача, њихове мотивисаности за извршење напада, коришћених средстава али и друга значајна питања за разумевање суштине и специфичности кибер ратовања.

3.8.1. Место и улога Интернета у Руско-грузијском конфликту 2008. године

У априлу 2007. године Естонија је оптужила Русију за кибер напад на њене информационе инфраструктуре што је, посредно, довело до угрожавања националног суверенитета.[378] Овај случај, нагласили смо, многи сматрају првим конфликтом који може бити назван кибер ратом.[379] Само годину дана након што је оптужена за ове нападе, Русија је у августу 2008. године поново оптужена за извођење кибер напада на Грузију.

У новембру 1989. Јужна Осетија је прогласила аутономију од Совјетске Социјалистичке Републике Грузије. Од тада, новонастала држава има напет однос са Грузијом који се коначно претворио у оружани сукоб. Да би поново успоставила контролу, Грузија је 8. августа 2008. године покренула војну офанзиву против отцепљене Јужне Осетије. Будући да већина грађана Јужне Осетије има руски пасош, Русија је на потез Грузије одговорила слањем тенкова да би одбранила оне које сматра својим грађанима. Док су се осетијске, грузијске и руске трупе бориле на земљи, сукоби су се разбуктали и на Интернету.

3.8.1.1. Хронологија догађаја у кибер простору

Први напад *дистрибуиране опструкције услуге*[380] догодио се 20. јула 2008. године и циљао је web сајт Михаила Сакашвилија (www.president.gov.ge), председника Грузије.

---

[378] Овај догађај је у неколико наврата разматран у претходним одељцима рада.

[379] European Parliament. Session of the European Parliament of 9th of May 2007, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//TEXT+CRE+20070509+ITEM-012+DOC+XML+V0//PT (retrieved, 2007)

[380] Да подсетимо, кибер напади под називом дистрибуирана опструкција услуге (Distributed denial of service – DDoS) имају за циљ да онемогуће клијенте или организацију да користе услуге рачунарске мреже или информационих ресурса. Опструкција електронских услуга постиже се нападом на системе који омогућавају те услуге (на пример, нападом на сервер на коме су ускладиштени web сајтови или на сервер електронске поште). Ова врста напада циља на доступност информација, а не на њихову поверљивост. Након ових напада најчешће нема крађе информација или осталих губитака информација поверљиве природе. Основна штета узрокована DDoS нападом испољава се у времену које је потребно утрошити да би се нападнути систем поновно оспособио. Најчешће коришћен метод за извођење ове врсте напада је излагање рачунара или рачунарских мрежа огромном броју захтева концентрисаних у кратком временском периоду. Процес напада је аутоматизован и започиње тако што нападач присваја контролу над првим рачунаром који постаје „мастер“ напада. Преко мастера се хиљаде других рачунара инфицирају малициозним кодовима и они постају такозвани „зомбији“. Зомби-рачунар сада може да изврши било коју акцију предвиђену програмом малициозног кода, коју позивањем једне једине команде са дистанце иницира нападач а да, притом, легитиман корисник рачунара тога не буде свестан. Коришћењем ове изузетно једноставне операције, хиљаде инфицираних рачунара (који творе компромитовану рачунарску мрежу botnet) могу да истовремено покрену напад DDoS против циља који је нападач одабрао.

Осмог августа је на мети DDoS напада био сајт Одбора за вести и медије владе Јужне Осетије (www.cominf.org), само неколико сати након што је грузијска војска извршила нападе на осетијска села.

Затим је уследио дигитални напад на Грузију – координисан из домена www.stopgeorgia.info (сајт је био стациониран у Немачкој и брзо је затворен од стране власника web сервера) и домена www.stopgeorgia.ru. Овај потоњи сајт је био стациониран у Великој Британији. Креиран је 9. августа 2008. године, био је активан до 13. августа када је уклоњен да би, након 24 часа, поново почео са радом али без једног дела софтвера и са неисправним форумом. У прогласу публикованом на сајту могло се прочитати следеће:

„Ми, представници руског хакерског подземља, не можемо толерисати грузијско провоцирање у свим његовим манифестацијама. Ми желимо да живимо у слободном свету, без агресије и лажи у кибер простору. Не треба нам усмеравање од стране власти или усмеравање неких других људи, већ да делујемо у складу са убеђењима заснованим на патриотизму, здравом разуму и веровању у снагу правде. Можете нас називати кибер криминалцима или терористима, који изазивају рат и убијају људе, али ми ћемо се борити јер је неприхватљива агресија против Руске Федерације на Интернету.

Захтевамо престанак напада и позивамо све медије и новинаре да објективно извештавају о догађајима. Док се ситуација не промени, ми ћемо заустављати пласирање лажних информација из влада Западних земаља као и из владе и медија Грузије. Апелујемо на све који нису равнодушни на лажи политичких сајтова Грузије, и који су у могућности да забране ширење црне пропаганде, да дају свој допринос.“[381]

Са наведених сајтова било је могуће преузети алатке за извођење DDoS напада, алатке за изазивање „ping-flood“[382] напада, алатке за блокирање телефонског

---

[381] José Rios M., Tenreiro de Magalhães S., Santos L., Jahankhani H.: “The Georgia’s Cyberwar“, Jahankhani H., Hessami G. A., Hsu F. (Eds*.), Global Security, Safety and Sustainability*, 5th International Conference, ICGS3 2009, London, September 1-2, Springer-Verlag, Berlin – Heidelberg, 2009, p. 45.

[382] „Ping-flood“ (или само „flood“) напад је подврста DDoS напада. Ова врста напада такође подразумева слање великог броја захтева web серверу, са циљем да засити његов опсег и успори или потпуно прекине његов рад.

саобраћаја помоћу IP софтвера, као и алатке за блокирање саобраћаја мобилне телефоније засићењем телефонских линија генеричким SMS порукама. На овим сајтовима је, у периоду од 13. до 25. августа 2008. године, била истакнута и листа препоручених циљева, потенцијалних мета кибер напада.

Већина, у конфликту ангажованих, руских сајтова је ограничила своје акције на ширење линкова ка сајту www.stopgeorgia.ru, али су неки отишли и даље од тога. Тако је, на пример, сајт http://clubs.ya.ru позивао на слање „ping“ захтева метама назначеним на сајту www.stopgeorgia.ru. Други сајт (http://aeterna.ru) је садржао html фајл са приступом метама, који кроз аутоматско ажурирање странице (које је могуће у неким web претраживачима) загушује циљане сервере непотребним саобраћајем.

Неки од руских сајтова су, такође, садржали и листу грузијских web сајтова који су рањиви на „SQL injection“[383] нападе, објашњавајући, за сваки случај, и начин за постизање најдеструктивнијег ефекта.

Једанаестог августа били су на мети web сајтови грузијског Парламента (www.parliament.gov.ge), Министарства спољних послова (www.mfa.gov.ge) и Националне банке Грузије. Почетне стране ових сајтова биле су замењене фотомонтажама слика председника Сакашвилија и Адолфа Хитлера. Одговорност за напад је преузела, до тада непозната, група хакера која себе назива „Хакерска посада Јужне Осетије.“[384]

Сајтови грузијске владе постали су, као резултат поменутих DDoS напада, привремено недоступни. Техничку помоћ Грузији пружили су Естонија и председник Пољске који је понудио простор на свом сајту, како би грузијска „перспектива“ могла бити доступна јавности. Грузијски министар спољних послова одржавао је комуникацију оснивањем посебног блога (georgiamfa.blogspot.com). Web

---

[383] Техника напада под називом „SQL injection“ заснива се на рањивост појединих апликација рачунарског система. Рањивост се манифестује тако што апликација не филтрира корисничке податке на добар начин, пре него што их пошаље систему за управљање базама података (*енгл*. Data Base Management System). Корисник несвесно убацује злоћудан код у апликацију која користи SQL наредбе. Ако апликација корисников унос не филтрира на добар начин, SQL наредба шаље се систему за управљање базама података и активира. Према: Antončić V.: *Napadi s uskraćivanjem usluge (DoS napadi)*, http://os2.zemris.fer.hr/ns/2007_Antoncic/index.html#G.SQL-ubacivanje

[384] Ifrah L.: “The Georgia-Russia conflict: Internet, the other battlefield”, *Défense nationale et sécurité collective*, October 2008, Committee for National Defence Studies, Paris, 2008, p. 2.

сајт председника Сакашвилија био је од 9. августа смештен у Сједињеним Државама. Нино Доијасхвили, директор Тулип система – провајдера Интернет услуга из Атланте, иначе етнички Грузијац, тврдио је да су и његови сервери били нападнути од стране Москве и Санкт Петерсбурга.

Тринаестог августа сајт грузијског председника је поново постао недоступан, као и web сајтови царинске службе, владе и Министарства одбране.

Од 15. августа па надаље глобалном мрежом почео је да се шири спем заражен тројанским коњем[385], наводно послат од стране Би-Би-Си-ја. Написана на лошем енглеском језику, порука је тврдила да је председник Грузије хомосексуалац и нудила линкове са видео записима и компромитујућим сликама. Отварањем линка, на рачунар лаковерног корисника инсталирао би се вирус са именом „name.avi.exe“. Овај спем дошао је са неколико различитих IP адреса и указивао је на коришћење botnet-a. У то време, само 4 од 36 комерцијалних антивирусних програма било је у стању да открије поменути вирус.[386]

Други спем се појавио са наизглед уверљивијом темом убиства новинара у Грузији. Овај имејл садржао је линк ка сајту који инсталира малициозни програм (Trojan.Popwin) на рачунар корисника.

Главни напади циљали су на грузијске сервере како би преусмерили кориснике Интернета ка неаутентичним сајтовима који садрже патворене информације или странице заражене малициозним кодовима. На крају, треба истаћи да је међународна заједница брзо и ефикасно реаговала како би сачувала грузијске сервере.

У време напада, Грузија је приступ Интернету остваривала преко Турске и Русије. Међутим, од септембра 2008. године Грузија излаз на Интернет остварује преко мреже оптичког влакна која испод Црног мора повезује грузијску луку Поти са Варном у Бугарској.[387]

---

[385] О карактеристикама спема и тројанског коња видети више у одељку 3.4.1.1. Малициозни кодови.
[386] Према: Garwarner.blogspot.com.
[387] Ifrah L., *op. cit*., p. 4.

Међутим, важно је напоменути да ни један од ових напада није био једностран, пошто је и сама Русија била жртва неколико DDoS напада.

Од почетка сукоба многи сајтови руских медија били су недоступни на неколико сати: RiaNovosti, Lenta, ITAR-TASS, Regnum, Russiatoday и Rian. Осим тога, влада Грузије је онемогућила приступ сваком домену са екстензијом „.ru“ спречавајући, на тај начин, било какав приступ руским сајтовима са своје територије. Исто тако су и телевизијски линкови били одсечени, руска телевизија се није могла гледати у Грузији.

3.8.1.2. Актери напада

Збивања у Русији потврдио је и Роман Зхолус, први секретар Амбасаде Руске Федерације у Паризу. Он је инсистирао на томе да је кибер сукоб у Русији (као и у Грузији) дело обичних грађана различитих способности, те да свакако није дело ИТ професионалаца, а још мање специјалних јединица у служби државе. У том смислу, први секретар Амбасаде званично је негирао било какву умешаност Руске Федерације у ове нападе.

Са друге стране, грузијска амбасада у Паризу децидирано је тврдила да је, осим идеолошки мотивисаних напада грађана, било и оних од стране руске војске.[388] Да ли је разумно веровати у тезу да је Кремљ, пошто је одлучио да пошаље своје војнике и тенкове да физички нападну Грузију, имао интереса да пориче своју умешаност у веома мали кибер конфликт?

Иако штета настала овим кибер ратом није значајније угрозила националну безбедност Русије, а поготово не Грузије[389], важно је размотрити улогу државних и недржавних актера у овом сукобу у циљу бољег разумевања актуелног и, по свему судећи, будућег феномена кибер ратовања.

---

[388] *Georgia accuses Russia of waging cyberwar*, *CBC News*, August 12, 2008, http://www.cbc.ca/technology/story/2008/08/12/tech-georgia.html

[389] Статистика британске компаније Renesis, специјализоване за праћење преноса података на Интернету, показује да је Грузија 74. земља на свету по бројности IP адреса, иза Нигерије, Бангладеша, Боливије и Сан Салвадора. Напади на њене мреже имали су минималан учинак на функционисање државе, у поређењу са Естонијом када је већина онлајн сервиса било погођено.

Резултати кибер-форензичке анализе, спроведене након конфликта, показали су да је домен www.stopgeorgia.ru, који је стациониран у Великој Британији, у власништву особе са имејл адресом anac109@mail.ru, са контакт бројем телефона из Иркутска, у Сибиру.[390]

Додатна истраживања су показала да је ова имејл адреса коришћена за регистрацију других домена: dokim.ru и rakar.ru, оба са седиштем у Сједињеним Америчким Државама. Ова информација је ИТ форензичарима омогућила да дођу до детаљнијих података о власнику домена, попут његовог наводног имена: Андреј В. Угловатуј. Име је, готово сигурно, лажно будући да је домен dokim.ru намењен продаји кривотворених пасоша из Руске Федерације, као и из Литваније, Летоније, Велике Британије и Немачке по цени од 3000 до 3500 €. Домен rakar.ru такође се користи у нелегалне сврхе – за продају фалсификованих кредитних картица по цени од 70 до 450 US$.[391]

Резултати спроведене анализе наводе на закључак да координатор кибер напада на Грузију не може бити повезан са било којом званичном институцијом у Москви. Овом закључку у прилог иде и чињеница да су за извршење кибер напада коришћене веома несофистициране технике[392], што указује на несумњив аматеризам нападача.

Очигледно је да су у случају руско-грузијског конфликта главну улогу имали појединци и друштвене групе, способне и мотивисане да мобилишу неопходна средства, како би успешно извршили напад на противничке сајтове. Реч је о новом облику герилске борбе, такозваном „хактивизму“, која се води на електронском пољу или, другачије речено, о идеолошки мотивисаним актерима чије је деловање усмерено против електронских контролних и информационих система и технологија непријатељских земаља.[393] У прилог овом закључку иду и резултати истраживања Хозе Назариа (Jose Nazario), експерта за ИТ безбедност у компанији Арбор. Анализирајући нападе усмерене ка Грузији, овај стручњак је открио да су

---

[390] José Rios M., Tenreiro de Magalhães S., Santos L., Jahankhani H., *op. cit*., p. 50.

[391] *Ibid*., p. 50.

[392] Тако се, на пример, напад ускраћивања услуге „ping-flood“ лако може осујетити једноставним firewall заштитним зидом, док је за извођење DDoS напада коришћен комерцијални софтвер америчке компаније Socketsoft, који се употребљава за тестирање безбедности web сајтова.

[393] Феномен „хактивизма“ детаљније је објашњен у наредном поглављу рада.

пакети података садржали речи „win+love+in+Russia“, што потврђује политичку мотивацију агресора.[394]

На основу изнетог, готово је извесно да су за анализирани кибер конфликт одговорни руски и грузијски националисти – појединци и групе који су личним ангажманом желели да пруже подршку својој земљи.

Управо се ова тенденција померања кибер ратовања изван војних граница на индивидуалну, друштвену па и комерцијалну раван сврстава у битно обележје ове савремене форме сукоба. Док је појмовно одређење информационог ратовања истицало његову војну димензију, данас већи део литературе о кибер ратовању управо истиче аспект његовог проширења ван војних области.

Проширење делокруга кибер ратовања изван војних активности је, у техничком смислу, омогућено дифузном и децентрализованом структуром глобалне рачунарске мреже – Интернета. Сваки корисник рачунара је слободан да се у кибер простору понаша у складу са властитим политичким уверењима и да учествује у псеудо-војним акцијама ван било каквог формалног ланца команде. Суштински, феномен сукобљавања у кибер простору помоћу оружја које нуди сам кибер простор, и његово преливање у сфере „цивилног“ света узроковано је противречном природом процеса глобализације и идеолошким, политичким, културним и социјалним диспаритетима које овај процес носи.

Из наведених разлога државе, које су се определиле за пут информатизације својих виталних процеса, морају предузети мере за обезбеђивање властитог „сегмента“ кибер простора као засебне државне границе. Случајеви Естоније и Грузије су несумњиво показали да суверенитет државе може бити угрожен и из „виртуелног света“.

3.8.2. Хронологија конфликата у кибер простору након августа 2008. године

Након Руско-грузијског конфликта догодио се велики број инцидената у кибер простору. Кибер напади, готово свакодневно, погађају различите кориснике

[394] Ifrah L., *op. cit*., p. 3.

информационих ресурса на свим меридијанима. Ови напади се, наравно, разликују по интензитету, техникама и последицама које изазивају те их је могуће на одређени начин градирати. За поједине од њих се може рећи да заузимају значајно место у хијерархији овог вида друштвених конфликата јер су, у знатној мери, утицали на савремена социо-политичка збивања у свету. Због тога су, у стручној и научној литератури, они и окарактерисани као чинови кибер ратовања. Размотрићемо, хронолошки, неке од њих.

Мјанмар

У ишчекивању прве годишњице „Шафран револуције“, 23. септембра 2008, године, влада је лансирала DDoS нападе против сајтова који су подржавали будистичке монахе: *Iravadi*, *Демократски глас Бурме* који се налази у Ослу, и *New Era* из Бангкока. Новински лист *Australian* писао је о том догађају: „Усаглашени напади – за које се чини да долазе из Кине, Русије и Европе, као и саме Бурме – једино могу бити дело посредника бурманске владе и могу бити покушај да се компензује прошлогодишњи неуспех те исте владе да задржи мноштво слика које показују непрегледне колоне ненаоружаних демонстраната и њихово разбијање кишом метака и пендрецима.“[395]

Представник *Демократског гласа Бурме* саопштио је да су напади највероватније доспели са сајтова из Русије и Кине што би, уколико је истина, показало да је влада Мјанмара ангажовала спољне сараднике за ове нападе.

Зимбабве

Како је известило удружење *Concerned Africa Scholars* у децембру 2008., у есеју званом „Стаклена тврђава: Кибер герилско ратовање у Зимбабвеу“, Мугабеова влада покушавала је да уђутка опозицију техником ометања радио таласа и Интернета, као и контролисањем саобраћаја електронске поште са домена са екстензијом .zw. Обе стране у сукобу су се, наводно, бавиле променом почетних страна опонентских сајтова, као и лансирањем DDoS напада. Ови напади су започети 2005. године и још увек трају.[396]

---

[395] Carr J.: *Inside Cyber Warfare*, O'Reilly Media, Sebastopol, 2010, p. 39.
[396] *Ibid*., p. 38.

Израел и Палестинска Народна Самоуправа

Поред војне акције Израела против база Хамаса у Палестинској Народној Самоуправи током децембра 2008. (назване *Операција ливено олово*), дословно је хиљаде израелских и арапских, како владиних тако и цивилних сајтова било изложено хакерским нападима који су се користили техником измене почетне стране (defacement). У овим нападима наводно су учествовали и чланови Израелских одбрамбених снага и Хамаса, што их чини једним од ретких кибер догађаја у коме су званично учествовале државе.

Киргистан

Јануара 2009. године DDoS напад избацио је из функције два до три од четири државна Интернет провајдера на неколико дана, и тиме онемогућио приступ Интернету већини становништва у време нарастајућих политичких немира. Још увек није познато ко је одговоран за овај напад. У оптицају су три теорије:

- Напад је организовала руска влада у покушају да присили председника Киргистана да затвори ваздушну базу Манас за америчке авионе;
- Председник Киргистана унајмио је недржавне руске хакере са намером да онемогући опозиционим партијама употребу Интернета;
- Напад је био резултат борбе за надмоћ између конкурентских Интернет провајдера.[397]

САД

Вол Стрит Џурнал (Wall Street Journal) је објавио, 21. априла 2009, да је безбедност Пентагоновог пројекта *Joint Strike Fighter* компромитована и да су непознати хакери, за које се претпоставља да су из Народне Републике Кине, украли неколико терабајта података.

Од 4-6. јуна 2009., DDoS напад релативно малих размера и непознатог порекла лансиран је против двадесет пет америчких владиних сајтова, од којих су неки због тога били недоступни и по неколико дана, укључујући и сајтове Федералне трговачке комисије и Министарства финансија, док су остали са листе, као што је

[397] *Ibid*., p. 38.

сајт Беле куће, били без последица. Други и трећи талас ових напада наредних дана је погодио сајтове владе Јужне Кореје.

Исте године догодио се други значајан напад на простору САД којим је саботиран рад вентилационог система опште болнице у Тексасу.

Татарстан

У нападу који се догодио јуна 2009., сајт председника Татарстана био је оборен и онемогућен је приступ Интернету. Званичници Татарстана су за напад оптужили руску Федералну службу безбедности (ФСБ).

Иран

Током председничких избора у Ирану 14. јуна 2009., стотине хиљада Иранаца протестовало је оспоравајући изборне резултате. Један од облика протеста била је употреба DDoS напада усмерених против сајтова иранске владе. Популарни сервис за друштвено умрежавање *Twiter* послужио је, том приликом, као платформа за организовање напада.

Јужна Кореја

Током викенда 4. јула 2009. и првих дана наредне недеље, DDoS напад у коме је коришћено између 30.000 и 60.000 зомби рачунара оборио је не само комерцијалне сајтове, већ и сајтове влада САД-а и Јужне Кореје. Јужна Кореја веровала је да је за ово одговорна влада Демократске Народне Републике Кореје или њени посредници, док нико од званичника САД-а није изразио формално мишљење по питању атрибуције.[398]

Шведска

Октобра 2009. године око четрдесет сајтова у власништву шведске полиције и медија било је оборено нападом типа DDoS.[399]

---

[398] Arora K., et al.: "Impact Analysis of Recent DDoS Attacks", *International Journal on Computer Science and Engineering*, Vol. 3, No. 2, Feb 2011, p. 881.

[399] *Ibid*.

Иран

Септембра 2010. године компјутерски вирус „Stuxnet“ заразио је рачунаре иранске нуклеарне електране „Бушер“. *Њујорк тајмс* је у јануару 2011. потврдио да овај опаки компјутерски вирус, који је саботирао иранска нуклеарна постројења, није дело хакера, већ подухват САД и Израела и њихових тајних служби, ЦИА и Мосада. Компутерски експерти на које се позива „Њујорк тајмс“ тврде да је „Stuxnet“ нешто најсложеније што је досад направљено, кад је реч о кибер оружју. Програмиран је тако да обавља више задатака и да, док производи штету, корисник не може приметити његово присуство. Поједини његови делови се по „обављеном задатку“ уништавају, а неки тек накнадно откривају.[400]

Списак кибер напада који смо навели, почев од унутрашњих покушаја да се уђуткају опозициони покрети (Зимбабве, Киргистан) до хакера ангажованих од стране државе са циљем преузимања стратешких сајтова (Израел, Палестинска Народна Самоуправа), илуструје колико је широко ово подручје. Било би наивно помислити да је до сада виђен сваки облик испољавања напада из широког спектра кибер ратовања.

Чини нам се да је овај преглед важнијих кибер конфликата у последње четири године, иако штур, довољан да подстакне на размишљање. На првом месту, намеће се питање који од претходно поменутих догађаја заиста може понети епитет кибер рата. Са формално-правног становишта одговор је јасан -ниједан од поменутих. До данас нема правног ентитета који се може назвати „кибер рат“. Међународним споразумима једино је дефинисано право државе да се брани када је нападнута, у смислу традиционалног, оружаног, напада.[401] Проблем правног статуса кибер ратовања подробније ћемо размотрити у последњем поглављу рада.

---

[400] „САД и Израел бацили сајбер бомбу на Иран“, Дневни лист *Политика*, 17. јануар 2011, стр. 1.

[401] Аврамов С., Креча М.: *Међународно јавно право*, Правни факултет Универзитета у Београду и Службени гласник, Београд, 2006, стр. 601.

4. ВИДОВИ КИБЕР РАТОВАЊА

Лексикон кибер ратовања постоји већ више од две деценије али се током већег дела тог периода скоро искључиво користио у круговима Министарства одбране САД. У затвореном свету Пентагона и његових огранака, искристалисао се нови, радикалнији концепт постиндустријског ратовања, који је био осмишљен како би се наставила америчка војна доминација у раздобљу након Хладног рата. Постоји обимна литература о теорији и пракси кибер ратовања, чији је већи део јавно доступан. Први научни радови о овом феномену појавили су се почетком деведесетих година прошлог века.[402]

И данас су у употреби терминологија, стил и метафоре који су претежно војног карактера, што прикрива чињеницу да многи од темељних принципа и претпоставки кибер ратовања имају примену која је много шира од пуког војног контекста.

Концепт кибер ратовања заслужује да буде ослобођен од својих чисто војних асоцијација и уведен у друге дискурсе који се баве изучавањем друштвених последица глобалне компјутеризације. Средства и технике кибер ратовања се могу препознати у мноштву цивилних контекста (од компјутерских превара до кибер шпијунаже), и постоји довољно доказа за претпоставку да ће се овај тренд само појачавати, што ће довести до потенцијално озбиљних социјалних проблема и стварања нових изазова за националне кривично-правне системе.

Појам „кибер ратовање“ се првобитно повезивао са високотехнолошким оружјем и призорима вођених ракета које непогрешиво погађају ирачке а потом и српске војне циљеве. Посматрање ратова са безбедне раздаљине, посредством медија, створило је поједностављену и прочишћену визију кибер ратовања. Почетно интересовање медија било је усмерено на паметне бомбе и интелигентне борбене

---

[402] На пример: De Landa M.: *War in the age of intelligent machines*, Swerve Press, New York, 1991.; Libicki M. C.: *What is information warfare?*, National Defense University, Institute for National Strategic Studies, Washington DC, 1995.; Schwartau W.: *Information warfare. Cyberterrorism: Protecting your personal security in the electronic age*, Thunder's Mouth Press, New York, 1996.; Adams J.: *The next world war: Computers are the weapons and the front line is everywhere*, Simon & Schuster, New York, 1998.; Denning D.: *Information warfare and security*, Addison-Wesley, Reading, 1999.

системе – опипљиве реквизите дигиталног борбеног поља – што је замаскирало потенцијално дубље друштвене импликације виртуелних ратних стратегија. Перцепција се, временом, почела мењати јер је научна и стручна анализа феномена кибер ратовања, као централне технике овог вида ратовања, истакла компјутерско хакерисање и уништавање података. Упркос поједностављењима и забунама, централна претпоставка кибер ратовања је да је памет битнија од снаге. На бојном пољу данашњице, било оно војно или цивилно, информациона технологија је постала пресудни фактор. Традиционална схватања о основама надмоћи и динамици моћи која постоји између нападача и мете ће, по свој прилици, морати да буду редефинисана.

Традиционална поимања борбе подразумевају одређени паритет у смислу бројности и почетних позиција – један вод неће се сукобити са батаљоном, мало предузеће неће преузети велику компанију итд. Наравно, историја је препуна изузетака од овог неписаног правила – паравојне формације, герилски покрети, нагли успеси нових компанија. У електронској арени, са друге стране, аксијалне претпоставке о паритету снага не морају нужно важити. Војна сила је децентрализована те се дигитални Давид, скоро без икаквих ризика (користећи ПДП енкрипцију)[403], може супротставити наизглед заштићеном Голијату. Ову ситуацију Кузумано и Јофи називају „џудо стратегијом“, што би значило, окретање величине непријатеља – у овом случају информатичке снаге – у корист нападача.[404]

---

[403] Скраћеница ПДП означава врсту енкрипције која гарантује „прилично добру приватност“. Изведена је из *енгл*еске синтагме Pretty Good Privacy – PGP. Реч је о необично јаком облику енкрипције, заснованом на криптографији јавног кључа која криптографима омогућава знатну предност над криптоаналитичарима. ПДП енкрипцију изумео је Фил Цимерман крајем осамдесетих година прошлог века. Према: Синг С.: *Књига о шифрама – умеће тајних комуникација од древног Египта до квантне криптографије*, ДН Центар, Београд, 2010, стр. 355-385.

[404] Cusumano M. A., Yoffie D. B.: *Competing on Internet time: Lessons from Netscape and its battle with Microsoft*, Free Press, New York, 1998.

Табела бр. 5: *Војни приступ у класификацији мета, циљева и средстава кибер ратовања*

МЕТА НАПАДА	ЦИЉ НАПАДА	СРЕДСТВА НАПАДА
Материјална имовина	Оштећење или уништење информационих и комуникационих система противника.	•Конвенционалне технике и средства ратовања
Нематеријална имовина	Инфилтрирање у противничке информационе системе и њихово подривање посредством рачунарске мреже или убачених агената и инсајдера. „Крековање“ заштитних програма и нарушавање перформанси информационих система противника.	•Малициозни кодови •Опструкција услуга •Социјални инжењеринг •Фишинг
Психолошке компоненте	Неприметни упад у информационе и комуникационе системе противника како би се контролисао пријем информација, обликовало мишљење, спроводиле обмане, и учестовало у „неокортикалном“ ратовању.	•Малициозни кодови •Социјални инжењеринг •Фишинг

Класификација мета, циљева и средстава кибер ратовања приказана у Табели 5, радо је прихваћена од стране оружаних снага различитих држава. Међутим, ова класификација не узима у обзир ефекте кибер напада што, са безбедносног, етичког и правног становишта, представља значајан недостатак. У ери глобалне умрежености кибер ратовање има потенцијално много шире импликације за друштво у целини, на шта је Истраживачки центар Ранд (Rand Research Agency) указао још 1995. у издању које је било посвећено кибер рату и безбедности у кибер простору.[405]

У овом поглављу рада размотрићемо четири сфере дејствовања у којима је кибер ратовање постало уобичајена појава: војна, корпоративно-економска, друштвено-социјетална и лична. Одређени концепти, стратегије и примене кибер ратовања су заједнички за сва четри окружења, иако могу постојати разлике у тумачењу, као и разлике у поимању легалности, етичности, и социјалне пожељности исхода којима различити учесници теже у различитим околностима. Наша намера је да осмислимо аналитички оквир за разумевање кључних димензија кибер ратовања као и да размотримо неке од многобројних друштвених импликација које се могу

[405] Cronin B., Crawford H., *op. cit*., p. 258.

јавити као последица кооптирања технологија глобалног умрежавања за вођење кампања кибер ратовања, без обзира на то да ли су оне по карактеру војне или цивилне, колективне или индивидуалне, систематске или алеаторне.

4.1. Војни аспект кибер ратовања

До пре десетак година у америчким војним круговима постојали су информисани скептици, који су одбацивали теорију кибер ратовања као „климаву визију рата... која убедљивије делује стратезима одбране него непријатељима Америке“.[406] Данас, међутим, више нико не доводи у питање реалност ове теорије.

На почетку двадесетпрвог века појам кибер ратовање је у широкој, мада недоследној, употреби у војним круговима САД-а, где су реторичко надмудривање и ривалство међу војним родовима увек присутни, док се различите интересне групе надмећу за јурисдикцију и контролу над активностима кибер ратовања. Пентагон улаже значајне суме у развој стратегија кибер ратовања (како офанзивних, тако и дефназивних), као и информационо-комуникационих технологија у намери да додатно ојача националну војну надмоћ.

Сједињене Америчке Државе систематично развијају нову врсту оружја, базираног на новим технологијама, али без до краја уобличене и промишљене стратегије. Оне су оформиле нову војну команду како би водиле нови високотехнолоши рат, без јавне дебате, дискусије у медијима, без парламентарног надзора, академских анализа и међународног дијалога.

Првог октобра 2009. године почела је са радом Кибер команда (U.S. Cyber Command), војна организација чији је циљ употреба информационих технологија и Интернета као оружја. Сличне команде постоје у Русији, Кини и мноштву других земаља. Ове војне и обавештајне организације припремају бојно поље развијајући алатке које се називају *логичке бомбе* и *trapdoors*, постављајући у мирнодопско време ове „виртуелне експлозиве“ у друге државе. У припремној фази цивили постају жртве покуса. Брзина којом хиљаде циљева могу бити погођене, широм света, носи са собом перспективу високо насилних криза.

---

[406] Peters R.: “How Saddam won this round“, *Newsweek*, November 30, 1998, p. 39.

Један од највећих апсурда у вези са протагонистима кибер рата можда је управо тај да су САД, док се припремају за офанзивне нападе, најугроженије од истих будући да истрајавају на политици која их чини неспремним за одбрану од кибер напада. Идејни творац новог офанзивног оружја, САД, може постати губитник у кибер рату јер не зна како да се брани од оружја које је сам изумео.[407]

У претходном поглављу рада пружили смо увид у различита појмовна одређења кибер ратовања. Суштински, може се рећи да кибер ратовање подразумева опсег мера или акција које за циљ имају да заштите, искористе, оштете, одбаце, или униште информације или изворе информација како би се постигла предност или победа над непријатељем.

Дакле, типичан циљ конвенционалног ратовања је уништење или смањење материјалних ресурса непријатеља, док је циљ кибер ратовања напад на информационе системе и инфраструктуру, на такав начин да резултирајућа штета не буде одмах видљива. Овакви напади, названи су „soft kills“ - онеспособљавање противника. У практичном смислу, кибер ратовање подразумева инфлитрирање у непријатељске информационо-комуникационе системе, нарушавање њихове операбилности или њихово подривање коришћењем логичких бомби, рачунарских вируса и других средстава кибер ратовања. Међутим, оно истовремено проширује и традиционална схватања психолошког ратовања. Циљ кибер ратовања може бити и неприметно упадање у информациони или комуникациони систем непријатеља како би се обликовала перцепција, спроводиле обмане, или усадио осећај несигурности – што је Шафрански назвао *епистемолошким* или *неокортикалним ратовањем*.[408]

Пропаганда и кампање за ширење дезинформација су дуго времена биле темељи конвенционалног ратовања. У борби за придобијање подршке контрола над медијима била је главни циљ. Ни појавом Интернета се суштински није много тога променило али се, у одређеном смислу, ситуација закомпликовала. Интернет је пружио могућност оглашавања најразличитијим појединцима и групама. Због вишесмерних комуникационих особина глобалне рачунарске мреже постало је могуће допрети до много ширег аудиторијума. У информационом добу, могућност

[407] Clarke R., Knake R.: *Cyber War*, Harper Collins Publishers, New York, 2010, pp. X – XIII.
[408] Szafranski R.: "Neo-corticalwarfare: The acme of skill?", *Military Review*, November 1994, pp. 41–55.

оглашавања доступна је свима, без обзира на политичку и идеолошку позицију учесника у процесу комуникације и на природу поруке која се одашиље. Једносмерни канали данас су замењени комуникационим обрасцем на принципу ризома, који скоро да и не оставља могућност за контролу и цензуру.

Битна обележја кибер ратовања детаљније смо описали у претходном поглављу рада. У циљу бољег разумевања предности које кибер ратовање пружа са становишта војних активности ове карактеристике се могу представити у сублимираној форми.

Табела бр. 6: *Карактеристике кибер ратовања*

- Кибер ратовање се може сврстати у операције ниског интензитета;
- Усмерено је на нематеријалну имовину;
- Карактерише га асиметрија у погледу бројности и почетних позиција;
- Отпочиње без упозорења;
- Дешава се у реалном времену;
- Као оружје користе се разновсна средства, алати и технике;
- Средства и алати кибер ратовања имају двојаку намену – офанзивну и дефанзивну;
- Софистицираност ИКТ је у сразмери са подложношћу нападима;
- Кибер ратови се могу поделити на офанзивне и дефанзивне;
- Напад је усмерен на рањивости критичне инфраструктуре;
- Нападач диктира правила ратовања;
- Обавештајна делатност је веома значана са стратегијског становишта.

Кибер ратовање пружа агресору бројне предности у односу на конвенционално ратовање. Поред малих трошкова приступа, у предности потенцијалног нападача спадају и лакоћа, брзина и тајновитост којима се планирани напад може спровести, као и опсег домашаја који глобална мрежа омогућава. Више ни даљина нити „неслога читаве машинерије“, да цитирамо Карла фон Клаузевица, не могу спутати потенцијалног нападача. Географија, терен и логистика постају безначајни чиниоци. Борбена зона се, теоретски, налази било где на мрежи. Међу најважније карактеристике кибер ратовања можемо сврстати и скоро потпуну

анонимност нападача као и немогућност сагледавања праве природе његових намера, што му пружа психолошку предност у односу на противника.

Психолози управо наглашавају овај значајан феномен који доприноси опредељености војног менаџмента за вођење кибер рата - кибер ратник се увек налази изван видокруга и домашаја мете (он је анониман током контакта са непријатељем) што код њега ствара осећај равнодушности према жртвама.[409]

Табела бр. 7: *Предности нападача*

- Нападача је обично немогуће идентификовати;
- Предност брзог удара;
- Флуидност начина напада;
- Могућност контролисања фреквенције и интензитета напада;
- Велики избор средстава и техника за извршење напада;
- Лака мобилизација савезника;
- Нападнута страна се ставља у потчињен положај;
- Нападнута страна мора претрпети колатералну штету;
- Понашање нападнуте стране се на силу мења;
- Етичка и легална неодређеност кибер агресије;
- Равнодушност према жртвама.

Свакако, кибер ратовање представља двосекли мач за нације са високом концентрацијом информација, попут САД-а. Што се војне структуре више ослањају на комплексне мреже и „интелигентно наоружање“, то су изложене већој опасности да их неприметно нападну материјално много слабији непријатељи који добро познају информационо-комуникационе технологије. Управо је овај аспект кибер ратовања – диспропорционалност у погледу ресурса – привукао највише пажње како међу војним планерима, тако и међу медијским аналитичарима, и подстакао мноштво расправа о офанзивним и дефанзивним стратегијама информационог ратовања. У ратовању заснованом на информационим технологијама, нападач има

[409] Meinel C. P.: “How hackers break in... and how they are caught“, *Scientific American*, October 1998, pp. 98 –105.

већу вероватноћу да постигне стратешко изненађење него у конвенционалним формама војних сукоба.

Поред тога, значајно је и одсуство раног упозорења, као потешкоћа да се сазна да ли је и до ког ступња „провађено“ у нечији систем и колико је исти угрожен – војним жаргоном речено, конфузија у смислу „ефекта оружја“, стварног узрока штете начињене одређеним оружјем или стратегијом напада. Такође, изазов може представљати и разлучивање да ли су у питању напади који угрожавају националну безбедност или су, суштински, од локалног значаја.

4.1.1. Преглед активности појединих држава и војних савеза предузетих у функцији развоја офанзивних активности кибер ратовања

Посматрано из историјске перспективе, кибер ратом првобитно су називани информатички напади који су пратили конвенционалне војне нападе или дипломатске инциденте. Један од првих напада тог типа догодио се 1999. године након бомбардовања кинеске амбасаде у Београду током ваздушне кампање НАТО. Овај конвенционални војни напад Алијансе изазвао је жељу за реваншизмом - уследио је низ напада од стране НР Кине на web странице америчких институција.

Па ипак, у самим зачецима развоја кибер оружја националне армије су испољавале опрезност у погледу његовог коришћења, опрезност једнаку оној везаној за употребу нуклеарног, биолошког и хемијског наоружања. Технолошки развијене армије су, такорећи, зазирале од употребе овог оружја против непријатеља који има једнаку технолошку моћ, то јест могућност да одговори на исти начин.

У стратешком контексту информационог доба доведена је у питање не само ефикасност противнапада већ и сама могућност одбране – да ли, и на који начин, може реаговати држава која открије да је нападнута кибер оружјем и има „војну“ способност да одговори? У периоду када је доминирала претња нуклеарним нападом механизам одговора је био релативно једноставан – непријатељ је био познат као и његове могућности и намере. Постојали су (и још постоје) техничко-технолошки системи који у делићу секунде сигнализују лансирање ракета са нуклеарним главама. У случају кибер претње, показали смо, околности су другачије: не само да је непријатељ *a priori* непознат, већ га је тешко идентификовати чак и након извршеног напада. Коме у том случају узвратити?

Без обзира на поменуте потешкоће, могућност да једна држава потегне за коришћењем кибер оружја неки осећају као реалну претњу – поготово оне државе које су зависне од властите информационо-комуникационе инфраструктуре.[410] Русија је, на пример, покушала да иницира забрану његовог коришћења на међународном нивоу. Два предлога у том правцу била су понуђена у УН 1998. и 1999. године, али нису прихваћена због противљења САД.[411]

На основу увида у доступну научну и стручну литературу, може се закључити да је на почетку XXI века, осим САД, и неколико других држава интензивно радило на развијању дефанзивних и офанзивних стратегија кибер ратовања. О овом феномену се, додуше, може судити само на основу отворених извора али су и они довољни да потврде изложени закључак.

Тако је још 2000. године представник ЦИА дао следећу изјаву: „Уочавамо, и то у појачаном опсегу, појављивање доктрина и наменских офанзивних програма за кибер ратовање у другим државама. Идентификовали смо их неколико, на основу обавештајних информација, које развијају офанзивне кибер програме под окриљем својих влада. Стране државе почеле су да укључују информационо ратовање у своје војне доктрине, као и у наставне програме војних академија, бавећи се и офанзивним и дефанзивним применама. Оне развијају стратегије и алате како би спроводиле информационе нападе.“[412]

Опште је позната чињеница да Сједињене Америчке Државе предњаче у истраживању дефанзивних и офанзивних метода кибер ратовања и могућности њихове примене. Политички и војни естаблишмент САД увелико перципира информатички рат као нови вид ратног конфликта. Почетком овог века америчко Министарство одбране формирало је посебну јединицу за ове намене. Она је

---

[410] У технолошки развијеним земљама све основне јавне услуге (као што су дистрибуција електричне енергије, поштански и телекомуникациони саобраћај, као и ваздушни саобраћај) засноване су на информационо-комуникационим технологијама. Кибер напад који би ускратио неку од ових услуга, не само да би изазвао панику већ би и угрозио функционисање нападнуте земље.

[411] Denning D.: “Reflections on Cyberweapons Controls”, *Computer Security Journal*, Vol. XVI, No. 4, 2000, pp. 43–53.

[412] Изјава Џона Сирејбијана (John A. Serabian, Jr.), менаџера за питања информационих операција, Централна обавештајна агенција, пред Удруженим економским Комитетом оба дома америчког Конгреса о кибер претњама и економији САД-а, 23. фебруар 2000. Наведенео према: Carr J., *op. cit*., p. 161.

основана под окриљем америчке авијације у савезној држави Тексас. Од оснивања, јединицу није сачињавало само техничко особље већ и стручњаци за међународне односе и стратешке студије.[413]

Успостављањем функције кибер-команданта, у Сједињеним Америчким Државама је прихваћена чињеница да су, са војне тачке гледишта, операције у кибер простору једнако важне за одбрану државе као и копнене, ваздушне и поморске борбене снаге. Постоји једна велика разлика - копнени, ваздушни и поморски ратови су се, у случају Америке, увек водили ван њених граница. Операције у кибер простору воде се унутар националних граница.

Првобитна америчка стратегија је била дефанзивно оријентисана. Задатак кибер ратника био је да спрече хакере, терористе и непријатељске армије да блокирају комуникације и информационе инфраструктуре те да на тај начин доведу земљу у хаос. Ова америчка визија кибер рата произашла је, у највећој мери, из потпуне зависности економије ове земље од Интернета и осталих информационих технологија.

Својеврстан искорак ка офанзивној употреби кибер оружја учињен је у октобру 2010. године, када је званично одобрена (али не и јавно објављена у целости) *Национална кибер стратегија САД.* У својој првој, официјелној, кибер стратегији Пентагон је закључио да рачунарска саботажа која долази од друге земље може представљати објаву рата, што отвара могућност да Сједињене Државе узврате користећи традиционалну војну силу, известио је 31. маја 2011. онлајн дневни лист *Вол Стрит Журнал* (The Wall Street Journal).[414]

Пентагонова кибер стратегија, чији поверљиви делови до сада нису објављени, представља покушај да се ухвати корак с променама у свету у коме рачунарски напад може представљати значајну претњу америчкој националној безбедности, наводи *Вол Стрит Журнал*.

У чланку се истиче да је једна од замисли која добија на замаху у Пентагону појам „еквиваленције“ - ако кибер напад проузрокује смрт, штету, разарање или

---

[413] *Ibid*.

[414] *Cyber napad može značiti i "objavu rata"*, AbrašMEDIA, http://abrasmedia.info/društvo/nauka-i-tehnologija/cyber-napad-može-značiti-i-objavu-rata

велики поремећај које би изазвао и традиционални војни напад, тада би био кандидат за „употребу силе“ која би била равна одмазди.

Документ Пентагона има око 30 страна у строго поверљивој верзији и 12 страница у оној која је доступна јавности. У њему се закључује да се ратно право, изведено из различитих споразума и обичаја, које је током година постало водич за понашање у рату и сразмери одговора, примењује у кибер простору као у традиционалном ратовању.[415]

Стратегија још наглашава важност усклађивања америчке доктрине кибер ратовања са доктринама америчких савезника те одређивања нових начела безбедносних политика.

Додатни искорак ка офанзивној употреби кибер оружја учињен је у мају 2011. године када је председник САД Барак Обама потписао наредбу којом су војни команданти добили смернице за извођење кибер напада и других компјутерских акција против непријатеља широм планете. Наредба обухвата и употребу средстава за кибер ратовање у рутинској шпијунажи.

Стручњаци за рачунарску безбедност Министарства одбране САД су, том приликом, изјавили да се наређењем прописује када војска мора да тражи председниково одобрење за кибер напад на непријатеља. Према њиховим речима, на овај начин се употреба кибер капацитета уводи у ратну стратегију. Наредба представља круну двогодишње кампање Пентагона да се утврде правила која ће отворити пут за ратовање у кибер простору. Такође, каже се да председникове смернице јако личе на оне којим се уређује употреба конвенционалних ратних средстава.[416]

Позиција Велике Британије у вези кибер ратовања је врло слична америчкој, мада има извесне специфичности. За британске стратеге, прави циљ кибер ратовања је контрола над софтверима који омогућују дистрибуцију информација, како на тактичком тако и на стратешком нивоу. У том смислу, уместо израза информационо

---

[415] U.S. Army Forces Cyber Command, September 23, 2010, http://democrats.armedservices.house.gov/index.cfm/files/serve?File_id=067ffc96-e5c1-4cef-baa2-010d16e3be57

[416] „Pentagon od Obame dobio smernice za cyber ratovanje“, *Personal magazin*, http://www.personalmag.rs/internet/pentagon-od-obame-dobio-smernice-za-cyber-ratovanje/

ратовање или кибер ратовање чешће је у употреби израз *софтверско ратовање* (*енгл*. software warfare).[417]

Британска влада објавила је 2010. године нову стратегију националне безбедности у којој су кибер ратовање и тероризам наведени као највеће претње земљи. Иан Лобан, први човек државног *Центра за прикупљање обавештајних података* (GCHQ) сматра да напади у кибер простору, на владе и друге организације, представљају озбиљну претњу по британску информационо-комуникациону инфраструктуру, која је од кључне важности за земљу.

Безбедносна стратегија је први део ревизије одбрамбеног система Велике Британије. У оквиру ревизије, биће смањени и трошкови за оружане снаге - што је део општих мера штење чији је циљ да смање велики буџетски дефицит Британије.[418]

На самиту у Лисабону, новембра 2010. године, усвојен је нови Стратешки концепт НАТО-а. У овом документу, међу наважније циљеве организације које је потребно остварити до 2020. године, сврстана је и заштита од неконвенционалних претњи, тј. ажурирање приступа Алијансе приликом решавања криза изазваних претњама попут тероризма, пролиферације оружја за масовно уништење, кибер напада и прекида виталних енергетских токова снабдевања.

У тачки 12 Стратешког концепта констатује се да кибер напади постају све учесталији, организованији и много скупљи са аспекта штете коју изазивају по државну управу, пословање, економију и, потенцијално, транспорт и снабдевање енергијом и другу критичну инфраструктуру. Они представљају претњу по националну и Евро-атлантску безбедност, стабилност и развој. Као актери ових напада апострофиране су националне армије и обавештајне службе, организоване криминалне групе, као и терористичке и екстремистичке групе.[419]

Из тог разлога, документ истиче неопходност проналажења одговора на опасности од кибер напада, заштитом сопствених комуникационих и командних

---

[417] *Ibid*.

[418] „Британија против ´сајбер рата´“, *BBC Serbian*, http://www.bbc.co.uk/serbian/news/2010/10/101018_britishsecurity.shtml

[419] “Active Engagement, Modern Defence”, *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation*, Adopted by Heads of State and Government, Lisbon, 2010, p.4.

система, помагањем савезница да побољшају сопствене способности спречавања напада, и развијањем могућности за одбрану од кибер напада с циљем ефикасног откривања и одвраћања.

Информатички рат постаје једна од делатности која се најбрже развија у већини технолошки развијених земаља. То је област безбедности којом могу да се баве не само људи у униформама, него мање више сви они који управљају неким кључним сектором инфраструктуре који зависи од Интернета.

Обавештајне службе Вашингтона су нагласиле значајан напредак који је начинила Индија у том пољу. Њено Министарство одбране усвојило је план под именом „Information Technology Roadmap 2000“ који предвиђа информатизацију свих војних структура и усвајање дефанзивних и офанзивних система за информатичко ратовање.[420]

Сиромашне и технолошки слабије развијене земље, попут Палестине и Пакистана, такође су доказале оспособљеност да воде кибер рат технолошким инструментима који их чине равноправнима са високоразвијеним Западним земљама.[421]

Истраживања феномена кибер ратовања указала су и на значајну улогу Русије и Кине у овим активностима. Њихов став по овом питању је, међутим, доста другачији и изражава скуп њихових војних и политичких искустава из прошлости.[422]

Посебну пажњу стручњака у овој области последњих година привлачи све већа заинтересованост Кине за инструменте „војне информатике“.

Док пред очима светског јавног мњења делује да Америка и Кина остварују добру сарадњу у привредној и политичкој сфери, међу двема земљама непрекидно се дешавају забрињавајући дипломатски инциденти везани за војне обавештајне активности. Према извештају америчких обавештајних служби, Кина увећава своје капацитете за кибер ратовање развијајући системе одбране својих цивилних и војних

---

[420] Mega S.: *La Cina vuol spiare il Pentagono*, www.analisidifesa.it

[421] Putignano D. S.: *La criminalità informatica: cyberterrorismo*, Facoltà di Giurisprudenza, Università degli Studi di Bari, 2002.

[422] Strano M, Neigre B.,Galdieri P.: *Cyberterrorismo*, Jackson libri, Milano, 2002, p.103.

информационо-комуникационих инфраструктура против спољашњих напада, али и офанзивних система који су у стању да угрозе непријатељске информационе мреже.

У последњих неколико година све су учесталије критике Запада на рачун Народне Републике Кине, која се оптужује за вођење кибер рата. Према наводима Пентагоновог годишњег извештаја Конгресу о развоју кинеске војне моћи, Кина је у потпуности развила могућности за вођење кибер рата. Извештај објављен почетком 2007. године наводи да је Народна ослободилачка војска (People's Liberation Army – PLA) успоставила информациону борбену готовост и организовала специјално обучене јединице способне да развијају рачунарске вирусе ради напада на непријатељске рачунарске системе и мреже, као и посебне тактике и мере за одбрану сопствених и пријатељских рачунарских система и мрежа. Стручњаци наводе да је PLA још 2005. године почела да имплементира офанзивне мрежноцентричне операције у војне вежбе, те да је и овај сегмент кинеске борбене готовости, попут већине кинеских оружаних система, оријентисан на филозофију „првог удара" (*first strike*), односно да им даје предност напада у евентуалном кибер конфликту.[423]

Наводе из Пентагоновог извештаја власти САД су додатно поткрепиле у септембру 2007. године, када су саопштиле да су кинески војници током јуна месеца успели да продру у рачунарску мрежу Пентагона. Дневник *Фајненшл тајмс* објавио је, позивајући се на представнике Пентагона, да је морао бити заустављен рад неколико рачунара у кабинету министра одбране Роберта Гејтса. Амерички званичници су утврдили да су хакери имали увид у систем за размену електронске поште првог човека Пентагона: „Унутрашња контрола је показала да иза овог хакерског напада стоје припадници Народноослободилачке армије Кине."[424] Министар одбране Кине је том приликом демантовао било какву умешаност ове земље у инцидент.

Да се у виртуелном свету води прави рат, потврђује и реакција немачке канцеларке Ангеле Меркел, која је у септембру 2007. године јавно покренула питање напада кинеских хакера. Према тврдњама листа *Шпигл*, на мети кинеских хакера у мају 2007. године били су рачунари у седишту немачке канцеларке и

[423] „Кина спремна за cyber-рат", Com&GSM, M3 d.o.o., бр. 236, 2007, Београд, стр. 4.
[424] „Кинески хакери 'ушли' у Пентагон", RTV B92, 4. 9. 2007, http://www.b92.net/indexs.phtml

министарствима спољних послова, привреде и истраживања. Савезни биро за заштиту устава извршио је преглед владиних Интернет-инсталација и спречио да још 160 гигабајта информација буде премештено у Кину. Кинеске власти су и овога пута демантовале умешаност у догађај.[425]

Пошто су медији објавили информације о нападима у Немачкој и САД, у листу *Гардијан* објављена је вест да су хакери, за које се верује како су припадници Народне ослободилачке армије Кине, напали рачунаре у влади Велике Британије. Према наводима листа, у почетку се веровало да је реч о индивидуалном нападу, међутим, испоставило се да је реч о акцији организоване групе кинеских хакера. „Напади кинеских хакера трају већ четири године. Они рефлектују нову доктрину кинеске армије“, изјавио је Алекс Нил, експерт за Кину.[426]

Информационо-комуникациона инфраструктура Новог Зеланда је, такође, у септембру 2007. године била на мети напада. Ворен Такер, директор безбедносно-обавештајне службе Новог Зеланда, изјавио је листу *The Dominion Post* да је кинеска влада одговорна за напад, позивајући се на претходне наводе канадске тајне службе о шпијунским активностима држава.[427]

Оптужбе су уследиле недељу дана пошто је кинески министар иностраних послова демантовао умешаност кинеске владе у нападе на информационе системе Немачке, САД и Велике Британије: „Било која оптужба на рачун кинеске војске неоснована је, неодговорна и вођена прикривеним мотивима...“ „Колико сам ја упознат, до сада ниједна од поменутих држава није проследила кинеској полицији било какав захтев за спровођење истраге или помоћ у истој.“[428]

Према мишљењу појединих аналитичара, превасходни узрок подизања информационе борбене готовности кинеске војске јесте евентуална војна интервенција на Тајвану, острву које Кина сматра примарним питањем националне безбедности. Наводној епидемији хакерских напада које изводи кинеска армија, о

---

[425] „Кинези читали мејлове министра одбране САД“, дневни лист *Блиц*, 6. 9. 2007, http://www.blic.co.yu/

[426] *Ibid*.

[427] “China accused of cyberattacks on New Zealand”, *ZDNet Australia*, September 13, 2007, http://news.zdnet.com/

[428] *Ibid*.

чијој веродостојности ми, сигурно, не можемо судити на основу доступних извора, Пентагон је већ доделио шифровано име – *Титанијумска киша*.

Без обзира на то да ли су напади извршени у организацији кинеске војске или не, нема сумње да су их извели хакери „високог нивоа“, са значајним техничким и финансијским ресурсима и са детаљним познавањем инфраструктуре својих противника. Ови циљеви нису једноставни за остваривање, те их није могуће постићи пуком импровизацијом. Много је теже извршити напад који има за циљ прикупљање поверљивих и заштићених информација него саботирати непријатељске сервере, као што је то био случај у Естонији.

Према доступним отвореним изворима, који укључују објављене радове и говоре, као и наводе из званичних војних журнала, преко 120 нација се бави развијањем доктрина кибер ратовања. Јасно је да би комплетан приказ сваке од њих превазилазио могућности опсега овог рада. Због тога смо у овом одељку рада покушали да дамо увид у доктринарна документа оних држава којима се, у научној и стручној литератури, приписује оспособљеност за офанзивну и дефанзивну употребу кибер оружја, тј. које се перципирају као потенцијални главни носиоци активности кибер ратовања.

4.1.2. Место и улога кибер технологије у војним доктринама Сједињених Америчких Држава, Руске Федерације и Народне Републике Кине

4.1.2.1. Сједињене Америчке Државе

Оружане снаге САД-а публиковале су у протеклих десетак година највећи број докумената о начину вођења кибер ратовања, више од било које друге државе. Заправо, Народна Република Кина и донекле Руска Федерација, засноване су своје доктрине на америчким основама које су објављене у следећим приручницима:

- *Информационе операције,* уредба Министарства одбране No. 3600.1, из октобра 2001.
- *План информационих операција*, Министарство одбране, 30. октобар 2003.
- Војна публикација 3.1.3 о информационим операцијама, 13. фебруар 2006.

У претходном поглављу рада већ смо указали на чињеницу да се у западним војним круговима осим појма *кибер ратовање* употребљавају и технички термини *информационо ратовање* и *информационе операције*.

Према дефиницији америчког Националног универзитета одбране „информационо ратовање је приступ оружаном конфликту који се усмерава на руковођење и користи информације у свим облицима и на свим нивоима да би се остварила одлучујућа војна предност, посебно у здруженом (међувидовском) и комбинованом окружењу“.[429] Амерички експерт за електронско ратовање Шлехер под информационим ратовањем подразумева „акције предузете да би се остварила информациона супериорност, као подршка националној војној стратегији, утицањем на противничке информације и информационе системе, док се истовремено штите сопствене информације и информациони системи.“[430]

Најпотпунију и, за потребе овог истраживања, најприхватљивију дефиницију информационог ратовања дао је Шафрански, према коме је информационо ратовање „активност уперена против било којег дела система знања и веровања противника. Без обзира на то да ли се води против спољњег противника или унутрашњих група, информационо ратовање има крајњи циљ да употреби информационо оружје да би променило (утиче, манипулише, нападне) системе знања и веровања неког спољњег противника“.[431] Из ове дефиниције може се уочити да информационо ратовање, осим пропагандне димензије, подразумева и конкретне активности које се огледају у спровођењу напада информационим оружјем.

У контексту америчке војне доктрине појам информационо ратовање сведен је и на оперативном нивоу означен као *информациона операција* (*енгл*. Information operation – IO). Информационе операције подразумевају предузимање потезâ да би се деловало на непријатељске информације и информационе системе, док се у исто време штите сопствене информације и информациони системи. Информационе операције захтевају софистицирани развој, повезаност и ослањање на информационе

---

[429] Вулетић Д.: „Шта је информационо ратовање?“, *Безбедност*, бр. 3/05, Београд, 2005, стр. 496.

[430] *Ibid*.

[431] Вулетић Д.: *Кибер ратовање као облик информационог ратовања*, стр. 3, према: Шафрански Р.: *Теорија информационог ратовања - припрема за 2020. годину*, приказ чланка - превод пуковник Бајић, 2001, http://www.singipedia.com

технологије. Информациона операција циља на информације или информационе системе са намером да утиче на процесе који су засновани на информацијама, били они аутоматизовани или мануелно вођени. Информационе операције, такође, обухватају дејства која се предузимају у не-борбеној или нејасној ситуацији ради заштите властитих информација и информационих система, као и дејства која се предузимају да би се утицало на циљне информације и информационе системе.[432]

Осим наведених појмова, у војним доктринарним документима САД-а користи се и појам *мрежноцентричне операције* за описивање истог феномена.

Војник или цивил који у служби државе изводи мрежноцентричне операције - посебну врсту војне акције, планирану и координирану у оквиру шире војне операције, која у периоду мира може бити и чисто превентивног карактера назива се *кибер ратником* (*енгл*. cyberwarrior). Један од експерата у пољу безбедности кибер простора, Дороти Денинг, сматра да „слика војника који седи пред рачунаром и нечујно напада непријатељске мреже верно одражава суштину кибер ратника“.[433]

Године 2003. у америчким медијима објављена је вест да је председник Буш донео такозвану *Директиву 16* о националној безбедности.[434] Овај поверљиви документ је у једном угледном листу окарактерисан на следећи начин: „Према речима функционера администрације, председник Буш је потписао тајну директиву која наређује влади да први пут припреми националну доктрину која би одређивала како и када би САД могле да се непријатељима супротставе кибер нападом. Слична стратешка доктрина водила је коришћење нуклеарног оружја од Другог светског рата до данас. Водич за кибер рат требало би да одреди правила по којима би САД могле да продру у стране информатизоване системе и наруше њихов рад. САД, према званичним изворима, никада до сада нису извршиле масовне кибер нападе, али је Пентагон убрзао развој кибер оружја, предвиђајући да ће бинарни кодови једног дана бити коришћени уместо бомби за брже, и мање крваве, нападе против

---

[432] *Ibid*., стр. 499.

[433] Denning D.: “Cyberwarriors, Activists and Terrorists Turn to Cyberspace”, *Harvard International Review*, Vol. XXIII, No. 2, 2001, pp. 70–75.

[434] Потпун назив Директиве гласи: *National Security Presidential Directive 16 – To Develop Guidelines for Offensive Cyber-Warfare*, July 20, 2003. Садржај Директиве је поверљиве природе. Извор: The National Security Archive, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/index.htm

непријатељских мета. Уместо да ризикују авионе и трупе, војни стратези ће управљати војницима који помоћу рачунара нечујно нападају непријатељске мреже да би угасили радаре, онемогућили уређаје за производњу електричне енергије и прекинули телефонске везе.“[435]

Дефиниција мрежноцентричних операција дата је први пут у уредби Министарства одбране No. 3600.1, под насловом *Информационе операције*, из октобра 2001. године.

У наведеној публикацији, као и у потоњим уредбама, кибер ратовање, подразумева *операције помоћу рачунарских мрежа*, или *мрежноцентричне операције* (*енгл*. Computer Network Operations – CNO), које се заснивају на способности *напада помоћу рачунарских мрежа* (*енгл*. Computer Network Attack – CNA),[436] *заштите рачунарских мрежа* (*енгл*. Computer Network Defense – CND)[437] и *искоришћавању рачунарских мрежа* (*енгл*. Computer network exploitation – CNE).[438]

Мрежноцентричне операције, поменули смо, део су групе операција под називом *информационе операције*. Под информационим операцијама се подразумевају „акције предузете у циљу утицања на информације, информационе системе и процесе доношења одлука противничке стране, којима се истовремено бране властите информације, информациони системи и комуникациона инфраструктура“.[439]

Информационе операције су усмерене, и у нападу и у одбрани, на „доносиоце одлука, информације које они прикупљају и користе у доношењу одлука и комплетан спектар организација и система који учествују у прикупљању ових информација“.[440] Њихов циљ је постизање информационе супериорности, која се

---

[435] Graham B.*: Bush Orders Guidelines for Cyber-Warfare – Rules for Attacking Enemy Computers Prepared as U.S. Weighs Iraq Options*, http://www.washingtonpost.com

[436] Операције које имају за циљ манипулацију, прекид или уништење противничких информација унутар рачунарâ или рачунарских мрежа.

[437] Скуп напора за одбрану од противничких CNO.

[438] Активности које подразумевају формирање специјалних служби и спровођење операција помоћу којих се могу прикупити подаци из информационих система или мрежа противника.

[439] Дефиниција је, као и претходне, преузета из: *Directive Number 3600.1*, Rev. one, Department of Defense, October 2001.

[440] Joint Vision 2020, Director for Strategic Plans and Policy, J5: Strategy Division, US Government printing office, Washington DC, June 2000, www.dtic.mil/jv2020/jv2020.doc

огледа у „способностима непрекидног прикупљања и обрађивања информација и ширења њиховог тока, уз истовремено осујећивање исте способности противника и искоришћавање његових слабости.“.[441]

Према томе, примарни циљ информационих операција јесте противничко руководство (политичко, војно, социјално, културно) као и „процес доношења одлука“ противничког руководства. Осим тога, мете напада су и војна инфраструктура (комуникациони системи и обавештајне структуре), цивилне инфраструктуре (телекомуникације, транспорт, енергетски систем, финансијски систем, банкарство и финансије) и оружани системи (авијација, морнарица, артиљерија и ПВО системи).

Све информационе операције се реализују у оквиру много ширег контекста који се назива *информационо окружење*. Наведено окружење прожима и превазилази појединачне границе копна, мора, ваздуха, свемира и кибер простора.[442]

Информационе операције се, даље, могу поделити на две главне врсте: офанзивне и одбрамбене.

Офанзивне информационе операције подразумевају обједињену употребу формацијских и подржавајућих потенцијала и активности уз подршку обавештајног фактора, са циљем да се на непријатељској страни онемогући рад личностима које доносе битне одлуке и да се постигну или промовишу неки специфични циљеви. Формацијски и подржавајући потенцијали и активности обухватају: оперативну безбедност, војно обмањивање, психолошке операције, електронски рат, физички напад/уништење и специјалне информативне операције, а могу обухватити и напад на рачунарску мрежу.

---

[441] *Ibid*.

[442] Информационо окружење се дефинише као скуп појединаца, организација или система за прикупљање, обраду или дистрибуцију информација. У оквиру информационог окружења, могу се разликовати три концептуалне димензије: физичка, информациона и сазнајна. Употреба информација експоненцијално расте са развојем друштва. Савремено информационо окружење се манифестује кроз информациону инфраструктуру. Разликујемо глобалну, националну и војну информациону инфраструктуру. Према: *Information Operations Primer*, U.S. Army War College, Dept. of Military Strategy, Planning, and Operations & Center for Strategic Leadership, 2007.; Правило *FM 100-6: Information operations*, Department of the Army, Washington, DC, 1996.; *Joint Doctrine for Information Operations - JP 3-13*, Department of the Army, Department of the Navy, Department of the Air Force, 1998.

Одбрамбене информационе операције обједињују и координирају политику и процедуре, операције, људство и технологију са циљем да заштите и одбране информације и информационе системе. Одбрамбене информационе операције се изводе и потпомажу кроз осигуравање информација, безбедност информација, физичку безбедност, контраобмањивање, контрапропаганду, контраобавештајну делатност, електронски рат и специјалне информативне операције. Одбрамбене информационе операције обезбеђују благовремени приступ тачним и релевантним информацијама и истовремено непријатељу онемогућавају да се користи савезничким информацијама и информационим системима.

Министарство одбране САД је 2003. године објавило *Information Operations Roadmap*. У овом документу се, осим мрежноцентричних операција, под инфорамционе операције подводе још четири вида операција: психолошке операције (PSYOPS), електронско ратовање (EW), војна обмана (MILDEC) и заштита операција (OPSEC).

Од наведених пет централних активности информационих операција, психолошке операције, војно обмањивање и заштита операција су имале тежишну улогу у војним операцијама ранијег датума. У савременом добу, тим активностима су придодате, прво, електронско ратовање а потом и компјутерске мрежноцентричне операције, које су замениле физичко уништење као елемент информационих операција.

Психолошке операције обухватају активности чији је задатак да страном аудиторијуму пренесу одабране информације и индиције. Циљ им је да утичу на емоције, мотиве, начин размишљања и, коначно, на понашање страних влада, организација, група и појединаца.[443] *PSYOP* се примењује на стратегијском, оперативном и тактичком нивоу. На стратегијском нивоу, *PSYOP* често има облик политичких или дипломатских ставова или саопштења. На оперативном нивоу, психолошке операције могу обухватати дистрибуцију летака, емитовање садржаја помоћу разгласа, радио и ТВ емитовање и остале облике преношења информација

[443] *Doctrine for Joint Psychological Operations - JP 3-53*, Department of the Army, Department of the Navy, Department of the Air Force*, 2003.*

које подстичу непријатељске снаге на бежање, дезертирање или предају. *PSYOP* могу подржавати операције војног обмањивања.

Електронско ратовање се дели на три основна елемента: електронски напад *(EA),* електронску заштиту *(EP)* електронску ратну подршку *(EC).* Сва три елемента доприносе офанзивним и одбрамбеним информационим операцијама. Електронско ратовање је свака војна акција која подразумева употребу електромагнетне и усмерене енергије ради управљања електромагнетним спектром или ради напада на противника. Електронски напад подразумева акције предузете ради напада на непријатеља са намером да се наруши, неутралише или уништи непријатељски борбени потенцијал и спречи или умањи ефикасна употреба електромагнетног спектра непријатеља.[444] Електронска заштита подразумева акције као што су самозаштитно ометање и контрола емисије ради заштите употребе савезничког електронског спектра минимизирањем ефеката савезничког или непријатељског коришћења електронског рата помоћу којег се нарушава, неутралише или уништава савезнички борбени потенцијал. Електронска подршка има за циљ прикупљање информација о актуелној ситуацији детектовањем, идентификовањем и лоцирањем извора намерно или ненамерно емитоване елктромагнетне енергије са циљем моменталног откривања претње. Електронски напад би требало да се користи у складу са утврђеним принципима ратовања.

Војно обмањивање се примењује у циљу обмане политичког руководства и команданата који доносе одлуке на противничкој страни, у циљу утицаја на доносиоце одлука, систем прикупљања, анализирања и дистрибуције информација противника.[445] Обмањивање захтева добро познавање противника и његовог процеса одлучивања. У процесу креирања концепта обмањивања, посебна пажња се поклања руководиоцима и војним командантима противника и њиховим идејама о томе како би противник желео да се неперијатељ понаша. Наведене идеје о жељеном понашању непријатеља постају циљ операција обмањивања. Циљ је да противничко цивилно и војно руководство стекне погрешне представе о потенцијалима и

---

[444] *Joint Doctrine for Electronic Warfare - JP 3-51*, Department of the Army, Department of the Navy, Department of the Air Force, 2000.

[445] *Joint Doctrine for Military Deception* - JP 3-58, Department of the Army, Department of the Navy, Department of the Air Force, 1994.

намерама савезничких снага, да се поремете непријатељске могућности за прикупљање обавештајних података или непријатељске снаге омету у коришћењу најадекватнијих борбених јединица или јединица подршке. Операције војног обмањивања зависе од обавештајних операција у смислу идентификације одговарајућих мета обмањивања, идентификације мета и процене ефикасности плана војног обмањивања.

Заштита операција доприноси офанзивним информационим операцијама тако што успорава циклус доношења одлуке на противничкој страни и ствара прилику за лакше и брже постизање циљева на савезничкој страни. За заштиту операција је веома важно разумевање могућности непријатеља у погледу благовременог прикупљања поузданих и адекватних обавештајних података. У комбинацији са другим потенцијалима, активности на заштити операција, када је то могуће, подразумевају и прикупљање корисних информација о непријатељским сазнањима и проценама у вези са властитим операцијама. Заштита операција има улогу да противничкој страни ускрати битне информације о савезничким потенцијалима и намерама које су му неопходне за ефикасно и благовремено одлучивање. Заштита операција је процес којим се идентификују сопствене информације од изразитог значаја и анализирају сопствене или операције савезничких оружаних снага са циљем одређивања: које су сопствене информације потребне противнику да би он имао тачне податке о стварним намерама савезничких снага, лишавање противничких командних структура значајних информација о намерама савезника и довођење противничког руководства до погрешне процене о стварним намерама, обезбеђујући тајност и безбедност таквих информација. С тим у вези заштита операција је у тесној вези са војним обмањивањем.

Мрежноцентричне операције су једне од најсавременијих и најмодернијих способности развијених за потребе подршке војних операција. Значај ових операција увећао се са наглим порастом коришћења умрежених рачунарских система и телекомуникационе инфраструктуре од стране војних и цивилних структура и организација. Мрежноцентричне операције, заједно са електронским ратовањем се користе за напад, ометање, прекид и уништење противничких информационих и рачунарских система. Као што је већ поменуто, мрежноцентричне операције се деле на офанзивне, дефанзивне и оне које се користе за експлоатацију рачунарских мрежа. Компјутерске операције које имају за циљ експлоатацију рачунарских

мрежа омогућавају обавештајно прикупљање података из противничких база података.

Дакле, можемо констатовати да у војним доктринарним документима САД садржај и обим појма мрежноцентричне операције у највећој мери одговара појму кибер ратовање.

Могућност борбе са велике раздаљине, и без ризика, чини мрежноцентричне операције изузетно моћним оружјем, иако је, до сада, доста легислативних, политичких и технолошких ограничења спутавало њихову ширу употребу од стране државних актера.

Чињеница о томе ко контролише мисију кибер ратовања САД била је једна од најоспораванијих током претходних неколико година. Америчко Војно ваздухопловство, Копнена војска и Морнарица имају засебна оперативна одређења кибер ратовања, али глобална команда над спровођењем мрежноцентричних операција била је, до 2010. године, додељена Стратегијској команди САД (USSTRATCOM), док је Национална безбедносна агенција (NSA) имала мисију да штити све војне мреже САД.

Веза између Националне безбедносне агенције и Стратегијске команде САД обављала се на нивоу Здружене команде наменских снага за глобалне мрежне операције при Министарству одбране САД (*енгл*. Joint Task Force Global Network Operations Command), под краћим називом Здружени Генералштаб за мрежноцентричне операције, чији је командант истовремено био и директор Националне агенције за безбедност.

Септембра 2010. године Кибер команда је преузела надлежности од Здружене команде наменских снага за глобалне мрежне операције, која се аспектима кибер ратовања бавила претходних десет година. Кибер команда САД, налази се у авио бази Форт Џорџ Мид, у држави Мериленд, где се налази и седиште Агенције за националну безбедност САД.[446] Ова команда је директно потчињена врховној

[446] Straton R. T.: *Organization of cyberspace forces*, Air Command And Staff College, Air University, Maxwell Air Force Base, Alabama, 2008.

Стратегијској команди САД, која се налази у ваздухопловној бази Офут (држава Небраска).[447]

Након номиновања у Сенату САД, на дужност команданта Кибер команде је 15. априла 2010. године, именован генерал Кит Александер (Keith B. Alexander), који уједно обавља и дужност директора Агенције за националну безбедност САД, на којој се налази последњих пет година.[448]

Кибер команда је постала оперативна маја 2010. године, а пун капацитет достигла је у новембру 2010. године. Истовремено са достизањем пуне оперативне способности, током одржавања Самита НАТО у Лисабону, Министарство одбране САД одобрило је и раније поменуту Националну кибер стратегију САД.

Задатак нове Кибер команде је заштита података и информација у информационим системима. Она треба да спречи противника да их се домогне или их злоупотреби, употребом електромагнетног спектра, рачунарских мрежа, система комуникација, система глобалног позиционирања итд. Такође, у основне задатке Кибер команде спада и предузимање мера за спречавање хакерских упада у рачунарске мреже Министарства одбране САД (или државе).[449]

Информациона инфраструктура оружаних снага САД, за кибер одбрану (и нападе по потреби), користи исти медиј одакле напади и долазе – Интернет. Војна информациона мрежа повезује целокупан одбрамбени систем, од јединица и команди размештених по целом свету, до министарстава и владе САД, које су међусобно повезане Интернетом. Зато се Интернет контролише не само од стране војних структура, већ и цивилних, јер је осетљив на нападе и манипулације споља.

---

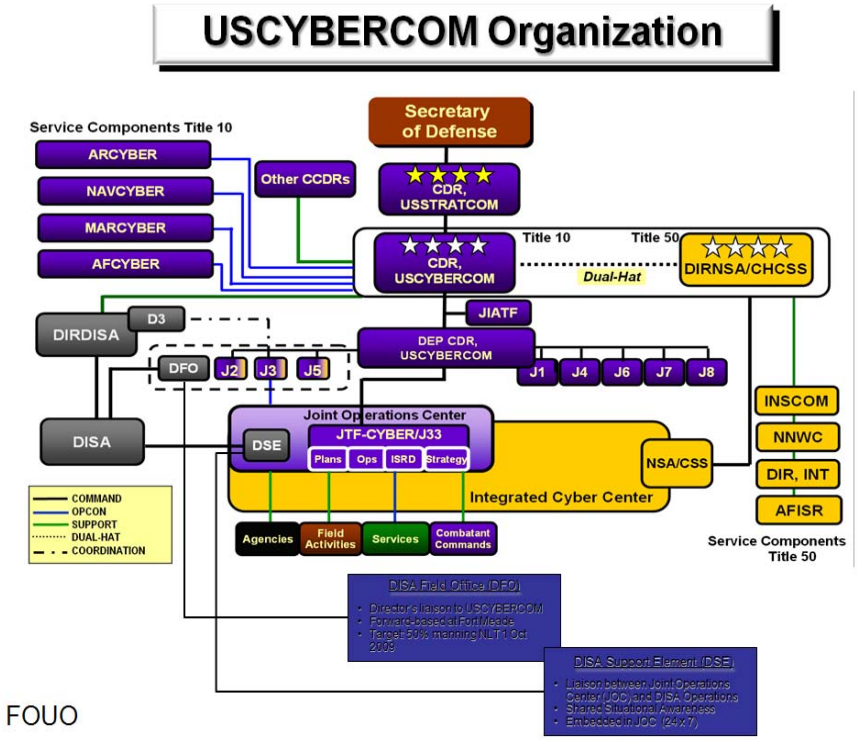
[447] Стратегијска команда оружаних снага САД (U.S. Strategic Command, STRATCOM) одговорна је за вођење стратегијских ваздухопловних, нуклеарних и кибер операција. Чине је Кибер, Свемирска и Интегрисана команда противракетне одбране. Налази се на око 1.2.00 км од авио базе Форт Џорџ Мид, где се налази Кибер команда.

[448] Reimer J.: "U.S. Cyber Command Preparations Under Way, General Says", March 16, 2010, U.S. Department of Defense, http://www.defense.gov/news/newsarticle.aspx?id=58355

[449] Последњи озбиљнији кибер упад из 2008. године, у поверљиву рачунарску мрежу коју користи Пентагон, уношењем малициозних кодова и њиховим масовним реплицирањем, био је одлучујући моменат да се формира Кибер команда САД. Према излагању William J. L., заменика државног секретара за одбрану САД, на тему: *A Conversation on Cybersecurity*, Брисел, 15. септембар 2010. године.

С друге стране, Команда има задатак да врши проверу компоненти које се уграђују у рачунарске системе. Контрола се врши из бојазни да су поједини чипови и програми, који долазе из других држава, пројектовани тако да подстичу отицање информација, тј. да утичу на повећање рањивости информационе инфраструктуре.

Схема бр. 6: *Организацијско-формацијска структура Кибер команде оружаних снага САД*



Извор: CrucialPoint,http://crucialpointllc.com/services/federal-services/government-markets/cybercom-org-chart/

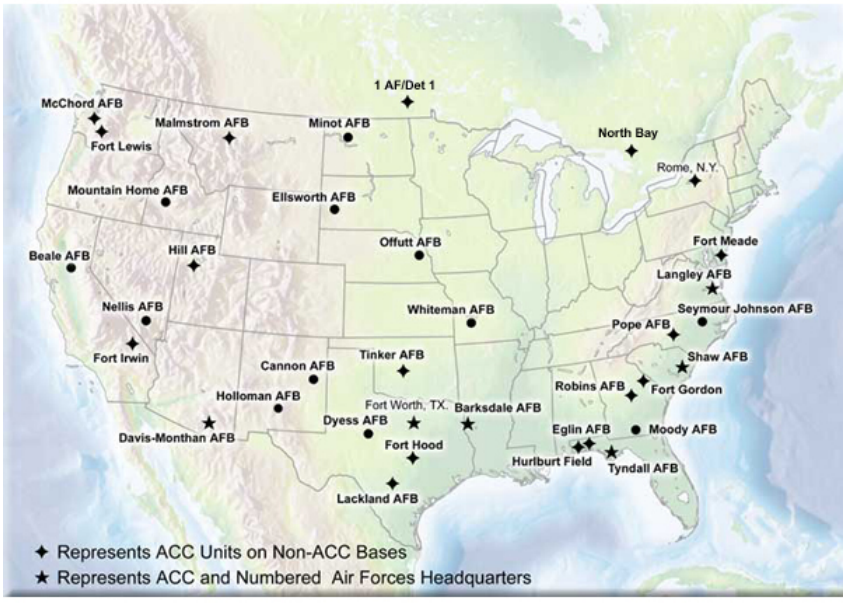
Примарни задатак Кибер команде је да брзо и прецизно открије локације одакле долази напад, да изврши тачну идентификацију нападача, ублажи последице напада и истовремено изврши противнапад, у циљу одвраћања од сличних офанзивних активности потенцијалних противника. Такође, као обавеза се налаже да са дистанце, помоћу кибер капацитета, онеспособи системе командовања, веза као и ракетни систем потенцијалних противника и да даље развија офанзивне кибер способности.

Један од циљева је и проналажење решења за заобилажење „заштитних зидова“ рачунара (*енгл.* firewall) и заштитних система противника, у циљу

омогућавања приступа и онеспособљавања истих. За ове потребе користи се систем за утврђивање локације и идентификацију нападача. Ако неко покуша напад на војни сегмент Интернета и војни информациони систем, то ће значити да је најпре извршен напад на SCADA систем, који има улогу превентиве и заштитне ограде око укупног информационог система. Подразумева се да ће исти одмах алармирати надлежне и сам одговорити на одговарајући начин, зависно од опасности. Опасности и покушаји упада, који долазе из спољашњег окружења, региструју се и приказују кодом за потребе SCADA система, што омогућава олакшано праћење информационог саобраћаја унутар информационе војне мреже. Ове могућности су достигнуте још почетком 2008. године, у оквиру 24. Кибер команде.

С обзиром на то да је кибер простор постао поприште сукоба глобалних размера, очекује се да ће будуће битке бити вођене управо у овом медију. Јуна 2009. године, одлуком о формирању Кибер команде САД, одређено је и формирање видовских кибер команди, њених потчињених видовских компоненти. Тиме су Кибер команди додељене четири видовске кибер команде:

- Кибер команда копнене војске (Army Forces Cyber Command);
- Кибер команда 10. Флоте ратне морнарице (Fleet Cyber Command / United States Tenth Fleet);
- Кибер команда корпуса морнаричке пешадије (Marine Corps Forces Cyberspace Command);
- 24. Команда ратног ваздухопловства за кибер ратовање (24th Air Force).



Слика бр. 1: *Размештај јединица потчињених Кибер команди на територији САД*

Формирање *Кибер команде копнене војске* обављено је 21. маја 2010. године, истог дана када је формирана Кибер команда САД. Кибер команда копнене војске, која се налази у Вашингтону, постала је оперативна октобра исте године. Основу команде чини део за мрежне операције 9. Команде за везу (9th Army Signal Command) као и 1. Команда за информационе операције копнене војске (1st Information Operations Command).

Од јединица копнене војске за вођење кибер ратовања, до 2011. године је формиран Батаљон за вођење мрежног кибер ратовања (Army Network Warfare Battalion). Успостављен је 2. јула 2008. године, при 9. Команди за везу, у бази Форт Џорџ Г. Мид. Намена овог батаљона је пружање подршке из области офанзивно-дефанзивних кибер активности, за потребе бригадних борбених тимова копнене војске (Army Brigade Combat Teams) у Ираку, као и подршка Командама здружених снага и међуагенцијским потребама на терену. Ово је прва јединица, формирана на нивоу Команде за обавештајно-безбедносне активности копнене воске САД (U.S. Army Intelligence and Security Command), која централизује кибер капацитете на нивоу копнене восјке САД.[450]

Кибер команда ратне морнарице, која представља морнаричку компоненту при Кибер команди, успостављена је 2002. године, док је кибер команда 10. флоте ратне морнарице формирана 29. јануара 2010. године, у бази Форт Џорџ Г. Мид, са здруженим и родовским капацитетима.[451] Команда, чији је командант вице-адмирал Бернард Џ. Мек Калаф (Bernard J. Mc Cullough), надлежна је за пружање подршке команданту ратне морнарице по питањима заштите информационих система ратне морнарице, као и вођења операција електронског и космичког ратовања. Такође, команда је по питању криптолошке заштите информација, потчињена Централној безбедносној служби (Central Security Service).

---

[450] Команду над батаљоном копнене војске за кибер ратовање, преузео је потпуковник Јен Истерли (Jen Easterly), од команданта 704. војно-обавештајне бригаде копнене војске САД, пуковника Џорџа Франца (George J. Franz), који се претходно налазио на дужности помоћника директора Агенције за националну безбедност САД. На церемонији формирања кибер батаљона, дужност команданта 704. војно-обавештајне бригаде преузео је пуковник Роберт Тејлор (Robert Taylor).

[451] *U.S. Fleet Cyber Command Mission*, Navy Forces Online Public Sites, http://www.fcc.navy.mil/

Кибер команди ратне морнарице, потчињене су:

- *Морнаричка команда за мрежно ратовање* (Naval Network Warfare Command);
- *Морнаричка команда за одбрамбене кибер операције* (Navy Cyber Defense Operations Command);
- *Команда за морнаричке информационе операције* (Naval Information Operation Command);
- *Комбиноване наменске снаге* (Combined Task Forces);
- *Команда за истраживање, развој, тестирање и оцењивање информационих операција* (Research, Development, Test & Evaluation Naval Information Operation Command).

У оквиру њих налазе се 23 институције ратне морнарице које се баве информационим технологијама, укључујући и поједине морнаричке команде и центре, попут *Морнаричке свемирске команде* (Naval Space Command), *Морнаричке команде за рачунаре и телекомуникације* (Naval Computer and Telecommunications Command), *Центра флоте за информационо ратовање* (Fleet Information Warfare Center) и *Морнаричке наменске снаге за одбрану рачунарских мрежа* (Navy Component Task Force-Computer Network Defense). Од 2005. године, прикључена им је и *Морнаричка група за безбедност* (Naval Security Group), која се бави криптографијом и специфичним проблемима везаним за изненадне прекиде терминалских процеса.

Кибер команда 10. Флоте ратне морнарице САД, која има 182 припадника, формирана је у циљу остваривања информационе доминације током извођења морнаричких операција. За потребе ових задатака, у Команди је од раније потчињених целина формиран један одсек - обавештајно-информациони - као нови модел организовања функционалних целина. Њиме руководи заменик начелника за морнаричке операције и информациону доминацију (Deputy Chief of Naval Operations for Information Dominance). Команда је формирана као централни оперативни састав за потребе кибер операција ратне морнарице САД. Основна формација која ће се бавити капацитетима за остварење овог задатка треба да буде Корпус за информациону доминацију (Information Dominance Corps), који ће обухватати свих 44.000 припадника у целој ратној морнарици, обучених за вођење кибер активности. Дужност команданта Кибер команде ратне морнарице САД припада адмиралу са две зведице.

Кибер команда корпуса морнаричке пешадије још увек нема развијене јединице извршне структуре за извођење информационих операција. Тек у последњем периоду, првенствено за реализацију задатака у мултинационалним операцијама, јединице корпуса морнаричке пешадије су почеле да уводе тактичке тимове за психолошке операције, као последицу бројних уочених недостатака током активности у зонама операција у Авганистану и Ираку.

24. Команда ратног ваздухопловства за кибер ратовање је најразвијенија формација у саставу Кибер команде оружаних снага САД.[452] Формирана је 18. августа 2009. године и размештена на девет различитих локација, широм САД. Главна локација Команде налази се у бази ратног ваздухопловства у Лакланду, недалеко од града Сан Антонија, држава Тексас. Од 540 формацијских места колико је било планирано у почетку, Кибер команда је смањена на 450 лица, а 90 лица је придодато потчињеним сквадронима (батаљонима), док ће цела формација располагати са 8.000 (почетно је планирано 14.000) припадника. Буџет ове јединице је одређен на 2 милијарде долара у првих годину дана рада. За њене потребе формирано је 17 нових ВЕС (војно евиденцијска специјалност) за нове специјалности за подофицире и официре. Основна оперативна целина ове команде је Кибер-безбедносни центар, у коме ће се обједињавати сви подаци о евентуалним кибер нападима и одакле ће се вршити контрола и покретање противодговора. Командант 24. Команде ратног ваздухопловства за кибер ратовање је генерал-мајор Ричард Вебер (Richard E. Webber).[453]

Важно је нагласити да Стратегијска команда САД није једина која има командну одговорност у овој комплексној арени. У публикацији JP 3.1.3 наводи се да: „специфичност овлашћења и одговорности команданта Стратегијске команде САД да координира информационе операције широм своје зоне одговорности и функционалних граница не умањује обавезу осталих војних команданата да координирају, интегришу, планирају, извршавају, и развијају информационе операције. Ови напори могу тежити ка томе да се постигну национални или војни

---

[452] *24th Air Force activated, 2 units realign in joint ceremony*, August 19, 2009, http://www.af.mil.usairforce

[453] *How the Pentagon is Organizing its Cyber Warfare System*, May 2008, http://www.IntelligenceOnline.com

циљеви обухваћени програмима за војну сарадњу и безбедност, да се обликује оперативно окружење за потенцијално ангажовање током периода повећаних тензија, или као подршка одређеним војним операцијама.“[454]

Иако су у наведеној публикацији технички термини одређени и дефинисани, јавно није објављена кохерентна стратегија кибер ратовања која ближе одређује где, када и како оно треба да буде примењено. Можемо претпоставити да је један од разлога тај што је реч о строго поверљивој материји. Други разлог могао би бити у томе што је стратегија још увек у фази развоја.

Постоје бројни проблеми са којима се војни планери сусрећу током покушаја да створе кохерентну доктрину кибер ратовања. Посебно су значајни они проблеми који су везани са немогућношћу откривања идентитета нападача и формулисања политике превентивног застрашивања противника. Како би САД требало да одговоре на кибер напад уколико не могу недвосмислено утврдити идентитет нападача? У којој мери политика застрашивања може бити ефикасна ако непријатељске државе знају да њихове кибер активности могу бити спроведене анонимно?

Осим тога, позната је чињеница да САД тежи стратешкој доминацији на свим пољима – на копну и мору, као и у ваздуху и свемиру. У настојању да контролишу ове просторе САД су остварile приступ свакоме од њих. Над кибер простором, међутим, не може се доминирати нити га може контролисати било која држава.

Из тог разлога САД имају интереса да подстичу процес формулисања међународног ратног права у домену кибер ратовања. Нека од питања дефинисања правила ратовања у кибер простору отворена су у извештају Националне академије наука под називом „Шта кажу технологија, политика, закон, и етика о стицању и коришћењу својстава кибер напада од стране САД?“: када спровести кибер напад (које су околности под којима кибер напад може бити оправдан?), опсег кибер напада (који ентитети могу бити мете?), Трајање кибер напада (колико дуго кибер напад треба да траје?), обавештења (ко мора бити информисан да је спроведен кибер

[454] Carr, J., *op. cit*., p. 176.

напад?) и овлашћење за изузетке (који ниво овлашћења је потребан да би се добили изузеци од важећих правила рата?).[455]

Према наводима Џефрија Кара, администрација САД планира да направи значајан напредак у овој области током 2012. године.[456]

Ефекти кибер напада, и поред његове усмерености на војне циљеве, могу бити опасни по цивилно становништво с обзиром на то да, као што смо разјаснили у одељку о критичним инфраструктурама, могу постојати међузависности ових циљева.[457] Дакле, могућност настанка непредвидиве колатералне штете чини напад недискриминишућим, што се свакако коси са принципима Женевских конвенција и међународним ратним правом.

4.1.2.2. Руска Федерација

Протеклих година Русија је била најактивнија по питању примене кибер напада против својих непријатеља, који укључују Чеченију (2002.), Киргистан (током 2005. и 2009.), Естонију (2007.), Литванију (2008.), Грузију (2008.), и Ингушетију (2009.). Без обзира на то да ли су напади спровођени од стране руске армије или хактивистичких група, индикативно је то да Кремљ није учинио ништа по питању санкционисања ових напада. У сваком случају, може се тврдити да су спроведени напади имали улогу у ојачавању званичне политике Руске Федерације.

Војно интересовање Русије за развој стратегије информационог ратовања датира од средине деведесетих година прошлог века, када је Подкомитет руске Думе за информациону безбедност изразио сумњу да су телекомуникационе платформе, купљене од САД, садржале тајни прекидач који би, када се активира, могао да обори телефонски систем целе Русије.[458] Страх је довео до акције те су, пар година касније, на Академији за државну безбедност Русије (ФСБ) ангажовани предавачи из области рачунарских мрежа и информационе безбедности.

---

[455] *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities*, William A. O., Kenneth W. D., Herbert S. L., editors, Committee on Offensive Information Warfare, National Research Council, 2009.

[456] Carr J., *op. cit*., p. 177.

[457] На пример, информатички вирус убачен у војни систем противника лако може да инфицира и цивилне системе, а затим да, без дискриминације, погоди информационе системе широм света, укључујући и земљу из које је вирус првобитно послат.

[458] Овај страх није својствен само Русима. На пример, САД су одбиле да купе штампане плоче од кинеског произвођача Huawei из суштински истог разлога. Према: Carr J., *op. cit*., p. 162.

Изградња доктрине кибер ратовања Руске Федерације, започела је Револуцијом у војним пословима током осамдесетих година прошлог века. Још од тада, Русија је испитивала велики број опција за нападе помоћу рачунарских мрежа, укључујући и логичке бомбе, вирусе, микрочиповање, и остале облике малициозних софтвера.

Русија је у покушају да контролише проток информација током позног периода Другог чеченског рата 1997 - 2001. учинила корак даље од онога што се у савременој америчкој теорији кибер ратовања назива *искоришћавање рачунарских мрежа* (CNE), усмеривши своју активност на нападе помоћу рачунарских мрежа. Мете ових напада, између осталог, били су и чеченски сајтови kavkaz.org и chechinpress.com и ти напади били су довољно јаки да оборе оба сајта.

Након Чеченије уследили су кибер напади који су циљали Киргистан и Литванију као и комбиновани кибер-кинетички напади на Естонију и Грузију. Током јула и августа 2009., ескалација насиља у Ингушетији била је праћена нападима опструкције услуга (DoS) усмерених против критичара владе која је била под контролом Кремља: http://www.ingushetia.org.[459]

Значајан утицај на организовање напада у кибер простору и мотивисање хактивиста на извршење ових напада има Фондација за ефикасну политику (ФЕП).[460] Фондација за ефикасну политику, историјски гледано, јесте једна од првих сила руског Интернета. Оригинални сајт ФЕП-а, ФЕП.ру, више није активан, али

---

[459] Власника првобитног сајта, Ingushetia.ru, убила је ингушка полиција док је био у притвору, августа 2008. Према: Carr J., *op. cit*., p. 162.

[460] Фондацију за ефикасну политику основао је Глеб Олегович Павловски, један од пионира Интернет технологије у Русији. Павловски је писао програме за Русский журнал а касније и елетктронске магазине Gazeta.ru, Lenta.ru и Inosmi.ru.

Руковођење Павловског ФЕП-ом често је била мета новинских чланака у Русији који су га оптуживали за мутне послове везане за пружање подршке властима. На пример, 4. децембра 1997., чланак у *Общая Газета* оптужио је Павловског за протурање информација које су нашкодиле Борису Березовском. Овај чланак је анализирао каријеру Павловског, и указао на то како је од Јељциновог противника постао Јељцинов присталица, као и на чињеницу да је након тога финансијски просперирао. 10. децембра 1997., *Московский Комсомолец* навео је да је Павловски по налогу Анатолија Чубајса, у то време вође председничке администрације, урадио политичку анализу за владајуће структуре.

У чланку објављеном 18. јануара 1999. у Експерту, Павловски је показао да је прилично информисан о ономе што следи и да има одличне везе. Павловски у чланку наводи да је руском друштву потребна десничарска, конзервативна влада. Како он каже, „Након деценије неуређених, суштински неконтролисаних промена у држави, помак према јакој и ауторитативној држави је предодређен“. До августа је Владимир Путин био председник владе, а већ у децембру је вршио дужност председника. Бројни новински чланци у Русији из 1999. детаљно пишу о успону Павловског као политичког оперативца од поверења, који се од подржавања Јељцина пребацио на подржавање Путина. И заиста, 24. децембра 1999., *Сегодня* приписала је Павловском заслуге за идејно решење Путиновог новог Центра за стратешке студије, који је за циљ имао разрађивање плана за будући развој Русије. *Ibid*.

архивске информације показују да је сајт био активан од 1998. до 2007. Сајт је хвалио експертизу ФЕП-а у Интернет операцијама, наводећи примере сајтова за подршку руских политичких фигура и њихових кампања које је ФЕП развио. Иако фондација није део Оружаних снага Руске Федерације, она је и данас један од званичних гласова Кремља и значајан фактор у оркестрирању реакције на говор или дела усмерена против Кремља.

Иако ова организација није у великој мери промовисана у медијима, она на веома суптилан начин дизајнира и обликује стратегије борбе против унутрашњих и спољних непријатеља Руске Федерације. Овој организацији се приписује активност на ширењу националистичке идеологије те подстицању хакерских група на спровођење кибер напада. Откривање идентитета нападача онемогућено је техником одвлачења пажње коју спроводи Фондација.

Током 2008. фокус Кремља био је више усмерен ка надзору а не пропаганди. И ови напори су превасходно потицали од ФЕП-а којим је руководио Глеб Павловски, и сајта Pravda.ru којим је руководио Вадим Горешенин.[461] Агенције су пратиле актуелна збивања у друштвеним срединама и друштвеним мрежама на Интернету.

Фондација за ефикасну политику основала је издавачку кућу *Европа*, која је издала *Хронике информационог ратовања* аутора Максима Шарова[462] и Томофеја Шевјакова. Књига се бави смерницама које је издавао први заменик начелника администрације председника Руске Федерације и некадашњи официр војне обавештајне службе ГРУ Владислав Сурков. Сурков је такође имао кључну улогу у стварању званичних омладинских организација, као што су „Наши“, које су имале важну улогу у имплементирању политике Кремља на разне начине, укључујући и хаковање противничких рачунара.

---

[461] Вадим Горшенин је издавач новина и портала Pravda.ru, Yoki.ru, Elektorat.info, и Politonlayn.ru. Познат је и по томе што је у пријатељским односима са некадашњим шефом за односе са јавношћу странке Јединствена Русија, који је од 2008. заменик начелника Управе за унутрашњу политику администрације председника Русије.

[462] Максим Шаров некада је радио за Никиту Иванова, заменика начелника Управе Председника Русије за међурегионалне и културне везе са страним државама и супервизора прокремаљских покрета младих (нпр. Наши). Шаров је познат по томе што је (преко *Европе*) објавио упуство за хакере који желе да „се боре са непријатељима Русије“ у блогосфери.

Убрзо након сукоба у Грузији, Сурков је одржао састанак иза затворених врата са руским „спин докторима“ где их је упутио у начине коришћења информација као оружја против руских непријатеља (попут владе Грузије). Ове опаске су забележили аутори Шаров и Шевјаков и ставили их у садржај своје књиге. Следећи цитат преузет је из уводне речи књиге: „Мрежни ратови су одувек били унутрашња особеност Интернета – и нису били интересантни било коме у реалном животу. Петодневни рат показао је да је Мрежа фронт исти као традиционални медији, и да је то фронт у коме много брже долази до одговора и на много ширем плану. Август 2008. био је почетна тачка конфликата у виртуелној стварности и тренутак препознавања потребе да је такође потребно водити рат и на пољу информационих технологија.“[463]

У фебруару 2008. године заменик начелника председништва Руске Федерације Александар Бурутин[464] одржао је говор на Националном форуму информационе безбедности под називом „Ратови у будућности биће информациони ратови“.[465]

У свом говору генерал Бурутин изнео је тврдњу да наука и технологија постају узрочници промена у друштву у целини, а особито у Оружаним снагама. Кинетичка сила мора уступити место информационој супериорности. Описао је како ће у ратовима у будућности акценат бити пребачен на нападање „државних и војних система контроле, навигационих и комуникационих система, и других битних информационих капацитета.“

Бурутин је објаснио како „информационим наоружањем“ може руковати мали, специјализовани тим, или чак врхунски обучен појединац, без потребе да икада физички пређе државну границу. Генерал је указао и на чињеницу да што је већи технолошки напредак неке нације, то је мрежна инфраструктура те нације подложнија кибер нападима.

---

[463] Наведено према: Carr J., *op. cit*., p. 164.

[464] Генерал Александар Бурутин је дипломирао на неколико војних академија. Од 2003. обавља дужност заменика начелника Генералштаба оружаних снага Руске Федерације. У априлу 2003., тадашњи председник Владимир Путин промовисао је генерала Бурутина у саветника председника за војна и одбрамбена питања. Извор: http://www.russiaprofile.org/

[465] Извор: *Независимое Военное Обозрение* – московски независни, војни недељник који објављује *Независимая Газета*.

Бурутин се у увијеној форми осврнуо и на „одређене нације“ које активно подижу ниво спремности војне кибер силе. Затим је обзнанио и реакцију Русије на то: „У ове сврхе биће оформљене специјализоване поддивизије оружаних снага и специјалних служби, биће развијени концептуални документи који регулишу питања припреме и спровођења информационих операција, и биће спроведена одговарајућа обука.“[466]

Бурутин, затим, прелази на дискусију о томе како је Русија, као један од светских лидера, одувек била на мети слабијих земаља које теже ка руској доминантној позицији, употребом релативно јефтиних комуникационих стратегија које изазивају анти-руско расположење. Потом је предложио додатне мере које Руска Федерација треба да предузме како би се заштитила:

- Систематски напори за откривање претњи и њихових извора у информационој области, стварање структуралног оквира за циљеве и задатке који обезбеђују информациону безбедност на пољу заштите и њихова реализација;
- Активно противдејство како би се утицало на свест људи са циљем промене националне идеологије;
- Развој домаће технолошке и производне базе на пољу информационих технологија;
- Повећање степена сигурности информационих и телекомуникационих система, увођење информационих технологија у наоружање и војну опрему, као и система контроле људства и наоружања;
- Побољшање структуре и средстава неопходних за постизање вишег степена информационе безбедности у области одбране;
- Обучавање експерата на пољу информационе безбедности.

Интересантна је чињеница да је у свом говору генерал посебно истакао Северни Кавказ (тј. Грузију) као проблематично подручје. Ово додаје другу димензију кибер компоненти руско-грузијског конфликта до ког је дошло неколико месеци касније, у августу 2008. године.[467]

---

[466] *Ibid*.

[467] Видети одељак: 3.8.1. Место и улога Интернета у Руско-грузијском конфликту 2008. године.

Прилично дуга студија аутора И. Н. Дилвеског, С. А. Комова, С.В. Короткова, С. Н. Родионова и А. В. Федорова под насловом „Војна политика Руске Федерације у међународној информационој безбедности“ објављена је 31. марта 2007. у *Московској војној мисли*.[468]

Ови аутори истражују руску перспективу о активностима других нација у области информационог ратовања, и онога што би Руска Федерација требало да ради у светлу тих активности. Аутори предлажу следећу дефиницију информационог ратовања: „Главни циљеви биће дезорганизација (прекид) функционисања кључних непријатељских војних, индустријских и административних објеката и система, као и вршење информационо-психолошког притиска на војно-политичко вођство, трупе и становништво противника, што се може постићи превасходно коришћењем најсавременијих информационих технологија и средстава.“[469]

Они такође упозоравају читаоце да су САД већ у потпуности способне да отпочну „психолошке и техничке информационе операције“. Како би додатно оснажили потребу Русије да развије своје могућности на пољу информационих операција, аутори критикују САД да не пружају подршку напорима Уједињених нација да се осигура међународна информациона безбедност: „Током 1998., Руска Федерација саопштила је Уједињеним нацијама да је неопходно консолидовати напоре светске заједнице како би се осигурала међународна информациона безбедност. Од тада Генерална скупштина сваке године усваја резолуцију „Развоји на пољу информација и телекомуникација у контексту међународне безбедности“. Ова чињеница потврђује значај осигуравања међународне информационе безбедности и спремност Уједињених нација да реше проблем. Али напредак по овом питању је веома спор услед контрапродуктивних ставова које износе Сједињене Америчке Државе.

На пример, ово је разлог због ког група владиних експерата за међународну информациону безбедност која је радила под покровитељством Прве Комисије Генералне скупштине Уједињених нација од 2004. до 2005. није успела да реализује

---

[468] С. А. Комов је руски војни теоретичар; пуковник Сергеј Коротков је при одсеку за оперативно управљање Генералштаба оружаних снага Руске Федерације; док је А. В. Федоров радио у Директорату контраобавештајне подршке Федералне службе безбедности Руске Федерације.

[469] Према: Carr J., *op. cit*., p. 167.

своје задатке. Камен спотицања био је предлог Руске Федерације (који су подржали Бразил, Белорусија, Кина и Јужна Африка) о неопходности проучавања војно-политичке компоненте претње међународној информационој безбедности.

За жаљење је чињеница да су САД одлучне у својој невољности да се проблем информационе безбедности пренесе на међународни ниво. На 60. и 61. састанку Генералне скупштине, САД су биле једина држава која је гласала против наведене резолуције. Не може се искључити да ће се Вашингтон слично понашати и према новој групи владиних експерата коју Уједињене нације треба да оформе 2009.“[470]

Аутори ове публикације указују на чињеницу да се се Кремљ дистанцира од активности својих хактивиста током конфликата у кибер простору: „По нашем мишљењу, изоловање кибер тероризма и кибер криминала изван општег контекста међународне информационе безбедности је, на неки начин, вештачки изазвано и није последица било какве објективне потребе. Ово се дешава јер ефекти „кибернетичког“ наоружања не зависе од мотивација које има извор деструктивног напада, док је управо мотивација оно што разликује чинове кибер тероризма, и кибер криминала, од војних кибер напада. Њихове остале карактеристике могу бити идентичне. Практични део проблема је то што мета кибер напада, док покушава да га неутралише, неће бити информисана о мотивима који наводе нападача, и стога, неће бити у могућности да оквалификује да ли је по среди криминални, терористички или војно-политички чин. Што је већи проблем, то је лакше окарактерисати те нападе као криминалне или терористичке чинове.“[471]

Након што су установили тактичку важност тога да „објашњење“ или покриће за чин кибер ратовања мора бити спроведено тако да се не разликује од чина кибер криминала или кибер терора, аутори прелазе на дискредитовање напора које САД улажу како би се осигурало међународно законодавство које би могло нарушити унутрашње послове државе по овом питању: „Међународна правна акта која регулишу односе настале током процеса борбе против кибер криминала и кибер тероризма не смеју садржати норме које крше такве непроменљиве међународне

[470] *Ibid*.
[471] *Ibid*., p. 168.

законе као што су немешање у унутрашње послове других држава, и суверенитет потоњих.

Штавише, политички мотивисани кибер напади спроведени по наређењу структура власти могу бити окарактерисани као војни злочини уз све пратеће процедуре истраге и кривичног гоњења окривљених. Поред тога, војни кибер напади могу се сматрати предметом међународног јавног права. У том случају, требало би да разговарамо о увођењу забрана на развој и употребу рачунара у сврхе напада на објекте у кибер простору других држава.

У сваком случају, војна политика на подручју међународне информационе безбедности где је укључена борба против кибер тероризма и кибер криминала требало би да буде усмерена ка увођењу међународних правних механизама који би омогућили спречавање потенцијалних агресора да неконтролисано и потајно користе кибер наоружање против Руске Федерације и њених геополитичких савезника.“[472]

Аутори покушавају да оправдају разлоге због којих треба увести међународне регулативе које би ограничиле могућности Западних држава да подрже опозиционе странке у отцепљеним републикама које се сада називају Заједница независних држава: „Пример који илуструје страно мешање у послове суверене државе било је коришћење бројних енглеских и руских сајтова за подршку опозиционим снагама у Киргистану током протеста у новембру 2006. Објављивање апела опозиционих лидера на Интернету у којима су позивали на масовне анти-председничке демонстрације довело је до таласа народног незадовољства у републици.“[473]

Наведени аутори помињу Киргистан и описују начин на који је опозиција користила Интернет да би изразила неслагање са режимом. Интересантно је да ови аутори воде дебату о слободи говора али да не помињу чин кибер ратовања који су спровели руски хактивисти како би уђуткали опозицију на Интернету годину дана раније током *Револуције лала*: „26. фебруара евидентни DDoS напад привремено је онеспособио све сајтове којима простор на серверу изнајмљују водећи киргиски Интернет провајдери (*Elcat* и *AsiaInfo*). Ови провајдери изнајмљују сајтове многим

[472] *Ibid*.
[473] *Ibid*. p. 169.

киргиским политичким странкама, медијима и невладиним организацијама. Појачан саобраћај који се повезује са прекидом услуга *Elcat* и *AsiaInfo* довео је до тога да велики провајдери у Русији и Европи блокирају приступ IP адресама ових провајдера, тако да појединим сајтовима више није било могуће приступити изван Киргистана.“[474]

Џефри Кар, експерт у овој области, сматра да Руска Федерација већ годинана користи тактику скретања пажње у својој војној стратегији, нарочито током преговора о нуклеарном разоружавању са Сједињеним Америчким Државама. Ипак, та тактика никада раније није била коришћена тако јасно и често као што је то случај у овом веку у време кибер сукоба.

У дискусијама о информационом ратовању, како у јавним обраћањима тако и штампаним медијима, руски војни званичници указују на будуће капацитете које тренутно развијају, као одбрану поротив капацитета које имају САД, а за које тврде да су много напреднији и који се већ употребљавају.[475]

Они одређују дебату скретањем пажње на оно што њихов противник развија и што, стога, они морају развити како би одбранили своју земљу. Након што су дефинисали шта је информационо ратовање, они ће говорити у корист режима договора који ограничава даљи развој тих способности. Овде лежи мајсторски примењено скретање пажње од стране руске владе, сматра Кар.

Кремљ ће преговарати о војним опцијама које није употребљавао, али неће преговарати о томе како је употребљавао услуге својих цивилних хакера. Заправо, потоње се сматра питањем унутрашњег криминала и не треба да буде предмет међународних преговора.

Вашингтон инсистира на међународној сарадњи и потписивању Конвенције о кибер криминалу (коју је потписало 22 државе међу којима нису Русија и Кина). Москви одговара споразум о нешириењу сличан оном, важећем за оружје масовног уништења (хемијско, биолошко, нуклеарно), док се енергично опире било ком

---

[474] *Ibid*. Према специјалном извештају који је издала OpenNet иницијатива 28. фебруара 2005.
[475] “US and Russia Differ on a Treaty for Cyberspace”, *The New York Times*, June 27, 2009.

покушају да допусти међународним полицијским снагама да кривично гоне кибер криминалце у оквиру њених граница.

4.1.2.3. Народна Република Кина

Из досадашње хронологије инцидената у кибер простору може се закључити да се Кина, за разлику од Русије која посредно или непосредно учествује у војним акцијама у којој је кибер ратовање једна од компонената, превасходно оријентисала на кибер шпијунажу. Кинески војни теоретичари и стратези заснивају доктрину кибер ратовања на доктринарним документима САД али и на властитој традицији војне теорије оличене у делима Сун Цуа и списима из времена династије Јужни Ћи (479-502.)

Ови списи говоре о ратним лукавствима и фокусирају се искључиво на чинове лукавства, преваре и стварања хаоса – што је пре област којом се баве шпијуни, а не војници. То чини овај древни документ инспирацијом савременим кинеским недржавним хакерима али и званичним пекиншким стратезима, који се ослањају на стварање лукавстава како би манипулисали лаковерним корисницима Интернета. Због тога, у хактивистичким нападима који потичу са територије Народне Републике Кине доминирају технике фишинга, социјалног инжењеринга, DDoS напада, као и употреба споредних врата, тројанаца и других малициозних програма.

Информациона технологија је подручје где, за разлику од области индустријских капацитета или војног наоружања, ниједна нација не може имати доминацију. Резултат тога је да су информациона технологија и информационо ратовање, веома привлачни Народној Републици Кини, која има невероватне ресурсе у бројности свог становништва и броју високо-квалитетних дипломираних математичара и научника. Кинези сматрају да ће губитници у информационом ратовању бити они са назадном технологијом, као и они којима недостаје вештина планског размишљања и способност примене стратегија.

У свом истраживању феномена кибер ратовања амерички научник Кар долази до податка да су званичници кинеске Народне ослободилачке армије почели да пишу о информационом ратовању још 1993. године, у отприлике исто време када је претраживање Интернета постајало нашироко популарно. Фактор подстрека било

је америчко приказивање технологије у Првом заливском рату, које је приметио и о коме је писао General Liu Huaqing, некадашњи потпредседник Централне војне комисије. Америчка победа била је од посебног значаја за Кинезе јер је Ирак користио наоружање добијено од Кине и Русије. Велики пораз ирачке војске такође је указивао и на недостатак ефикасности кинеског наоружања у односу на евидентно надмоћнију силу.

Други позив на узбуну за Кинезе представљало је бомбардовање кинеске амбасаде у Београду 1999. године. Иако су уследила извињења, овај напад довео је до тога да кинески хакери нападну званичне мреже америчке владе, укључујући и сајтове америчких Министарстава енергетике и унутрашњих послова.

У априлу 2001. године, када се америчка летелица за надзор EP-3 Signals сударила са кинеским војним авионом, што је довело до погибије кинеског пилота, бесни цивилни хакери лансирали су кибер напад на мреже у САД-у. Ови догађаји нису прошли непримећено од стране званичника кинеске Народне ослободилачке армије, који су посматрали како „рачунарски ратници“ могу искористити технолошку зависност надмоћније силе у асиметричном сукобу.

У скорашњем истраживању, заснованом на америчкој здруженој доктрини као основи за истицање разлике између кинеског и америчког информационог ратовања, Кејт Ферис (Kate Farris) тврди да „САД имају тенденцију да се фокусирају на аспекте информационог ратовања који се односе на нападе помоћу рачунарских мрежа, док Кина има много ширу перспективу, која почива на темељима попут психолошких операција (PSYOP), одбијања и обмане.“[476]

Проблем који је неодвојив од технолошки напредне војне силе јесте њена зависност од технологије. Што је сложенија мрежа, то је она и рањивија. Генерал-мајор Wang Pufeng, који је често називан „оцем информационог ратовања“, написао је 1995. године утицајну књигу *Изазов информационог ратовања*. У њој он разматра питање како употребити слабост да би се поразила снага и како водити рат против слабих непријатеља да би се искористила информациона надмоћ и постигао већи број победа по мањој цени. Осим тога, он сматра да је информационо ратовање један

[476] Carr J., *op. cit*., p. 171.

од најважнијих фактора модернизације кинеске војске у будућности: „На крају крајева, информационим ратовањем управљају људи. Један од аспеката је неговање талената у информационим наукама и технологији. Развој и ток информационог ратовања може се до велике мере предвидети у лабораторијским условима. Таленти у области информационих наука и технологија су претече научних и технолошких истраживања.“[477]

Кинеска влада сматра информационо ратовање правом „народном борбом“, што значи да могу регрутовати техничке стручњаке из круга цивилног становништва.[478] Истраживање корпорације RAND о информационом ратовању, дало је идеју кинеским војним стратезима да конципирају скицу „народне борбе“ у информационом добу: „Иако је влада мобилисала трупе, бројност и улоге традиционалних ратника биће осетно мањи од броја техничких експерата на свим линијама... пошто хиљаде персоналних рачунара може бити повезано да би се извршила заједничка операција, да би се извршили многи задаци уместо војног супер-рачунара, победа у информационом ратовању ће у великој мери бити одређена чињеницом која страна може мобилисати највише рачунарских експерата и повремених присталица. То ће бити права „народна борба“.[479]

Упоредо са овим концептом организације грађанске кибер паравојске, постоје извештаји да су се стварне вежбе информационог ратовања одржавале у кинеским провинцијама, попут оне у провинцији Hubei 2000. године. Војна вежба из области информационог ратовања била је одржана у граду Езхоу и приказала је брзу мобилизацију цивилних мрежа (нпр. станица кабловске телевизије, мреже банака,

---

[477] Pufeng W.: *The Challenge of Information Warfare*, http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm

[478] Данас се кинески ђаци редовно пласирају у врх међународних научних и математичких такмичења, много изнад својих вршњака из других држава света. На пример, приликом упоређивања знања ученика из области математике, природних наука и читања 2003. године, у оквиру ког је било проверено 250.000 ђака из 41 државе, Кина је освојила прво место из области природних наука и треће место из математике. Многи од ових ђака ће у будућности стећи високо образовање на елитним светским универзитетима а неки ће можда служити као официри у Народној ослободилачкој армији. Према: http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm

[479] Thomas T.: *Like Adding Wings to the Tiger: Chinese Information War Theory and Practice*, http://www.iwar.org.uk/iwar/resources/china/iw/chinaiw.htm

телекомуникационих мрежа и осталих повезаних система) како би служиле као офанзивне јединице информационог ратовања у доба рата.[480]

Ово је још један од доказа да су кинески политички лидери и те како свесни сопствених недостатака на пољу традиционалног ратовања, на првом месту застарелости кинеске војне технологије, и да покушавају да максимално искористе своје капацитете, цивилне и војне, како би стекли додатну стратешку предност.

Кина сагледава будуће сукобе на исти начин као и САД – као ограничена војна ангажовања, а не као тотални рат. У том смислу, кинески теоретичари кибер ратовања наглашавају комбиновану употребу различитих војних, политичких, економских, и дипломатских мера.[481] Cilj ове активности nije уништење противника већ она има задатак да учини цену ратовања неприхватљивом: „Мете рачунарског ратовања су рачунари – језгра оружаног система и системи за командовање, управљање, комуникацију и извиђање – како би се непријатељ паралисао... [и да би]... се уздрмала одлучност за ратовање, уништили ратни потенцијали и постигла предност у рату.“[482]

Према кинеској доктрини, у конкретна оружја офанзивног и дефанзивног информационог ратовања спадају: физичко уништење, доминација електромагнетног спектрума, мрежноцентрично ратовање и психолошка манипулација.

Интересантно је да ова својства скоро у потпуности одражавају доктрине САД-а о информационом ратовању, као што су „Шест стожера информационог ратовања“ и „Здружена визија 2010.“ Ратног ваздухопловста САД-а. Народна ослободилачка армија је такође добавила и превела примерке документа војне публикације JP3-13.1., „Здружена доктрина за команду и управљање ратним дејствима“. Због тога не изненађује податак да стратези Народне ослободилачке армије користе исту терминологију као и Оружане снаге САД-а: CNO

---

[480] Carr J., *op. cit*., p. 172.

[481] “The Science of Strategy”, Guangqian P., Youzhi Y., eds., *Military Science Press*, Beijing, 2001.

[482] Carr J., *op. cit*., p. 173., према: Daohai L.: “Information Operations: Exploring the Seizure of Information Control”, *Junshi Yiwen Press*, Beijing, 1999.

(мрежноцентричне операције), CNA (напад помоћу рачунарских мрежа), CND (заштита мреже) и CNE (злоупотреба мреже).[483]

Први приоритет међу овим компонентама је злоупотреба мреже (CNE), јер Народна Република Кина верује да је тренутно мета напада помоћу рачунарских мрежа од стране САД-а.

Верује се да су напади помоћу рачунарских мрежа (CNA) најефикаснији на почетку сукоба и могу бити употребљени са најбољим резултатима као превентивни удар. У идеалним околностима, уколико је напад помоћу рачунарских мрежа довољно разоран, то може довести до краја сукоба пре него што прерасте у прави рат.

У погодне мете за мрежни напад спадају „чворишта и друге круцијалне везе у систему који покреће непријатељске трупе као и ратну машинерију, као што су луке, аеродроми, превозна средства, објекти на ратишту, и системи за командовање, управљање, комуникације и информације“ како у свом чланку „Превентивни удари су од круцијалног значаја у ограниченом високо-технолошком ратовању“ наводи Lu Linzhi.[484]

Народна ослободилачка војска усвојила је *Стратегију за ометање контроле и управљање приступом*, како би успорила напредовање или омела оперативни темпо непријатељске војске на ратишту током ратних сукоба. Корпорација RAND издала је одличну студију ове стратегије. Она баца додатно светло на то како Народна Република Кина планира да се бори у будућим ратовима.[485]

---

[483] *Ibid*.

[484] Рањивост САД-а према овој стратегији била је скоро наглашена након објављивања извештаја генералног инспектора Савезне управе за цивилно ваздухопловство о стању мрежне сигурности америчке Агенције за контролу летења (ATC). Једно од открића било је и да је свега 11 од неколико стотина система Агенције заштићено обавезним системима за детекцију упада. Извештај даље наводи да су неки кибер напади могли имати успеха у преотимању контроле над системима Агенције: Током фискалне године 2008, Организација за ваздушни саобраћај, која је одговорна за функционисање Агенције за контролу летења, добила је више од 800 упозорења о кибер инцидентима. Од краја фискалне године 2008, више од 150 инцидената (17%) није било санирано, укључујући и критичне инциденте у којима су хакери могли преузети контролу над рачунарима Организације за ваздушни саобраћај. *Ibid*. p. 174.

[485] Mulvenon J., Tanner S. M., Chase M., et al.: *Chinese Responses to U.S. Military Transformation and Implications for the Department of Defense*, RAND Corporation, 2006.

На самом почетку они објашњавају да „ометање контроле и управљања приступом“ само по себи није формална кинеска војна стратегија - то је пре начин сумирања кинеске доктрине који се бави проблемом надвладавања супериорнијег непријатеља. У случају Сједињених Америчких Држава, то значи схватање да се САД у великој мери ослањају на информационе мреже што представља значајну рањивост која би, уколико буде искоришћена, могла направити хаос у плановима САД-а и одложити или суспендовати било који предстојећи напад.

Технике ометања контроле и управљања приступом имају широк спектар деловања, па чак и активирање уређаја који користе електромагнетне импулсе. Мете би могли бити рачунарски системи који се налазе у САД-у или иностранству, чворишта за контролу и управљање, инфраструктура за надзор, осматрање, извиђање и комуникације стационирана у свемиру.

Да безбедност рачунарских мрежа није више само технички проблем, него и важно стратешко питање, потврђује и позив ветерана америчке дипломатије Хенрија Кисинџера из јуна 2011. године да САД и Кина започну „кибер детант” - склопе неку врсту споразума којим би неке области прогласиле недодирљивим за компјутерске хакере.[486]

Кисинџер полази од тезе да и Вашингтон и Пекинг имају значајне могућности за кибер шпијунажу и диверзије, па би због тога морали да нађу начин да ту тему ставе на преговарачки сто. „Нема другог начина да се ово реши осим да се постигне нека врста разумевања о ограничењима”, изјавио је овај архитекта историјског америчког отварања према Кини.

---

[486] Кисинџер је био главни гост скупа који је организовала агенција Ројтерс поводом објављивање његове најновије књиге „О Кини”, а на којем су били још неки експерти за ову земљу која је у исто време све важнији амерички билатерални партнер и њен растући глобални ривал.
Питање кибер ратовања постало је неизбежно у свим разговорима о Кини, после серије хакерских напада на америчке државне институције (најновија мета био је Конгрес), корпорације из војно-индустријског комплекса (Lokid Martin) и финансијске куће (City bank). Ове компјутерске мреже нису наиме предмет интересовања компјутерских криминалаца, па се зато сврставају у категорију кибер шпијунаже, са учесталим спекулацијама да имају кинески печат.
Из Пекинга се то одлучно демантује, са образложењем да је и Кина жртва хакерских напада, па је због тога „отворена за сарадњу са међународном заједницом о Интернет безбедности”, изјавио је 14. јуна представник кинеског Министарства иностраних послова. Према: Мишић М.: „Време је за сајбер детант“, *Политика*, 16. јун 2011.

Пошто је реч о сасвим новом, али изузетно осетљивом проблему, где би прихватање разговора о томе подразумевало и прећутно признање да су оптужбе основане – за почетак дискусије би могле бити предложене неспорне теме, као што је злоупотреба Интернета за ширење дечије порнографије и пропагирање и организовање тероризма. У сваком случају, Кисинџер сматра да то треба учинити тако да не добије форму „војног обуздавања".

Бивши амерички амбасадор у Пекингу, Џон Хантсмен, проблем кибер напада сврстава у исту категорију са разговорима о ракетној одбрани и војној употреби свемира, који су за Кинезе подједнако осетљиви: „У једном моменту ми морамо да створимо контекст у коме о овом питању можемо да разговарамо и у том погледу повучемо неке црвене линије".[487]

4.2. Корпоративно-економски аспект кибер ратовања

Вокабулар који се користи у савременом пословању и појединим научним дисциплинама има доста сличности са војном терминологијом. У оквиру наука менаџмента, на пример, надметање је доминантна метафора а уџбеници из менаџмента препуни су војне терминологије и аналогија са ратовањем – бочне стратегије, герилски маркетинг, ратови цена, пословна шпијунажа, предност првог удара итд. То није без разлога: „Сличности између света рата и бизниса повећавају се из дана у дан. Оба се базирају на надметању између противника са различитим имовинама, мотивима и циљевима. Надзирање непријатеља и пословна шпијунажа су обавезни на оба поља".[488] Са прогресивном глобализацијом трговине посредством транснационалних корпорација и интернационализацијом пословања, паралеле се додатно појачавају.

Појава и успон транснационалних корпорација, као све значајнијих субјеката међународних економских односа, неретко важнијих и од самих држава, јесте једно од најважнијих обележја економске глобализације.

---

[487] *Ibid*.

[488] German M., Donahue D. A., Schnaars S. P.: "A chink in marketing's armor: Strategy above tactics", *Business Horizons*, March/April 1991, p. 78.

Своју глобалну моћ транснационалне компаније остварују путем контроле три најзначајнија тржишта: тржишта роба и услуга, финансијског тржишта и тржишта информација. У свим земљама где делују транснационалне компаније, преко ових тржишта се остварује ефективна контрола производње, робних токова, цена, штедње и инвестиција, али и неекономских процеса (политички, културни, идеолошки итд).

Ако се упореди економски значај транснационалних компанија и држава у светској привреди, очиглељно је да су државе постале другоразредни привредни субјекти. Од 100 највећих привредних субјеката 51 чине компаније, а 49 државе, док највећа транснационална компанија има већу продају од друштвеног производа више од 150 држава.[489] Данас у свету расте број великих и моћних транснационалних корпорација које по својој економској снази и потенцијалу далеко превазилазе многе државе и као такве могу да утичу на бројне економске и финансијске процесе у све већем броју земаља света.

Из тог разлога транснационалне компаније се неће устручавати да предузму све што сматрају потребним да заштите своје монополске интересе и светску јавност увере да је економски, али и сваки други рат, легитимно средство у заштити слободне трговине, слободног тока капитала, знања, људи и свега осталог што доприноси повећању профита. Иза утицајних транснационалних компанија стоје њихове моћне националне државе које су увек спремне да их подрже у „светој мисији глобализације“, ако треба и својом оружаном силом.[490]

Бизнис је данас постао место правог дискурса кибер ратовања, што је МекКроен антиципирао још 1998. године.[491] Ако се у обзир узме чињеница да се компаније све више ослањају на софистициране информационе системе и, још више, на убрзан раст веб и електронског пословања, не изненађује податак да је теорија информационог ратовања већ установљена као део наставног плана у водећим пословним школама.

---

[489] Anderson S., Cavanagh J.: “Corporate Empires”, *Multinational Monitor*, Vol. 17, No 12, December 1996.

[490] Петковић Т.: *Пословна шпијунажа и економско ратовање*, Protexi Group System, Нови Сад, 2009, стр. 41.

[491] McCrohan K. F.: “Competitive intelligence: Preparing for the information war“, *Long Range Planning*, 31(4), 1998, pp. 586 – 593.

4.2.1. Корпорацијско информационо ратовање

У раздобљу рађања нове економије, либералне економије са својим светињама – приватном својином и слободном конкуренцијом на светском тржишту – економска информација још није имала тако пресудан значај. Данас је информација постала не само важно средство напретка, већ и оружје које уноси револуционарне новине у економско надметање на глобализованом тржишту. Зато не треба да чуди толика пажња која се посвећује методама регулисања електронске трговине (*e-commerce*) и новим системима обезбеђења електронских информација, односно пословања преко Интернета.

Знање, технолошка открића и иновације су од почетка индустријске револуције доносили предности (бенефиције и зараду) онима који су их поседовали или у њих инвестирали. Истраживачи и предузетници су у њима видели средства за увећавање профита али су мало пажње посвећивали могућностима за постизање предности, стечене њиховом применом, на светском тржишту, супериорност над конкурентима у економском надметању и ратовању.

Један од најстаријих видова економског ратовања и борбе против економског супарника на тржишту јесте нелојална конкуренција. Нелојална конкуренција или од неких аутора названа и нелојална утакмица, подразумева примењивање начина и поступака „противних добрим обичајима“. Овде спадају нарочито: нелојална реклама, односно изношење неистина о свом или туђем предузећу или роби, њеним квалитетима, пореклу и слично, затим, издавање и искоришћавање пословне тајне, као и међусобна борба робних произвођача за освајање тржишта и бољих услова привређивања уопште. У таквом надметању све је „дозвољено“. Многи се служе недозвољеним средствима и методима, како би уопште опстали на тржишту. Тиме се не само спречавају способнији да овладају тржиштем, већ се настоји спречити и деловање неумољивих економских законитости, без обзира на кршење постојећих закона. Санкције за такве методе нелојалне конкуренције на тржишту су веома оштре, због чега се примењују суптилније методе економског надметања, односно ратовања против конкурента.

Често се у оквиру економског ратовања примењују нелегалне методе и технике, а, пре свега, коришћење корупције или подмићивања у пословним преговорима и коришћење политичких или економских притисака и уцена, како би

се обезбедила реализација уговора, набавка одређене опреме или интеграција са одређеном компанијом. Тако се најчешће понашају велике транснационалне компаније у одређеној области производње.

Не мање значајан инструмент економског надметања, јесте крађа индустријских тајни злоупотребом Интернет сајтова супарничких компанија. Уколико су тајни подаци заштићени системима електронске заштите, користе се и друге методе: неовлашћени упад у информационе системе противника, подмићивање конструктора и службеника, врбовање руководилаца и главних пројектаната, посете сајмовима, изложбама и стручним скуповима на којима се расправља о будућим пројектима, и слично. Зато не треба да нас изненади потпуна идентичност идејних решења појединих производа.

У последње време, промене изазване развојем Интернета и информатизацијом друштва довеле су до нових форми сукоба на тржишту. Ове промене су последица технолошке револуције и примене технолошких открића у организацји рада и начину пословања компанија.

Претходна поглавља су већ указала на чињицу да је данашња зависност друштва од информација истовремено и предност и недостатак. Недостатке ствара чињеница што је информација постала једно од најмоћнијих оружја савременог човека. У савременом пословном свету влада голема „глад“ за информацијама, при чему се често не бирају средства којима се до њих долази. То значи да је и савремени свет економије и пословања суочен са два општа негативна феномена када су у питању информације: ратом за информације и информационим ратом. Другим речима, информације су, с једне стране, предмет угрожавања, а с друге, извор и средство угрожавања. Док рат за информације означава силовиту борбу у настојањима да се до информација дође, информациони рат је сукоб у којем су информације главно оружје. У савременим пословним условима, које карактерише оштра тржишна борба, рат за информације али и рат информацијама, део су пословне свакодневице.

Рат за информације, као и рат информација поткрепљују бројни примери из савремене праксе.

Директор америчке Централне обавештајне агенције Роберт Гејтс још је 1992. године упозорио да су 33 стране државе ангажоване у обавештајном деловању

против америчких пословних компанија. Три године касније Федерални истражни биро (FBI - *Federal Bureau of Investigation*) изнео је јавно процену да америчке компаније, због индустријске шпијунаже, изгубе годишње 100 милијарди долара.

Да су Сједињене Америчке Државе, као најмоћнија држава данашњице, стварно обавештајна мета на подручју економије показују и следећи примери. Крајем 1990-их објављено је како су Французи службено признали да су, како би прикупљали инфбрмације о америчким пословним системима, инсталирали прислушна средства у авионима *Air Fransa* на релацији Париз - Њујорк, којом најчешће путују амерички пословни људи. С друге стране, процене показују да је 80 одсто свих јапанских обавештајних напора усмерено на пословни свет САД и европских држава.

Међутим, ни САД не заостају у обавештајном деловању у области економије за другим земљама. На пример, фебруара 2000. године Европски парламент оптужио је САД да, заједно са Великом Британијом, Канадом, Аустралијом и Новим Зеландом, посредством система „Ешелон", а у циљу прикупљања података везаних за економију обавља контролу комуникација држава Европе и њихових пословних система.[492]

Имајући у виду ове примере, данашњу важност економске димензије националне безбедности, као и улогу националних обавештајних система у остваривању националне безбедности, можемо закључити да су све државе света ангажоване у рату за информације и рату информацијама у односу према пословном свету.

Американци су у томе најдаље отишли. Прво су деценијама, под изговором опасности са Истока, користили огромна буџетска средства одобрена од Конгреса за развој и комплетирање најмодернијих, сателитских и других информационо-обавештајних система, распоређених да комплетно премреже земаљску куглу. Тако

---

[492] Примери су дати према: Joyal M. P.: *Industrial Espionage Today and Information Wars of Tomorrow*, 19th National Information Systems Security Conference, Baltimore Convetion Centre, Baltimore, October 22-25, 1996; *Annual Report to Congres on Foreign Economic Collection and Industrial Espionage*, July 1995, http://www.fas.org/sgp/; Winkler S. I: *Case Study of Industrial Espionage Trough Social Engineering*, National Computer Security Association, Pennsylvania, http://www.simovits.com/archive/socialeng.pdf; *Prevention of Industrial Espionage*, Model United Nations of the University of Chicago, 2003, http://www.munuc.org

су обезбедили сталан прилив информација на олакшан, супериоран и мање ризичан начин. У последњој фази информатичког развоја, дефинитивно су обезбедили преимућство на том плану и предности у евентуалним конфликтима. Ако се може генерализовати, они су први прибегли цивилној примени средстава, информатичких и обавештајних информација произашлих из војне употребе и војних истраживачких центара. Већ више деценија, упоредо са развојем сателитских, електронских, обавештајних, прислушних и других система за прибављање информација, Американци обезбеђују да део квалитативне надмоћи и поверљивих информација које детектују електронски системи послужи за развој и успон америчких привредних компанија.[493] Војно коришћење информационе предности у регионалним конфликтима, као што је био Заливски рат против Ирака, наметнуло је идеје о коришћењу информационе предности и у геоекономским сукобима на светском тржишту.

Рат за информације и информациони рат омогућили су да су у савременим условима додатно развијени, претходно успостављени и институционализовани, нови различити механизми за прикупљање информација и заштиту сопствених информација. Неки од њих су нелегални и тајни (економска, индустријска, информатичка шпијунажа), други су у оквиру легалног и јавног деловања, док трећи садрже све те елементе, а ради се о систему информационог ратовања.

Када је реч о институционализацији информационог рата, већ смо истакли да је појам првобитно био везан за војно подручје. Међутим, значај информација у савременом свету условљавао је њихово ширење и на остала подручја људске делатности, па тако и на економију. Са аспекта економије, под информационим ратом можемо подразумевати „акције које се предузимају како би се постигла информациона супериорност, која је подршка пословним стратегијама, и то утицајем на информације конкурента, уз истовремено задржавање моћи, односно заштиту сопствених информација.[494] Анализа ове дефинције показује да она има три елемента, односно три димензије: офназивну, дефанзивну и експлоатациону.

[493] Петковић Т., *op. cit*., стр. 6.
[494] *Ibid.*, стр. 112.

Офанзивна укључује напад информацијама да би се разоткриле негативне стране противника, негирале или уништиле супарничке информације, односно да би се утицало на перцепцију супарника.

Дефанзивна подразумева заштиту сопствених информација али и заштиту информација пословних партнера, док експлоатациона настоји да искористи сопствене информације на прави начин и у право време као подршку одлучивању, са основним циљем да се спречи конкуренција да искористи своје информације.

Једна од најраспрострањенијих врста информационог ратовања, коју је у својој класификацији дао Швартау (Schwartau), јесте тзв. корпорацијско информационо ратовање.[495] Велике привредне корпорације користе Интернет да би се обавестиле о пословним кретањима, али исто тако и да би дезинформисале своје конкуренте. У конкурентским секторима су прикупљање података и избор тражених профила противника од изузетног значаја. Кибер простор представља један неисцрпан и свима доступан извор за такве активности. С обзиром на то да ће у скорој будућности све врсте знања постати стратешка тајна, може се, према Петровићу, очекивати драстичан пораст ове врсте ратовања.

Из доступне литературе дâ се утврдити да је до сада на Интернету покренут велики број програмираних кампања ширења дезинформација, економског карактера, чији је циљ био опањкавање противника. Такве акције дезинформисања представљају утолико мањи ризик за покретача што он, генерално посматрано, не учествује директно у акцији, већ, најчешће, преко неке од приватних агенција специјализованих за пружање овакве врсте услуга. Развој информационе технологије и жестина у суочавању са конкурентима доводе до умножавања активности ове врсте, до стварања правог тржишта дезинформација.

Понекад се „непријатељ“ може појавити у обличју *bona fide* потрошача који имају легитимну основу да се жале. Лакоћа са којом незадовољни клијент, или група клијената, може исказати свој бес и задобити подршку на Интернету, како би се угрозила репутација компаније, представља нови проблем за службе маркетинга, пропаганде и односа са јавношћу, у великим корпорацијама. На електронском

[495] Осим корпорацијског, поменута класификација садржи још персонално и глобално информационо ратовање. Према: Петровић С.: *Компјутерски криминал*, МУП Србије, Београд, 2001, стр. 337.

тржишту роба лошег квалитета, неиспуњавање обећања, лажно оглашавање, или надуване цене могу бити довољни разлози за покретање оркестриране, осветничке кампање или подношење групне тужбе од стране разочараних клијената. У кибер ратовима, могућност рањивости репутације (личне, производа, институционалне) постала је драстично увећана.

Као што Пентагон не жели да допусти упад хакера у информационе системе од националног значаја, јер би био осрамоћен, тако ни велике дуванске компаније не желе да њихова унутрашња документација и потенцијално инкриминишући извештаји и истраживања буду постављени на јавне сајтове од стране активиста за борбу против пушења, а научници и истраживачи не желе да буду жртве мутних кампања које преиспитују интегритет њихових истраживања и објављених радова.

Из перспективе страног непријатеља, терористе, или унутрашњег дисидента, напад на корпоративну имовину могао би створити исти симболички одјек као директан напад на конвенционалну војну или цивилну мету. Размислимо, на пример, о тренутним последицама и накнадним ефектима кибер напада усмереног на главни рачунарски сервер компаније Master Card, убацивање тројанца у компјутеризовани систем за резервацију карата неке авио компаније, или систематску модификацију или обзнањивање досијеа пацијената у некој престижној клиници.[496] Ако би било шта од овога хакери могли постићи, без ризика да ће изгубити живот или слободу, није тешко увидети привлачност офанзивних стратегија кибер ратовања у контексту глобалног економског ратовања.

Директне последице ове претпостављене подложности нападима су повећана корпоративна свест о потреби за интегритетом система како би се спречило саботирање виталних или приватних информација од стране конкурентских компанија или страних влада.[497] Корпорацијама не преостаје ништа друго већ да се ангажују на пољу стратегија дефанзивног информационог ратовања у напорима да се заштите од крађе, поремећаја, извртања, немогућности приступа сервисима, или уништавања осетљиве информационе имовине. Ово не значи само израду јачих

[496] Сличан инцидент се догодио 2009. године у државној болници у Тексасу. Том приликом је посредством информатичког напада саботиран вентилациони систем болнице чиме су угрожени животи пацијената.

[497] Fialka J. F.: *War by other means: Economic espionage in America*, Norton, New York, 1997.

програма заштите, повећање постојећих процедура за енкрипцију, или инсталацију софтвера који врши контранападе, већ инвестирање ресурса у стварање ефикасније обавештајне и контра-обавештајне способности у напорима да се предвиде могући напади и њихови извори.[498] У том контексту Тофлерови наводе да: „ратовање знањем подразумева обликовање непријатељских деловања манипулисањем протока обавештајних сазнања и информација.“[499]

Све је то довело до тога да пословна шпијунажа (*business intelligence*), као нова економска дисциплина, заузме значајно место у односиму међу државама и водећим транснационалним компанијама. Наиме, у прошлости је конкуренција између држава и водећих транснационалних компанија била мање оштра, тржишта више пасивна, а купци мање захтевни. Данас, конкуренција намеће борбу за сваког купца. Произвођачи и трговци настоје да нижим ценама, бољим квалитетом услуге и већим асортиманом производа привуку потрошаче, продају своје производе, освоје тржиште и остваре што већу добит. Другим речима, конкурентност значи пословну способност, односно способност економије да произведе производе и услуге који могу да задовоље тестове међународног тржишта и подигну просечан ниво развоја и животног стандарда људи.

4.2.2. Пословна шпијунажа

Осим војне и политичке шпијунаже, у новије време све чешће се помињу и економска, индустријска, компетитивна и пословна шпијунажа, као засебне врсте обавештајне делатности.

Економска шпијунажа је настала као резултат снажног индустријског и технолошког развитка у свету. Тек када је индустријски развитак обухватио низ земаља у свету, када је на тржиште пласиран вишак производа и када је почела борба за освајање тржишта, економска шпијунажа је почела да постаје све значајнији фактор у склопу целокупне обавештајне делатности једне земље. И она је, као и сви други облици шпијунаже, била првенствено подређена потребама војне шпијунаже.

---

[498] Cronin B., Crawford H.: *Information Warfare: Its Application in Military and Civilian Contexts*, School of Library and Information Science, Indiana University, Bloomington, 1999, p. 260.

[499] Тофлер А., Тофлер Х.: *Рат и антират,* Paideia, Београд, 1998.

Међутим, док су сви остали облици шпијунаже (војна, политичка, итд.) резултат делатности обавештајних организација једне државе, економска шпијунажа је попримила и елементе приватне шпијунаже.

Фабрике, корпорације, концерни и удружења, било да су приватно или државно власништво, свако на свом подручју и у оквиру своје надлежности, оснивају своје службе за прикупљање података о производњи, плановима производње нових производа, ценама, иступима на домаћем и светском тржишту истоврсних предузећа у својој и страним земљама. Чврста повезаност и међузависност привреде свих земаља у свету, конкуренција која стоји изнад свега тога, условили су и развитак економске шпијунаже до невероватних размера. Због тога је економска шпијунажа остала искључиви вид делатности свих оних који се баве производњом и организацијом производње.[500]

Када је реч о индустријској шпијунажи уопште, често се настоји да се ова врста шпијунаже прикаже као нешто посебно, изузето из општих појмова, циљева и задатака обавештајних служби у оквиру њихових основних и одређених подручја делатности.

Поједини теоретичари (Лукић, Берже, Дедијер и др.), који су се бавили овим проблемом, настојали су да издвоје индустријску шпијунажу као посебну врсту делатности. Њен настанак и интересе, односно циљеве, претежно су објашњавали техничким и технолошким развојем у свету и ужим интересима одређених професионалних групација.

Неспорна је чињеница да је индустријска шпијунажа типична карактеристика савремене шпијунаже, јер је индустрија производ и карактеристика савременог друштва. Међутим, не може се порећи да је индустрија само део привреде једне земље и да су се туђе идеје и тајне у области производње вековима крале.

Циљ економске шпијунаже одувек је био да се дође до нових и важних података о економском развоју и односима у једној земљи (производња, нови проналасци, наступи на тржиштима других земаља, уговори економског карактера са

[500] Петковић Т., *op. cit*., стр. 115.

другим земљама итд), који су од интереса за другу државу, корпорацију или организацију. Тако Е. Потер сматра да појам економске шпијунаже: „обухвата политику или комерцијално релевантне информације, укључујући финансијске, трговачке или информације неке владе, које помажу сопственим националним интересима (државним или интересима економских субјеката), непосредно или посредно помажу подизање релативне ефикасности и продуктивности или помажу конкурентност сопствене економије у свету.“[501] Она може снажно помоћи једној држави, односно штетити другој, што ће се посебно огледати у различитим економским пословима, инвестицијама, продуктивности, конкурентности или економском расту.

Појам индустријске шпијунаже Потер одређује као „употребу легалних, тајних и присилних или непоштених начина или метода да се дође до одређених сазнања унутар субјеката у приватном сектору.“[502] Међутим, оба појма подразумевају тајно прикупљање осетљивих, рестриктивних или посебно класификованих информација. Појам индустријска шпијунажа подразумева и крађу информација од конкурената. Индустријска шпијунажа представља само једно подручје, tj. део економске шпијунаже, јер је она по својим задацима усмерена само на одређену, специфичну и стручну делатност у области економије.

Индустријска шпијунажа је, према томе, само део ширег појма, који се назива економска шпијунажа. Међутим, не може се рећи да економска шпијунажа обухвата и све друге области људске делатности. Из наведеног се може извести закључак да су и један и други вид шпијунаже саставни делови пословне шпијунаже, јер се она не изражава само у интересу једне државе према другој него и у посебно израженом интересу појединаца или групација у једној држави према сличним ентитетима у другим државама, као и у сопственој. То значи да пословна шпијунажа, за разлику од осталих облика шпијунаже, представља спој интереса приватних субјеката (правних и физичких лица) и државе према истим таквим субјектима у другим државама, на једној страни, али и интерес правних лица у приватном сектору према истим таквим лицима у сопственој држави, на другој страни.

---

[501] *Ibid*.
[502] *Ibid*.

Важно је напоменути да нема општеприхваћене дефиниције појма „пословна шпијунажа“. Тако, на пример, *The Free Encyclopedia* наводи да је „пословна шпијунажа процес прикупљања информација у пословном свету... с циљем стицања предности у односу према кокуренцији.“ Аустралијска Организација за научна и индустријска истраживања *(Commornvealth Scientific and Industrial Research Organization* - CSIRO), пак, истиче да је пословна шпијунажа процес за побољшање конкурентске предности интелигентном употребом расположивих података у процесу доношења одлука.

Може се закључити да пословна шпијунажа има две димензије, односно два вида, а тиме и два циља, који се, условно, могу одредити као офанзивни и дефанзивни. Офанзивни вид, односно циљ подразумева прикупљање података ради остварења даљег развоја, а дефанзивни је усмерен на остварење сопствене безбедности (заштита података, пословне политике, пословне стратегије итд.) и чување постојећих пословних положаја. Другим речима, пословна шпијунажа има офаназивну обавештајну димензију, али и дефанзивну, контраобавештајну димензију.

Да би се описале специфичности пословне шпијунаже у информационој ери, последњих година је у употребу уведен још један појам. Реч је о шпијунажи која се обавља посредством рачунарских мрежа (*енгл*. netspionage). Та шпијунажа подразумева употребу рачунара и рачунарских мрежа, као и других, са тим повезаних способности, како би се украле тајне информације других пословних субјеката.

Најчешће мете и предмет интересовања „информатичара шпијуна“, када је реч о технологијама, укључујући и војне, јесу америчке дуалне технологије и то: информациони системи, сензори и ласери, електроника, аеронаутика, наоружање и енергетски материјали; космички системи, вођење, возила, материјали, израда и производња, технологија нуклеарних система, системи напајања, хемијско-биолошки системи, ефекти оружја и контрамере, земаљски системи, директни и кинетички системи и др.[503] Водеће транснационалне компаније из САД носиоци су три четвртине светских технолошких иновација и зато су оне најчешће на удару

[503] Матовић Ј.: *Војни послови Југославије и свет XX века*, Тетра ГМ, Београд, 2003, стр. 33-38.

крадљиваца технологија. На удару су посебно тајне војне информације и осетљиве војне технологије. Тако су разне америчке студије у протеклој деценији указале на постојање прилично ригидне листе земаља крадљиваца осетљивих технолошких иновација и економских информација.[504]

У добу економског и корпоративног информационог ратовања, системи за управљање превентивним обавештајним делатностима постали су неопходни за компаније високог профила. Тако, на пример, Национални контра-обавештајни центар (National Counterintelligence Center) има све већи значај у саветовању фирми из приватног сектора у САД, о томе како да се носе са претњама које стране обавештајне службе представљају по њихову пословну делатност.[505]

Због економске шпијунаже и активности страних обавештајних служби, према процени FBI-а, штете које су претрпеле САД само у току 1997. године износиле су око 300 милијарди долара, док су штете 1999. године од економске и индустријске шпијунаже, учињене преко Интернета, износиле око 10 милијарди долара.

Питању пословне шпијунаже изузетну пажњу поклањају не само велика предузећа и компаније и њихове безбедносне, односно обавештајне службе, већ и сама држава. О томе сведоче изјаве највиших државних функционера САД. Тако је амерички председник Клинтон изнео тврдњу да је економска безбедност примарни циљ спољне политике САД, док је амерички министар спољних послова Кристофер новембра 1993. године пред Комитетом за спољне односе Сената изјавио да је америчка национална безбедност недељива од економске безбедности.

Естаблишмент САД сматра да је данас доминантна економска моћ, за разлику од времена Хладног рата када је најзначајнија била војна моћ. У том смислу у САД чак изјављују да ће им дојучерашњи политички савезници данас постати главни економски конкуренти. Председник Клинтон је у складу с тим основао Национално економско веће (NEC - *National Economic Councit)* којег упоређују с Већем за националну безбедност (NSC - *National Security Council),* док је ЦИА

---

[504] Међу водећим државама су: Кина, Канада, Француска, Индија, Јапан, Немачка, Јужна Кореја, Русија, Тајван, Велика Британија, Израел и Мексико. *Ibid*.

[505] Cronin B., Crawford H., *op. cit*.

отпочела са издавањем дневних економско обавештајних извештаја (*Daily Economic Intelligence Brief)*, које доставља високим функционерима америчке владе.

У новој, информационој ери, велике обавештајне могућности САД су се с војних и других подручја преусмериле на подручје економске обавештајне делатности.[506] Такав тренд не запажа се само у САД већ и у другим државама. Познати су случајеви продора француских обавештајних служби у америчке компаније.[507]

Исто тако, у више наврата забележена је активност и деловање француске војне обавештајне службе DGSE (*фр*. Direction Générale de la Sécurité Extérieure) према немачким компанијама, односно немачким економским интересима.

Израелска економска шпијунажа, позната је већ више деценија. Тако је Израел још шездесетих година прошлог века основао посебну обавештајну службу LEKEM (акроним од *хеб*. ha-Lishka le-Kishrei Mada) која је била специјализована за крађу научних и технолошких достигнућа.[508] Такође, Јапан већ дуго „слови“ за државу чија предузећа имају праве приватне обавештајне службе итд.[509]

Економска и пословна шпијунажа присутне су и међу предузећима унутар граница једне државе. Ранија истраживања су показала да приближно 70 одсто обавештајне делатности против америчких фирми реализују друге америчке фирме, 23 одсто стране фирме, а само 7 одсто стране обавештајне службе.[510]

Подаци указују на чињеницу да је пословна шпијунажа и систем „мониторинга“ информација о конкурентима, потрошачима, пословним партнерима, тржишту и његовом развоју, као и о кључним смеровима развоја у науци, технологији, економији уопште и политици сагласан циљевима и интересима пословног субјекта. У суштини, савремена пословна шпијунажа представља интеграцију обавештајне методологије и информатичких технологија, примењених у оквиру пословног света.

---

[506] Johnson K. L.: *Secret Agencies. U.S. Intelligence in a Hostile World*, Yale University Press, 1996, p. 152.
[507] *Ibid*., p. 169.
[508] *Ibid*., p. 170.
[509] *Ibid*., p. 171.
[510] *Ibid*., p. 244.

Да би се успоставио ефикасан систем пословне шпијунаже, према мишљењу Тодора Петковића, експерта у овој области, потребно је интегрисати, организовати и ускладити неколико елемената: људски (кадровски), оперативни (делатност), организациони (оквир функционисања) и технички (информатички). То значи да је за изградњу система пословне шпијунаже потребно имати стручне људе који ће у оквиру одређеног организационог оквира, оперативно и уз помоћ савремених информатичких достигнућа реализовати задатке из оквира пословне шпијунаже.[511]

Посматрано из перспективе безбедности и заштите пословања од кибер претњи, важно је указати на још један, додатни, проблем. Овај проблем везан је за право на корпоративну приватност. У циљу што боље заштите од кибер претњи, америчка влада врши притисак на пословне корпорације да са њом, као и са другим корпорацијама у приватном сектору, размењују приватне информације о властитим мрежама које су изградиле или којима управљају.[512] Чињеница да је отприлике 85% критичне инфраструктуре у приватном поседу ствара тензију између владе и пословног сектора због владине намере да се меша у приватност корпорација.[513] Овај проблем ниже и друга питања везана за могућности интер-корпоративне сарадње због саме природе конкурентских приватних предузећа и жеље да се од ривала сачувају пословне тајне.

4.2.3. Инсајдери као фактор угрожавања безбедности пословања

Термин *инсајдер* се, према дефиницији Комитета за националну безбедност САД у области телекомуникација и информационих система (National Security Telecommunications and Information Systems Security Committee), односи на особу запослену у једном привредном субјекту, снабдевача добрима и услугама и, шире, на било кога ко располаже легитимном ауторизацијом за приступ информационом систему одређеног правног лица.[514] Под термином *инсајдер*, у најширем смислу,

---

[511] Петковић Т., *op. cit*., стр. 276.

[512] Homer-Dixon T.: "The Rise of Complex Terrorism", *Foreign Policy*, January/February 2002.

[513] Buxbaum P.: "U.S. Grapples with Cybersecurity", *ISN Security Watch*, October 10, 2007.

[514] The Insider Threat to U.S. Government Information Systems, National Security Telecommunications and Information Systems Security Committee, NSTISSAM INFOSEC/1-99 (Fort Meade, MD: July 1999), http://www.cnss.gov

можемо подразумевати оне злонамерне актере који дејствују прикривено, унутар и против организације чији су део.

Досадашња истраживања о односу између ИКТ и корпоративне безбедности су показала да је људски фактор једна од најслабијих карика у систему заштите лица, имовине и пословања.[515] У том смислу, могу се издвојити следећи битни елементи:

- Могућност утицања на нормално функционисање аутоматизованих инфраструктура подразумева поседовање специфичних информатичких знања, као и сазнања о мерама заштите конкретног система. Извршење напада није једноставно чак ни за оне који познају систем и имају на располагању посебно ефикасне инструменте.
- Заштитни механизми су често недовољни, а особље задужено за безбедност система неприпремљено за ефикасно спровођење активности надгледања и превенције.
- Успешан напад готово увек захтева одређено познавање система „изнутра“ или структуре која је мета напада.
- Управо ова упознатост са системом чини инсајдере најопаснијим актерима претње у пољу кибер безбедности.

Истраживање Института за рачунарску безбедност (Computer Security Institute – CSI) и Федералног истражног бироа (Federal Bureau of Investigation – FBI), извршено 2003. године на узорку менаџерâ, показало је следеће резултате: 45% испитаника је изјавило да има сазнања о случајевима неауторизованог приступа запослених информационом систему предузећа, а чак 80% испитаника указало је на злоупотребе рачунарске мреже предузећа.[516] Табела која следи приказује перцепцију испитаникâ о потенцијалним изворима претње.

Табела бр. 8: *Перцепција могућих актера кибер напада према истраживању "2003 Computer Crime and Security Survey CSI/FBI"*

ПОТЕНЦИЈАЛНИ ИЗВОР ПРЕТЊЕ	ПРОЦЕНАТ ИСПИТАНИКА
Независни хакери	82%
Незадовољни радници – инсајдери	77%
Национални конкуренти САД	40%
Стране владе	28%
Стране корпорације	25%

[515] Видети: Путник Н., *op. cit.*, стр. 125.

[516] *2003 CSI/FBI Computer Crime and Security Survey*, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

Слични резултати су добијени и у истраживању поновљеном 2006. године.[517]

Мотивисаност инсајдера за нарушавање безбедности кибер простора може бити различита: другачији систем вредности у односу на организацију која их запошљава, радозналост, освета, уцена, изнуда, нелегална зарада итд. У већини случајева, међутим, нарушавање безбедности није изазвано са умишљајем, већ наступа као последица слабог познавања система и безбедносних процедура или, пак, из непажње. Одређени чинови са атрибутом ненамерности (на пример, дезинсталација антивирусног програма, остављање лозинке на видноме месту или инсталација неауторизованог софтвера) отварају могућност злонамерним актерима за продор у рачунарски систем и приступ информационим ресурсима организације.

Истраживање спроведено у Европи 2005. године, показало је да 21% запослених дозвољава пријатељима и члановима породице да, код куће, користе службени рачунар.[518] Најчешће се службени рачунар употребљава за „сурфовање" Интернетом, што не само да повећава ризик од инфекције рачунара малициозним програмима (а у перспективи и рачунарске мреже компаније), већ и излаже поверљиве пословне документе неауторизованим лицима; 10% испитаника је признало да са Интернета „скида" садржаје за приватне потребе, тј. практикује ризично понашање, с обзиром на то да излаже информационо-комуникациони систем компаније ризику, а послодавца законским санкцијама; 5% испитаника је признало да је направило приступ заштићеним, поверљивим зонама пословног система фирме (мањи број је признао и крађу информација).

На основу резултата спроведеног истраживања дефинисане су четири категорије неодговорних радника:

- „Security softie[s]" („нежна срца") – у ову категорију спада већина запослених. Њих одликује ограничено познавање безбедносне културе; најчешће се ризично понашање ове групе своди на омогућавање приступа рачунарским ресурсима предузећа трећим лицима;

---

[517] Видети детаљније: *2006 CSI/FBI Computer Crime and Security Survey*, pp. 12, 25, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

[518] Leyden J.: *The enemy within*, November 21, 2005, http://www.theregister.co.uk. Чланак се ослања на истраживање које је урађено за „McAfee", угледну фирму за производњу безбедносних софтвера.

- „Gadget geek[s]“ („фанатици техничких направа“) – у ову категорију сврстани су они запослени који службене рачунаре користе за повезивање са разноразним хардверским уређајима, неауторизованим од стране администратора мреже или лица одговорног за унутрашњу безбедност организације.
- „Squatter[s]“ („непоштоваоци закона“) јесу они који користе ИКТ ресурсе компаније на недозвољен начин (за складиштење и дистрибуцију недозвољених садржаја, играње видео-игара и сличне активности).
- „Саботери“ представљају, статистички гледано, мали број запослених. У ову категорију сврстани су они који покушавају да приступе заштићеним информацијама или ресурсима ИКТ или, пак, који убацују малициозне програме у рачунарски систем компаније.

Последња категорија запослених, колико год статистички била безначајна, представља једну од најопаснијих претњи за безбедност пословања компаније. Шнајер сматра да је „злонамеран инсајдер опасан и скривен противник. Он је већ у систему који жели да нападне и на тај начин може да игнорише било коју периметријску[519] одбрану система сачињену ради заштите од спољашњег напада.“[520]

Са становишта кибер безбедности посебна пажња се, унутар категорије људског фактора, посвећује програмерима, тј. писцима софтвера.[521] У досадашњој пракси су евидентирани случајеви да писац софтвера намерно оставља отворена „споредна врата“ како би себи (или другом лицу) омогућио накнадни неауторизовани приступ систему. Многе корпорације, произвођачи софтвера, препуштају производњу појединих програмских сегмената стручњацима који нису запослени у корпорацији, а све чешће предузећима и појединцима стационираним у азијским земљама,[522] где су цене рада ниже него на Западу и где постоји технолошки *know how*. У азијском региону, међутим, постоје снажни покрети религиозног

---

[519] Периметријска одбрана је скуп техничких мера (хардвер и софтвер) усвојених ради одбране система од спољних напада.

[520] Schneier B.: *Secrets and Lies. Digital Security in a Networked World*, Wiley computer publishing, New York, 2000, p. 47.

[521] У категорију инсајдера спада, да подсетимо, и онај који снабдева организацију неким сервисом или добром.

[522] Најчешће у Индији, Малезији и Пакистану. Корпорација „Gartner Inc.“, која се бави истраживањима у пољу ИК технологија, проценила је да је још у 2004. више од 80% предузећа у САД започело активности везане за „offshore outsourcing“. Преузето из: Thibodeau P.: “Offshore’s Rise Is Relentless”, *Computerworld*, 2003, vol. 37, n. 26, p. 1.

фундаментализма, који у оквиру својих стратегија борбе укључују и регрутовање или сарадњу локалног становништва што ради на развоју софтвера, са циљем тајног убацивања малвера у комерцијалне производе који ће се накнадно користити у целом свету, као и за посебно осетљиве намене и за пружање специфичних услуга.

Афера са јапанским култом „Aum Shinrikyo“[523] јесте, у том смислу, еклатантан пример. У марту 2000. године, јапанска полиција је обзнанила аферу у којој је и сама била жртва. Према сазнањима, софтвер купљен ради надзора кретања 150 полицијских возила произвела је поменута секта. Преко посредничких фирми софтвером је, осим полиције, снабдевено и осамдесет приватних фирми и десет владиних организација. У тренутку када је афера откривена секта је већ поседовала класификоване податке о рутинском кретању 115 полицијских возила, а страховало се да су у самом производном процесу у софтвер убачене и додатне скривене апликације. Да убацивање малициозних програма у производе који се развијају у „спољашњем окружењу“ представља ризик, доказује и чињеница да је амерички GAO[524] наредио ревизију мера усвојених од стране Министарства одбране са циљем смањивања ризика који произлази из коришћења комерцијалних софтвера на подручју војних система.[525]

Представници софтверске индустрије, са друге стране, сматрају да се ризик за интегритет софтвера не може сводити само на „изворе у спољашњем окружењу“, с обзиром на то да се већина основних компоненти производа развија у Сједињеним Америчким Државама, где ради велики број инжењера иностраног порекла. Због тога би, верују они, било ефикасније контролисати и, по потреби, редефинисати

---

[523] „Aum Shinrikyo“ је религиозни покрет који је основао Shoko Asahara у Јапану 1987. године. Ова секта, која је достигла број од 40.000 следбеника у целом свету, званично је регистрована августа 1989. захваљујући закону о религијским удружењима. „Aum Shinrikyo“, који комбинује елементе будизма, хришћанства и варијације азијске традиције, постепено је постао апокалиптички покрет. Секта је извела низ насилних напада, од којих се посебно истиче напад на метро у Токију 20. марта 1995, у којем је живот изгубило дванаест особа, док је око 5.000 отровано гасом „сарин“. Shoko Asahara је осуђен на смрт вешањем, заједно са још једанаест поглавара секте.

[524] Government Accountability Office (GAO) јесте агенција која се бави евалуацијом програмâ, политичким анализама, давањем мишљења и доношењем одлука у вези с правним питањима широког спектра програма и активности федералне владе САД, у земљи и иностранству. Њен основни задатак је „да провери да ли су политике и програми усклађени са циљевима и реалним потребама друштва, и да контролише на који начин министарства и владине организације троше новац од пореза“. Према: GAO, http://www.gao.gov

[525] Wilson C.: *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report for Congress, 2005, http://fpc.state.gov

технике контроле квалитета од стране продаваца софтвера, независно од места његове производње. Међутим, строжа контрола би наметнула и веће трошкове производње и продужила време неопходно за пласирање нових производа на тржиште.[526]

Претња која потиче од умишљајних или ненамерних чинова ангажованог особља јасно указује у којој мери је људски фактор битан елемент кибер безбедности. Једна од препоручених стратегија за решење проблема састоји се у константном информисању запослених о ризицима, организационој политици и безбедносним процедурама, као и, у мери у којој је то могуће, запошљавању поузданог и провереног особља. Од велике важности је, такође, и перманентна едукација особља задуженог за безбедност − у циљу откривања, али и процене штете нанете од инсајдерâ, као и за имплементацију законских мера.

4.3. Индивидуални и друштвено-социјетални аспект кибер ратовања

4.3.1. Хакеризам и крекеризам

У популарној литератури и медијима честа је употреба термина „хакер“ као збирног назива за све субјекте претње у кибер простору. Хакери се, према овом колоквијалном одређењу, користе техникама „хакинга“ за нарушавање безбедности кибер простора. Термин „хакинг“ би, дакле, реферирао на скуп акција, способности, информатичких знања и познавања техника неопходних за извршење кибер напада. Хакингу се често приписује позитивна или негативна вредност, у зависности од тога ко га користи и са каквим циљем.

У афирмативном смислу се о хакингу говори као о активности у домену превенције и заштите рачунарских система. На пример, истиче се његов значај за указивање на рањивости одређеног система. Није редак случај да фирме које развијају ИКТ производе унајмљују хакере како би пронашли слабе тачке система. У

[526] Изјава S. Charney-a, шефа одељења за безбедносне стратегије Мајкрософта, дата на семинару *Information Technology in the 21st Century Battlespace*, одржаном 24. 7. 2003, http://commdocs.house.gov/committees/security/has294260.000/has294260_0f.htm

негативном контексту се технике хакинга критикују, јер се често користе за илегалан приступ туђим рачунарским системима.

Научни приступи проблему класификације субјеката претњи у кибер простору вођени су тежњом за научном објективношћу и семантичком прецизношћу. У стручној литератури се, у том смислу, прави разлика између актера претњи на основу циљева које теже да остваре и њихове мотивисаности за нарушавање безбедности кибер простора. На основу мотивације као критеријума за класификацију могли бисмо издвојити три различите категорије актера: хакери у ужем смислу речи, крекери и хактивисти. За све наведене категорије актера заједничко је коришћење техника хакинга.

Према прилично романтичној аутодефиницији „прави“ хакер или *хакер са белим шеширом* (*енгл*. white hat hacker или sneacker) јесте „особа која ствара изван стандардних техничких лимита, користећи сопствене вештине, са циљем да надмудри и креативно превазиђе ограничења која му се намећу, не само у пољима његових интересовања (која се могу сврстати под информационе технологије) већ и у свим осталим аспектима живота.“[527] Хакери, дакле, „траже спознају“ без штете за друге и, када је могуће, покушавају да допринесу побољшању општих услова кибер безбедности.

Циљ хакера је да се подробно информише о систему који га интересује или који му окупира пажњу. Међутим, углавном нису на располагању све неопходне информације, нити су лако доступне (најчешће зато што нису објављене од стране произвођача хардвера односно софтвера). Тај недостатак хакер решава практичним истраживањем – „упадом“ у систем, тј. хакингом. Хакинг је, дакле, инструмент за добијање информација и сазнања који, иако се сматрају заштићеним и поверљивим, и имају власника – по хакерском етичком кодексу припадају заједници.

Без обзира на привидну нешкодљивост хакинга, чија је корист реална само у случајевима када је напад извршен под контролом онога ко жели да тестира свој производ, немогуће је не сумњати у добронамерност таквог деловања. Шнајер позива на размишљање: „Замислите да се вратите кући и нађете на фрижидеру

[527] Сигурност рачунарских мрежа, http://www.conwex.info/draganp/SRM_Predavanje_16.pdf

поруку на којој пише: 'Контролисао сам безбедност врата у комшилуку и открио да су твоја откључана. Само сам бацио поглед, али нисам узео ништа. Требало би да промениш браву.' Да ли бисте се осећали угрожено? Наравно да бисте."[528] Са скептичке позиције би, дакле, била оправдана употреба термина „хакер" за денотацију било којег субјекта претње.

Са друге стране, неки инсистирају на семантичкој доследности, која подразумева повлачење разлике између „трагалаца за спознајом" и других, злонамерних актера у кибер простору. Сигурно да је један од узрока терминолошког неспоразума недостатак емпиријских сазнања. Од тога како ће овај спор бити решен зависиће и потенцијална квалификација хакера као посебне, аутономне, категорије субјеката претњи са атрибутом ненамерности или, пак, поистовећивање ових учинилаца са категоријом злонамерних актера –крекера.

Такозвани *крекери*, или *хакери са црним шеширом* (*енгл*. black hat hacker), за разлику од претходних, имају циљ да посредством информационих система, нелегалним радњама (крађа или модификација информација, шпијунажа, пиратерија софтвера итд), остваре одређену корист или, једноставно, нанесу штету рачунарском систему жртве (на пример, техником web defacement-a). У ову категорију могли бисмо сврстати највећи број субјеката претњи кибер безбедности, тј. све оне актере чија се мотивисаност може описати као декадентна, усмерена на рушење друштвеног система и општеприхваћених вредности.

Уколико, осим мотивационог фактора, као основног критеријума категоризације, у разматрање узмемо и способности актера, можемо у категорију крекера укључити и оне актере чији је жаргонски назив „лејмери" (*енгл*. lamers)[529] или „деца скриптова" (*енгл*. script kiddies).[530] Реч је о обесним појединцима који не владају у довољној мери информатичким знањима. Искључиви циљ кибер вандала јесте наношење штете корисницима глобалне мреже. Ови појединци најчешће употребљавају малициозне програме како би инфицирали рачунаре корисникâ Интернета у циљу омогућавања приступа зараженим системима ради модификовања

[528] Schneier B.: "Airplane Hackers", *Crypto-Gram Newsletter*, 15. 11. 2003, http://www.schneier.com

[529] Израз који се користи у ироничном смислу и значи „шепав".

[530] „Script" је листа команди (информатичког програма) које се могу извршити без директне интеракције између корисника и програма.

или уништавања информација ускладиштених на њима. Осим малвера, у употреби су и специфични алати, „готови“ програми доступни на Интернету, намењени извршавању напада на web сајтове.

Досадашња истраживања показују да је код деструктивно настројених појединаца, крекера, све израженија и тежња ка удруживању у веће организоване скупине.

4.3.2. Хактивизам

Хактивизам је специфичан вид хакерског деловања, који се, због прокламованих циљева и изабраних објеката напада, може сврстати под облик герилске борбе. Реч је о новом облику герилске борбе која се води на електронском пољу или, другачије речено, о идеолошки мотивисаним групама чије је деловање усмерено против електронских контролних и информационих система и технологија непријатељских земаља. Хактивисти у кибер простору виде инструмент којим не-државни актери могу да учествују у конфликтима ван националних граница. Према њиховим етичким начелима не могу само државе бити овлашћене за започињање ратова или агресије. За разлику од државе, „хактивисти се не сматрају ограниченима законом о оружаном конфликту или Повељом Уједињених нација“.[531]

Хактивисти користе исте методе и технике као и хакери, с тим што је њихов циљ да кибер нападом привуку пажњу јавности на одређени друштвени или политички проблем. Пример хактивизма би представљао напад на сајт чији садржај нападач перципира као противан личним политичким убеђењима, мењањем почетне странице сајта – истицањем видљиве поруке која је отворено у контрасту са вредностима које заступа дотични сајт. У многим случајевима нападач и блокира сајт, најчешће нападом типа DoS. Хактивизам пружа многе предности, првенствено визибилност по ниској цени, без географских ограничења и без потребе за излажењем на улицу и јавним демонстрирањем.

---

[531] Denning D.: “Cyberwarriors, Activists and Terrorists Turn to Cyberspace”, *Harvard International Review*, Vol. XXIII, No. 2, 2001, pp. 70–75.

Хактивизам постаје запажени вид грађанске непослушности средином 90-их година прошлог века. У пролеће 1998. године британски хакер под псеудонимом „JF“ неовлашћено је изменио почетне странице на скоро 300 Интернет сајтова. Оригиналне садржаје он је заменио сликом облака у облику печурке и текстом: „Ово масовно изобличавање (defacement) посвећено је свим оним људима који желе да виде мир у свету“. Међу нападнутим сајтовима били су сервери индијског Центра за атомска истраживања и Саудијске краљевске породице.[532] У том тренутку, то је био највећи напад ове врсте. Од тада, евидентирани су бројни случајеви неовлашћеног приступа сајтовима чији се садржај замењује другим, политичким, садржајем.

Данас је овај облик „електронске непослушности“ у широкој употреби од стране великог броја друштвених група и других политичких активиста на свим континентима. У зачетку, њихова активност евидентирана је у Великој Британији, Аустралији, Индији и Кини.[533]

Интересантно је истаћи да су хактивисти били активни и у Србији, 1999. године, током агресије НАТО-а на Србију и Црну Гору. Најагилније су биле две хактивистичке групе, *Црна рука* и *Српски анђели*, чији су чланови нападали електронске базе података америчких, британских и албанских обавештајних, војних и државних служби, те присвајали, мењали и брисали одговарајуће информације. Поменимо и занимљиву чињеницу – без претензија да се бавимо дубљом анализом његових политичких и социјалних узрока – да је овај вид деловања врло брзо попримио озбиљније размере, претећи да прерасте у први електронски рат: српске групе су добиле подршку руских хакера, а након бомбардовања кинеске амбасаде, придружиле су им се и кинеске хакерске групе. Удружено деловање хакерских организација онеспособило је на неколико недеља важне америчке војне информационе системе, што је довело до развоја догађаја са неочекиваним последицама: америчка служба FBI покренула је велику „контраофанзиву“ у циљу подизања нивоа заштите рачунарских система, при чему су ухапшене десетине

---

[532] Glave J.: “Anti-Nuke Cracker Strikes Again”, *Wired*, 3 July 1998.

[533] Wray S.: *Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics*, A paper for The world Wide Web and Contemporary Cultural Theory Conference, Drake University, 1998.

америчких хакера. То су америчке хакерске групе схватиле као објаву рата, па су и саме почеле да учествују у акцијама против служби властите државе.

Да се по наведеним, апстрахованим диференцијалним карактеристикама – начину настанка, организацији, циљевима и борбеној тактици – хактивистичка и војна герила[534] практично не разликују, сведоче објаве и прогласи хактивиста: „*Црна Рука је устала у 'електронску одбрану' интереса ове земље и не одустаје од напада на сајтове који пласирају лажи о ситуацији у овој земљи*“, и даље, припадници *Црне руке* тврде да се залажу за „*мир, љубав и благостање на целој планети*“, а као доказ прилажу чињеницу да „*никада нису непотребно обрисали податке, иако су били у прилици*“.[535] „Нова герила“ се, дакле, ограђује од хакера чији је циљ искључиво малициозно и деструктивно деловање усмерено према „обичним“ корисницима Интернета, већ заступа поменуту идеологију националног ослобођења, промовишући при том пацифистичку идеју општег мира и поштујући етичко начело ненаношења штете неутралним корисницима електронских ресурса.

Хипотетички гледано, у случају да довољно велика група хактивиста широм света синхронизовано покрене електронски напад, величина штете би била огромна. Осим тога, у таквој ситуацији било би тешко идентификовати правог актера напада, тј. разликовати хактивистички напад од почетне фазе напада у оквиру војне кампање кибер ратовања.

На крају, није наодмет још једанпут нагласити тезу да је кључна разлика која квалификује актере као претњу по кибер безбедност њихова мотивација – од оних који је готово немају, као што су кибер вандали, оних који се служе хакингом за терористичке нападе, попут кибер терориста, обичних кибер криминалаца, до оних који се боре у служби државе за доминацију над информацијом, тзв. кибер ратника.

---

[534] О појму и суштини гериле видети више у: Милашиновић Р., Путник Н.: „Герила као специфичан вид друштвеног конфликта“, у: *Герила на Балкану: борци за слободу, бунтовници или бандити*, Tokyo: University Meiji, Institute for Disarmament and Peace Studies, Београд: Институт за савремену историју, Факултет безбедности, 2006, стр. 327–339.

[535] Дингарац Д., Станчевић Т.: „Српски хакери Црна рука“, *Свет компјутера*, новембар 1998.

4.3.3. Друштвено-политички активизам посредован друштвеним мрежама на Интернету

Посматрајући са технолошког, социолошког, а потом и безбедносног и политиколошког становишта, Интернет је начинио прекретницу у схватању и функционисању свакодневног живота и рада. Небројене, разноврсне информације (у виду текстуалних, фотографских, аудио или видео записа), путем web презентација и пратећих апликација, постале су доступне за сазнавање, допуну и размену, стотинама милиона људи широм Планете. Таква виртуелно-информациона повезаност била је инспирација и основа за креирање и имплементацију онога што данас устаљено називамо друштвеним мрежама, међу којима су најпознатије Фејсбук (*енгл*. Facebook) и Твитер (*енгл*. Twitter).

Као модеран и данас неизбежан облик комуницирања и повезивања људи без директног контакта (не улазећи у педагошко-психолошку оправданост таквог „тренда"), друштвена мрежа собом носи и комплексне друштвено-политичке и безбедносне импликације. Оно што друштвене мреже разликује од других web страница, јесте узрочно-последична веза између садржаја Интернет презентације и њених корисника. Заправо, корисници су ти који формирају и шире обим и обухват друштвене мреже и они сами су суштина, циљ и средство настанка и опстанка друштвене мреже, а не пасивни посматрачи, што је случај са осталим web страницама. Ове чињенице условиле су да друштвене мреже убрзо прерасту од виртуелног места за упознавање и комуницирање, до простора на којем се (поред мас-медија), промовишу идеје, идеологије, подстичу кампање, мотивишу и групишу људи сличних ставова и жеља. Поред информативне и забавне црте, web странице овога типа, попримају и психолошко-емотивне обрисе, које чланови друштвене мреже кроз своју активност преносе, чинећи своје ставове, дилеме и осећања јавно доступним. Друштвене мреже данас су животна чињеница за трећину светске популације.[536]

Са једне стране, друштвена мрежа јесте брз, ефикасан и врло комуникабилан медиј за упознавање, сарадњу и окупљање људи сличних склоности и интересовања.

---

[536] Бошковић М., Путник Н.: *Улога друштвених мрежа у савременим социо-политичким и безбедносним појавама*, XIX Телекомуникациони Форум – Телфор, зборник радова, Београд, 2011.

Са друге стране, пак, ова својства друштвених мрежа могу бити у функцији ангажовања њених чланова те њиховог подстицања на практичну акцију. Дакле, она јесте катализатор политичког активизма, што некада може представљати и субверзивну делатност.

Развој друштвеног умрежавања је за резултат имао интензивирање дебата о бројним проблемима у друштву. Овај вербални онлајн рат се, посматрано хронолошки, прво појавио у САД.[537]

Рана истраживања показују да су најактивнији корисници друштвених форума по опредељењу били либертаријанци[538] који страствено верују у способност пословних кругова и појединаца, а не државе, да могу решити проблеме данашњице.[539] Лако је уочити како се идентитет групе може брзо оформити, оспособити и ојачати употребом дистрибуираног рачунарства. На виртуелним друштвеним мрежама усамљени гласови лако и брзо добијају одјек. Корак који дели наизглед безазлено лобирање и ватрено критиковање стања у друштву од дигиталне анархије је врло мали.

Оно што чини дистрибуирано рачунарство, или да будемо прецизнији - друштвене мреже, тако привлачним појединцима и групама, заинтересованим да се њихово мишљење чује, је одсуство ограничења. Цензура, особито у јавној сфери, није нов концепт. Федерална комисија за комуникације (Federal Communications Commission - FCC) у САД регулише садржај радио и телевизијских преноса до те мере да неки напомињу да и нема доказа слободе говора, што је Уставом гарантовано право. Влада, ипак, не контролише Интернет онако како то чини са штампом, радијом и телевизијом. Иако је било правних покушаја (и још увек их има) да се контролише садржај пласиран на Интернету (нпр. Закон о пристојности у комуникацијама I и II), њих су спречили заступници слободе говора и интелектуалне слободе, од којих су најзапаженији Америчка унија за грађанске слободе (American

---

[537] Cronin B.: "Digibabble", *International Journal of Information Management*, 18(1), 1998., pp. 73 – 74.

[538] Либертаријанизам (слободарство, либертерство) је политичка филозофија која заступа становиште да би појединци требали бити слободни да чине што год желе са собом и својом имовином све док не угрожавају ову исту слободу осталих. У познате либертаријанце можемо сврстати Џимија Велса, суоснивача Википедије као и Џулијана Асанжа, оснивача контроверзног сајта Викиликс.

[539] Katz J.: "The digital citizen", *Wired*, 5(12), 1997., pp. 68 – 82.

Civil Liberties Union - ACLU) и Удружење америчких библиотека (American Library Association - ALA).[540] Због тога Интернет остаје арена комуникације где се дискурс, позитиван и негативан, рационалан и ирационалан, слободно развија.

Мрежно рачунарство, дакле, довело је до процвата електронских форума. Ова дигитална састајалишта омогућила су појединцу и различитим или маргинализованим групама људи да размењују најразличитије идеје. Борбене активистичке групе попут удружења за заштиту права животиња или геј и лезбејских организација, које су одлучне у томе да се изборе за једнака права својих чланова, употребљавали су форуме као једно од својих најранијих оружја за јефтино и далекосежно изражавање сопственог мишљења. Стратегија и тактика, као такве, нису биле од значаја. Њихов циљ је био масовно ширење идеја.

Осим што су омогућили слободну размену идеја, Интернет форуми и њихови наследници, друштвене мреже, су истовремено одшкринули врата дигиталног окружења групацијама жељним вођења неких властитих облика кибер рата.

Са напретком глобалне рачунарске мреже и графичких корисничких интерфејса, социјални и политички активисти имају још више простора да одржавају дебате, доказују властите „истине“, или оштро критикују. Религиозно или идеолошки мотивисане групације сада на располагању имају средства за вођење електронског џихада. Познати су случајеви употребе друштвених мрежа од стране активистичких група које се залажу за забрану абортуса, еутаназије и клонирања. Оне су, на неки начин, биле наговештај милитаризације друштвеног и идеолошког активизма.

Последњих година друштвене мреже попут Фејсбука и Твитера, постале су незаобилазни елемент у окупљању политичких активиста и чак покретању револуционарних промена у државама. Њихова улога и значај постојања нарочито су долазили до изражаја у земљама условно речено недемократског уређења или озбиљних друштвено-правних поремећаја, у којима су медији попут радио и телевизијских станица, штампаних и Интернет часописа контролисани од стране

[540] Cronin B., Crawford H., *op. cit*. p. 261.

владајућих структура. Испоставило се да ауторитативни режими нису обратили пажњу на раширеност и значај друштвених мрежа, па је њихова цензура изостала или је, пак, била *post factum* примењена.

Јануара 2011. године, два масовна окупљања против актуелних власти, одиграла су се у кратком временском раздобљу, а оба су била потакнута активизмом и организовањем преко Фејсбук и Твитер мрежа. Према писањима журналиста-извештача медија попут *The Observer* и *The Time*, режим на чијем је челу Бен Али, у Тунису спроводи контролу над информацијама које се тамошњим грађанима пласирају преко медија. Међутим, Фејсбук је изостао од цензуре. На тај начин Тунижани су могли да пронађу и размене информације и искуства која су им преко других гласила била недоступна. Противници режима су успели да на овој друштвеној мрежи окупе истомишљенике, организују, координирају и спроведу масован протест против власти у земљи. Инспирисани овим протестом, незадовољни становници Египта, након само неколико дана од тзв. „Тунижанске Фејсбук револуције", успели су да на сличан начин организују демонстрације у сопственој земљи. На Фесбук налогу, названом *Револуционарни дан*, отвореном у циљу окупљања опозиционара Мубараковом режиму, за протесте заказане за 25. јануар 2011. пријавило се 85.000 египћана. Организатори протеста у данима пред демонстрације истицали су да је велики успех ако на улице изађе и половина људи који су се идеји и акцији прикључили на онлајн начин. Блиски исток је ушао у паничну недељу, у којој су се ауторитарни режими од Алжира до Јемена суочили са ефектима пада Тунижанског председника Бен Алија.[541]

Власти су на овај вид онлајн активизма одговориле не само блокирањем Твитера и Фејсбука, већ и целокупног Интернета. У запањујућем развоју догађаја, без преседана у модерној историји Интернета, земља са преко 80 милиона људи нашла се скоро сасвим искључена од остатка света.

Наравно, употреба друштвених мрежа од стране политичких или друштвених активиста не мора нужно резултирати нежељеним исходима. У теорији, кибер активизам је подједнако у стању да постигне позитивне резултате, баш као што има негативне и разорне ефекте по друштво. Ипак, ако се узме у обзир да

[541] Hauslohner A.: "Is Egypt about to have a Facebook revolution", *The Time*, January 24, 2011.

глобална рачунарска мрежа дозвољава објављивање многобројних становишта, постоји ризик да би кохезија националне државе могла ослабити, што би довело до огромног броја конкурентских микро-циљева и локализованих система вредности. Губитак друштвене кохезије и националног идентита би, у најгорем случају, могао бити иронична цена дигиталне демократије.

4.3.4. Кибер клевета и виртуелно озлоглашавање

Сваки појединац је рањив на различите врсте отворених и прикривених напада од стране злонамерних актера, било да за циљ имају прављење несланих шала или јасне криминалне намере. Хакерска култура описује електронске провале и преузимање другог идентитета као враголасто али прихватљиво понашање.[542] Жртва, међутим, на ствари гледа другачије. Осећај нарушавања и губитка личног мира и приватности може имати дуготрајне психолошке последице.

Као и у случају војних и пословних ресурса, информациона имовина појединца и његов онлајн идентитет су потенцијално угрожени од стране различито мотивисаних хакера. То никако не значи да само мали број појединаца може постати потенцијална мета систематског напада злонамерних актера у кибер простору.

Посебно осетљиву категорију представља популација деце и адолесцената. Они су, уједно, и најчешћи и најлаковернији корисници друштвених мрежа. Услед недостатка едукације у погледу опасности којима су изложени на друштвеним мрежама, најмлађи корисници на своје профиле непромишљено „каче“ информације и мултимедијалне садржаје који могу бити злоупотребљени од стране педофила и других патолошких личности. Чест је случај да информације које деца остављају на корисничком профилу бивају злоупотребљене од стране њихових вршњака. Реч је феномену тзв. *kiber bulinga* (*енгл*. cyber-bullying) односно задиркивања, кињења или, у тежим облицима, злостављања у виртуелном свету. Овај вид тортуре може оставити значајне психолошке последице, о чему се у стручној литератури водила широка дебата након откривања првог случаја виртуелног силовања.[543]

---

[542] Thomas D.: *Hacker Culture*, University of Minnesota, Minneapolis, 2002, p. 115.

[543] Видети више у: Џонсон Д.: *Компјутерска етика*, Службени гласник, Београд, 2006, стр. 267.

Кронин и Крафорд сматрају да би се, због тога, могло чак и преиспитати веровање у Први амандман,[544] док Дибел пише: „Што сам озбиљније схватао појам виртуелног уништавања, то сам био мање у стању да озбиљно схватим идеју слободе говора, са њеном јасном поделом света на симболички и реални.“[545] Дигитални медији опскрбљују непријатеља знатно богатијим и моћнијим арсеналом алата којима се може упустити у психолошко ратовање, како на индивидуалном тако и на глобалном нивоу. Кибер клеветање или дигиталне кампање за озлоглашавање имају потенцијал да допру до невероватно великог броја људи, огромном брзином, и да, при томе, нанесу велике фрустрације и колатералну штету жртви. Поновно успостављање поверења и спасавање репутације у јеку виртуелних кампања за озлоглашавање представљају велики изазов нападнутим појединцима и колективитетима.

Није тешко замислити ситуацију у којој злонамерни актер намерава да уништи углед и репутацију реномираног научног истраживача. Пракса у целом свету је да се на јавним (а све чешће и приватним) сајтовима публикује радна биографија истраживача са његовим целокупним научним опусом, други релевантни подаци као и мноштво личних детаља. Нападач поседује одређени број опција на располагању: он би могао систематски да уништава податке истраживача; отпочне кампању за компромитовање објављивањем непоткрепљених, иако на први поглед уверљивих, критика на рачун његових истраживања на великом броју мејлинг листа, или да пошаље члановима научне заједнице дезинформације о датом истраживачу.

Лакоћа са којом јавне кампање „оцрњивања“ могу бити отпочете на Интернету ствара значајну диспропорционалност у корист нападача. Мета напада се ставља у положај да се брани и у стању је несигурности поводом нападачевог идентитета, мотива, локације, циљева, као и тога да ли је напад извршио појединац или група људи. Она, најчешће, и не зна коме се може обратити за помоћ у таквој ситуацији будући да је у већини држава изражена конфузија надлежности над оваквим деликтима. Даље, хакер може одабрати и да преузме виртуелни идентитет

---

[544] Cronin B., Crawford H., *op. cit*., p. 261.

[545] Dibbell J.: “A rape in cyberspace or how an evil clown, a Haitian trickster spirit, two wizards, and a cast of dozens turned a database into a society“, *The Village Voice*, December 21, 1993, p. 41.

мете напада, тј. жртве. Онтолошко ратовање је, стога, још једна од нових опција у оквиру дигиталног борбеног простора.

4.3.5. Кибер криминал

Глобална рачунарска мрежа отворила је нове могућности за извршавање криминалних дела. Интернет, који је по својој природи рањив и несигуран, услед огромног броја корисника, отворености и правне нерегулисаности, постао је полигон, али и идеално скровиште за криминалце различитог типа.

Са аспекта правних наука, у *кибер криминал* спадају они деликти који су инкриминисани законима. Ми смо до сада користили шири појам *кибер претње*, будући да он реферира и на инкриминисане радње, али и на оне које у важећим кривичним законицима још нису проглашене кривичним делима. Ово разјашњење је неопходно узети у обзир како би се избегле семантичке забуне.

Реномирани стручњак на пољу кибер безбедности, Брус Шнајер, сматра да су криминалци тренутно водећи протагонисти напада у кибер простору.[546] У 2004. години је, на пример, кибер криминал у САД превазишао величину посла у односу на дрогу и достигао цифру од 105 милијарди долара. Деликти у кибер простору у области индустријске шпијунаже, производње и дистрибуције педофилске порнографије, манипулације берзанским тржиштем, изнуђивања и пиратерије толико се повећавају да правни систем није у стању да им се супротстави.[547]

Осим израза „кибер криминал“, неретко се употребљавају и други термини: *Интернет-криминал*, *електронски криминал*, *криминал високих технологија*, *мрежни криминал* итсл. Не постоји општеприхваћена дефиниција кибер криминала. У покушају да протумаче размере ове врсте криминала и његове последице, Уједињене нације су на Десетом конгресу посвећеном превенцији криминала и третману починилаца, у документу *Криминал везан за рачунарске мреже* (*енгл*. Crime related to computer networks), под кибер криминалом подразумевале „криминал

---

[546] Schneier B.: *The Hackers are Coming!*, http://www.schneier.com

[547] Изјава Valerie McNiven, специјалисте финансија и безбедности Светске банке и саветника америчке владе за питања кибер криминала, током самита Riad о питањима кибер безбедности у области банкарства, 29. 11. 2005, http://www.channelregister.co.uk

који се односи на било какав облик криминала који се може извршавати посредством рачунарских система и мрежа, у рачунарским системима и мрежама или против рачунарских система и мрежа".[548] То је, у суштини, криминал који се одвија у електронском окружењу. Ако се под рачунарским системом подразумева „сваки уређај или група међусобно повезаних уређаја којима се врши аутоматска обрада података (или било којих других функција)", како је то дефинисано у Конвенцији о кибер криминалу (*енгл*. Convention on Cybecrime)[549] Савета Европе, онда је јасно да овог криминала нема без њих и рачунарских мрежа. Кибер криминал је комплексан феномен, а сâм појам се сматра кишобран-термином, који покрива разноврсне криминалне активности, укључујући нападе на рачунарске податке и системе, нападе везане за рачунаре, садржаје или интелектуалну својину.[550]

Према неким ауторима, о кибер криминалу можемо говорити ако је криминално дело „извршено коришћењем кибер технологије у кибер домену".[551] Остале деликте, чији се учиниоци користе кибер технологијом, а који нису извршени у кибер простору, исправније је називати криминалним деликтима повезаним са кибер технологијом (*енгл*. Cyber related crimes).

---

[548] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, http://www.oun.org

[549] *Convention on Cybercrime*, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[550] При томе се рачунарска мрежа, односно информационо-комуникациона технологија, појављује у вишеструкој „улози", као:

а) Циљ напада – нападају се сервиси, функције и садржаји који се налазе на мрежи. Краду се услуге, подаци, идентитет, оштећују се или уништавају делови или цела мрежа и рачунарски системи или се ометају њихове функције.

б) Алат – криминалци су од памтивека користили различита оружја и оруђа. Модерни криминалци данас успевају да не „испрљају" руке користећи мрежу за постизање циља.

в) „Окружење" у којем се напади реализују. Најчешће то окружење служи за прикривање криминалних радњи, као што то веома вешто успевају даураде педофили, а ни други криминалци нису ништа мање успешни.

г) Доказ – Мрежа и ИКТ се могу користити у доказном поступку за кибер криминал.

Према: Дракулић М., Дракулић Р.: *Cyber криминал*, 2005, http://www.bos.org.yu/cepit/drustvo/sk/cyberkriminal

[551] Tavani H. T.: *Ethics and Technology: Ethical Issues in an Age of Information and Communications Technology*, Hoboken, John Wiley & Sons Inc., 2003, p. 103.

Савет Европе је, 2004. године, у *Извештају о организованом криминалу: Претња кибер криминала* под кибер криминал прагматично сврстао следеће категорије дела:[552]

- дела против поверљивости, интегритета и расположивости (доступности) података (*енгл*. Computer data) и рачунарских система (*енгл*. Computer systems) – у ову категорију се, уопште узев, могу сврстати кибер напади (неовлашћен приступ неком систему, напади типа DoS, напади помоћу малициозних програма, фишинг итд);
- традиционална дела извршена уз помоћ рачунара (*енгл*. Computer related traditional crimes), попут: превара, фалсификовања, злоупотребе кредитних картица, изнуда итд;
- дела везана за садржаје (*енгл*. Content related offences) – поседовање, дистрибуција, трансмисија и складиштење недозвољених садржаја (порнографских, расистичких итд);
- дела везана за кршење ауторских и сродних права (неовлашћена репродукција и дистрибуција неауторизованих примерака аудио/видео-програма, банака података, дигиталних књига и, уопште, радова у електронском формату;
- дела везана за нарушавање приватности (неовлашћен приступ системима који садрже личне податке, прикупљање и дистрибуција личних података итд).

На основу претходно изнетог може се констатовати да су кибер простор и, уопште, информационе технологије постали окосница диверзификације криминалних дела и инструменти који криминалним организацијама омогућавају бољу оперативну ефикасност. Није случајно то што се хакинг, који је иницијално представљао чисто хобистичку активност, последњих година постепено трансформисао у криминалну активност. Управо је тежња за нелегалним стицањем профита оно што разликује нове криминалце од традиционалних хакера, који су мотивисани забавом, славом или, једноставно, злобом.

Али, прављење разлике између хакерâ и криминалаца не може се сводити само на дивергенцију у погледу мотивације. Постоје и други елементи који чине нове агресоре опаснијима и потенцијално штетнијима у односу на оне којима је

---

[552] *Organised crime situation report 2004 – The threat of cybercrime*, Council of Europe, Strasburg, 6. 9. 2004, http://www.coe.int

хакинг хоби. Хакерима је циљ да перманентно развијају нове, софистициране технике напада, док су криминалци заинтересовани једино да достигну циљ, и у ту сврху су спремни да користе било који инструмент, софистициран или деструктиван. Хакинг је праћен жељом за доказивањем и скретањем пажње на постигнути учинак, док је тежња кибер криминалаца усмерена на прикривање учињених дела. Хакери бирају своје жртве на основу угледа који поседују у области информационо-комуникационих технологија, критеријума престижности, на основу којег њихово дело добија на важности, док криминалци бирају жртве на основу опортунистичких критеријума и спремни су да преузму већи ризик од хакера, који се труде да се никада не изложе опасности да буду ухапшени.

Према мишљењу професора Мирјане и Ратимира Дракулића, профил кибер криминалца карактеришу још и софистицираност, продорност, техничка поткованост, бескрупулозност, опседнутост и понекад осветољубивост: „Он све чешће не жели да буде сâм, већ му је потребно друштво, као што му је неопходна и 'публика'. Лакоћа 'вршљања' кибер простором даје му осећај моћи и неухватљивости. Ови осећаји нису без разлога, јер стварно га је изузетно тешко открити у моменту чињења дела, што, углавном, представља и 'прави' тренутак за његово идентификовање и хватање."[553]

О учесталости поменутог феномена трансформације хакинга у кибер криминал последњих година сведоче подаци о извршеним нападима у периоду од јануара до јуна 2005. године. Према истраживању британске *BT Counterpane*, компаније за пружање услуга у области заштите рачунарских мрежа, финансијски сектор је, по угрожености, на другоме месту, одмах иза технолошког. Велики број напада уперених против финансијског сектора извршен је са простора Балкана, а већина њих са територије Румуније, једне од најпознатијих земаља по бројности организација које се баве кибер криминалом.[554]

[553] Дракулић М., Дракулић Р., *op. cit*.
[554] BT Counterpane, http://www.counterpane.com/

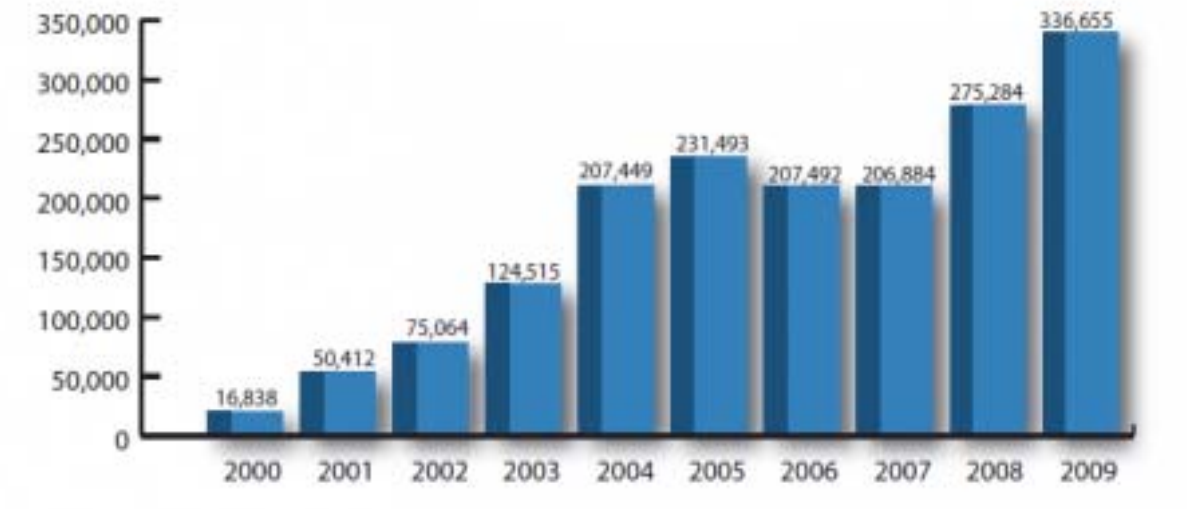
Табела бр. 9: *Статистика извршених напада у периоду јануар–јун 2005. године по секторима*

СЕКТОР	ПРОЦЕНАТ ИЗВРШЕНИХ НАПАДА
Технолошки	26%
Финансијски	18%
Биолошко-здравствени	17%
Осигурање	9%
Јавна управа (владин сектор)	8%
Мануфактурна производња	7%
Малопродаја	6%
Транспорт	1%
Медији	2%
Индустријска производња	1%
Услуге/Енергија	4%
Игре на срећу	1%
Непрофитни	0%

Извор: *Извештај BT Counterpane-а од 13. децембра 2005. године, http://www.counterpane.com*

Статистика FBI о кибер криминалу показује тренд повећања ове врсте деликата на годишњем нивоу.

Графикон бр. 1.: *Број пријављених кибер деликата FBI-ју по годинама*



Извор: The Federal Bureau of Investigation and Internet Crime Complaint Center, http://scamfraudalert.wordpress.com/2010/03/13/fbi-2009-cybercrime-statistics

Осим што број деликата расте, уочљива је и промена у њиховој врсти и заступљености. У табели која следи приказане су најчешће жалбе грађана по питању кибер криминала, упућене Федералном истражном бироу током 2009. године.

Табела бр. 10: *Предмет жалбе и проценат пријава*

ПРЕДМЕТ ЖАЛБЕ	ПРОЦЕНАТ ПРИЈАВА
Нарушавање приватности електронске поште од стране FBI	16,6%
Неиспоручена роба купљена ел. путем	11,9%
Додатно наплаћене услуге у ел. трговини	9,8%
Крађа ел. идентитета	8,2%
Финансијске преваре	7,3%
Преваре друге природе	6,3%
Спем	6,2%
Преваре везане за кредитне картице	6,0%
Преваре на виртуелним аукцијама	5,7%
Оштећења рачунара	4,5%

Извор: The Federal Bureau of Investigation and Internet Crime Complaint Center, http://scamfraudalert.wordpress.com/2010/03/13/fbi-2009-cybercrime-statistics

Перцепција потенцијалних жртава, такође, сведочи о томе да је кибер криминал достигао забрињавајуће размере. Резултати анкете коју је спровела корпорација IBM у 600 америчких предузећа показали су како 57% менаџера предузећа у сектору здравства, финансија и трговине сматра да мањак профита, утрошено време запослених на превенцију или поправљање штете нанете кибер нападом и губитак поверења од стране клијената представља већи проблем него конвенционални криминал.[555] Најзабринутији су менаџери финансијског сектора (71% испитаника). Према истом истраживању, 74% анкетираних водећих службеника информационе безбедности (*енгл*. Chief Information Security Officer) признаје да претња кибер напада од стране инсајдера представља значајан ризик, док 84% њих примећује да организоване кибер криминалне групе замењују традиционалне хакере по опасности претње.

[555] Leyden J.: *Cybercrime costs a bit more than physical crime*, http://www.channelregister.co.uk

Перцепција није много другачија ни у другим регионима света. Резултати сличног истраживања, спроведеног у шеснаест земаља света,[556] показали су да се штета нанета кибер криминалом сматра већом (43% испитаника) од штете нанете традиционалним криминалом (42% испитаника). Док већина америчких фирми верује да је усвојила одговарајуће противмере, само половина предузећа других земаља (53%) оцењује да је одговарајуће припремљена, док обе групе деле исте страхове у погледу штете нанете кибер криминалом. Обе групе испитаника страхују од губитка профита (63% америчких испитаника и 74% испитаника ван територије САД) и губитка клијената (56% и 70%), што значајно утиче на њихово пословање. Поготово се не-америчка група показала осетљивом на могућу штету нанету имену или репутацији фирме (69% у односу на 40% америчких испитаника).

Додатно истраживање које је спровео Питер Трокслер (Peter Troxler), реномирани криминолог са специјализацијом у области информационих технологија, у сарадњи са надлежним органима који се баве деликтима у пољу високе технологије у Великој Британији, Француској, Немачкој, Италији, Холандији и Шпанији, на још евидентнији начин је показало да је кибер простор постао ново поље акције организованог криминала. Истраживање је потврдило претпоставку да се организоване криминалне групе брзо прилагођавају новим технологијама, напуштајући физичко застрашивање у корист кибер оружја, попут *botnet*-а и малвера, који се у 70% случајева користе искључиво са циљем стицања противправне користи.[557]

Компромитована рачунарска мрежа (енгл. *botnet*), сачињена од 20 до 30 хиљада заражених рачунара којима управљају „информатички плаћеници“, користи се за нападање и уцењивање привредних корпорација и других комерцијалних организација. Евидентирани су и случајеви давања *botnet*-а у закуп, при чему цена њеног изнајмљивања достиже износ и до 28.000 долара месечно, а тарифа по сату и до 100 долара. Претпоставка је да се, на дневном нивоу, број компромитованих

---

[556] Кина, Велика Британија, Индија, Русија, Пољска, Чешка, Немачка, Шпанија, Италија, Француска, Аргентина, Бразил, Аустралија, Мексико, Јапан и Канада.

[557] Студија Питера Трокслера, истраживача швајцарског Федералног института за технологију из Цириха (Eidgenössische Technische Hochschule – ETH), *Virtual Criminology Report: the first pan-European study into organised crime and the Internet*, доступна је на адреси http://www.mcafee.com

рачунарских мрежа увећава за 25. У истраживању је регистрован и пораст случајева израбљивања *script kiddies*-а, које добро организоване криминалне групе користе као покриће, смањујући на тај начин ризик да буду откривене. У мору разноврсних превара на Интернету, оне везане за берзу постају све уносније за организоване криминалне групе. Начин извршења је релативно једноставан: криминална организација купује акције једне фирме по ниској цени, а затим, служећи се Интернетом, шири лажну информацију о расту цена тих акција и потом их продаје по вишој цени. Истраживање указује на постојање неколико криминалних мрежа ове врсте у свету: „Boca Raton“ на Флориди, „Малага“ у Шпанији и на Девичанским острвима. Позната америчка компанија „Concorde“, уз многе друге, била је жртва ове врсте напада. Њене акције су вештачки порасле након пар лажних обавештења објављених на сајту који се бави берзанским пословима.

Процењује се да ће у будућности доћи до повећања броја деликата који се извршавају познатим техникама (употребом фишинга, малициозних програма, компромитованих мрежа или, пак, изнајмљивањем *botnet*-а), али и до појављивања нових техника и алата за компромитовање технологија које се тек устаљују. Нарочито застрашује чињеница да би легалне комерцијалне организације могле доћи у искушење да се преоријентишу на кибер криминал, с обзиром на лакоћу којом се овај прелаз може извршити у мрежи.

Ефикасно супротстављање кибер криминалу онемогућавају бројне потешкоће. Међу отежавајућим околностима неке се могу истаћи као посебно значајне:

- Тек мали процент деликата у кибер простору пријављује се надлежним органима (око 5%), што због недовољне информисаности, што због страха од губитка репутације (ово је посебно изражено код предузећа која се баве електронском трговином или банака), тако да се не познаје стварна размера феномена.
- Кибер криминал не представља врсту традиционалног криминала, који је уско везан за територију. Овај облик криминалитета карактерише транснационалност, тј. трансцендирање државних граница.
- Просторна раздаљина између криминалца и жртве битна је карактеристика кибер криминала. Просторна прикривеност каузалитета жртва–нападач (места где се налази жртва и оног са којег делује криминалац), отежава откривање учиниоца. У оним случајевима када је

могуће открити његов идентитет праћење и хапшење учиниоца показују се као додатно тешки задаци.

- Транснационални карактер кибер криминала захтева усвајање заједничке, усклађене легислативе на међународном нивоу како би се олакшало деловање националних институција у пољу превенције и репресије.

Конвенција о кибер криминалу (*Convention on Cybecrime*) Савета Европе из 2001. године представља покушај усклађивања правне регулативе на међународном нивоу, са циљем супротстављања овом феномену.[558] У садржинском смислу, унутар Конвенције разрађене су следеће теме: 1) усклађивање националних законодавстава у дефинисању кибер криминала; 2) оснаживање националних процедура и дефинисање неопходних инструмената за истраживање и репресију кибер криминала, повезаних криминалних дела, извршених путем информационих система и оних за која постоје докази електронског облика; 3) стварање брзог и ефикасног система међународне сарадње.

Конвенција предвиђа основна правила која би олакшала спровођење истраге у виртуелном свету, са облицима узајамне помоћи између ауторитета различитих земаља. Ове одредбе подлежу законским условима земаља потписница и морају да гарантују поштовање људских права и примену принципа пропорционалности. Ове процедуре се могу узети у обзир само под дефинисаним условима и са претходним овлашћењем правосудних органа или независних ауторитета.

Под облицима узајамне помоћи Конвенција предвиђа да ауторитети и полицијски службеници једне државе могу бити ангажовани и за потребе друге државе у потрази за електронским доказима. Предвиђена је и мрежа контаката која би била на располагању 24 сата дневно, свим државама потписницама Конвенције, како би се омогућила тренутна помоћ истрагама које су у току. Надлежност над деликтом, у правном слислу, припада оној држави на чијој је територији, броду или другом превозном средству учињен деликт, односно када је извршилац држављанин те земље, осим ако је прекршај у територијалној надлежности друге државе.

---

[558] Конвенција о кибер криминалу потписана је у Будимпешти 23. 11. 2001, а ступила је на снагу јула 2004. У раду Конвенције учествовале су 44 земље чланице Савета Европе, заједно са Канадом, САД, Јапаном и Јужном Африком. Извор: Council of Europe, http://conventions.coe.int

Међутим, активности у пољу међународне сарадње се, према тренутном стању ствари, не чине довољнима. Тек су предузети први кораци у процесу разрешавања овог проблема на међународном нивоу, из којих се не може закључити да ће проблем кибер криминала у догледној будућности бити решен. Кибер криминал тренутно представља озбиљну претњу информационом друштву, а све су назнаке да ни у скоријој будућности ова кибер претња неће бити сведена на прихватљив ниво. Иако нов, овај феномен има потенцијал да виртуелни простор учини посебно ризичним за индивидуалне кориснике. Док комерцијалне организације имају некакве инструменте заштите или их на релативно лак начин могу прибавити и имплементирати, индивидуални корисник је најчешће неедукован у пољу кибер безбедности и, самим тим, практично незаштићен. То га чини изузетно рањивим приликом упражњавања данас врло популарних активности везаних за електронску трговину, електронско банкарство и електронску управу.

4.3.6. Тероризам

Недостатак правила и граница, могућност достизања широког медијског ефекта, брза размена информација и готово апсолутна гаранција анонимности карактеристике су кибер простора које га чине идеалним пољем за прикривене организације и покрете. Кибер простор је за терористичке организације постао једна врста виртуелне оперативне базе коју је немогуће опколити и неутрализовати. Практично су све светске терористичке организације било које политичке или религиозне оријентације показале да имају жељу и способност да искористе карактеристике кибер простора, колико год то звучало парадоксално, у односу на групе које се традиционално сматрају антимодернистичким.

Према подацима Стејт дипартмента, 1998. године 15 од 30 организација које су САД прогласиле терористичким имало је своје *web*-сајтове, а од 2000. године све оне су присутне на светској комуникационој мрежи. Вајман (Weimann) констатује да готово све активне терористичке организације, њих преко четрдесет, имају по један или више Интернет-сајтова, и то, углавном, доступних на неколико језика.[559] Организације из свих делова света заступљене су на Интернету. Ипак, и са́мо присуство на мрежи говори да су многе од њих, како тврди Вајман, не само транснационално, већ и трансрегионално усмерене и профилисане. Овај аутор

[559] Weimann G.: *How Modern Terrorism Uses the Internet*, United States Institute of Peace, Special Report, New York, p. 3, http://www.usip.org/pubs/specialreports/sr116.pdf

класификује терористичке организације присутне на мрежи по једноставном, географском критеријуму поделе:

- Блиски исток: Хамас, Хезболах, ПЛО, Фатах танзим, Палестински исламски џихад, покрет „Кахан живи“, Курдистанска радничка партија, Иранski муџахедини (PMOI), Партија народног демократског ослободилачког фронта и Велики источни фронт исламских одметника (IBDA-C);
- Европа: ЕТА, ИРА и Корзиканска армија;
- Латинска Америка: Тупак амару, Сендеро луминозо (Перу); FARC и Колумбијска национална ослободилачка партија (Колумбија);
- Азија: Ал каида, Хизб-ул муџахедини Кашмира, Ансар ал ислам, Јапанска црвена армија, LTTE, Исламски покрет Узбекистана, Исламски ослободилачки фронт Моро (Филипини), Јапанска супериорна истина (Aum Shinrikyo), Laskhar-e-Taiba (Пакистан) и чеченски побуњенички покрет.

Набројане организације користе Интернет веома активно и имају, углавном, по неколико сајтова које контролишу и уређују.

Табела бр. 11: *Преглед Интернет-адреса појединих терористичких организација*

Хамас	http://www.hamas.org http://www.palestine-info.net/hamas/index.html http://www.qassam.org/ http://www.palestine-info.com/index_e.htm
Хезболах	http://www.Hizbollah.org http://www.moqawama.org http://www.moqawama.tv/ http://www.almanar.com.lb/
Aum Shinrikyo	http://Aum-internet.org/ http://Aum-shinrikyo.com/english/ http://info.aleph.to/index_en.html
Тамилски тигрови	http://www.eelam.com/ http://www.eelamweb.com/
FARC	http://www.contrast.org/mirrors/farc/ingles.htm http://www.farc-ep.org/pagina_ingles/
ИРА	http://www.utexas.edu/students/iig/archive/ira/history/irahist.html. http://www.sinnfein.org/
Курдистанска радничка партија	http://www.pkk.org/
Исламски покрет Узбекистана	http://www.ummah.net/uzbekistan/
Палестински исламски џихад	http://www.jihadislami.com/
Ал каида	http://www.alneda.com http://www.jihadunspun.net http://www.aloswa.org http://www.drasat.com http://www.jehad.net http://www.islammemo.com http://www.qassam.net http://www.assam.com

Извор: Weimann G.: *How Modern Terrorism Uses the Internet*, United States Institute of Peace, Special Report, New York, p. 11, http://www.usip.org/pubs/specialreports/sr116.pdf

И овај сумарни преглед Интернет-страница које служе ширењу терористичке идеологије, сматрамо, довољан је да прикаже њихову распрострањеност на Мрежи и могућности за одашиљање жељених порука у свет. На Мрежи су, дакле, присутне све најзначајније светске терористичке организације, како оне глобалног, трансрегионалног типа, тако и оне са уским, етничко-сепаратистичким или левичарским, револуционарним циљевима. Речју, терористичка идеологија је „преплавила“ Интернет, који је, очигледно, због свих погодности које пружа, постао водеће медијско средство терориста. Поменуте терористичке организације путем мрежних сајтова износе јавне прогласе, претње или врше психолошке притиске на противнике, врбују и индоктринирају нове чланове и одржавају везе са географски удаљеним ћелијама или члановима.

4.3.6.1. Употреба Интернета за терористичку пропаганду и психолошки рат

Пре појаве Интернета су могућности терориста за привлачење пажње широке јавности биле уско повезане са добијањем визибилитета путем традиционалних медија (телевизија, радио, новине итд). Представа коју поменути медији пружају аудиторијуму, међутим, увек има негативну конотацију за терористе. Став јавности према терористичкој активности формира се под утицајем приказаних трагичних слика или информација пуштених у етар, које успут бивају филтриране, промењене или чак цензурисане према избору уредника средстава информисања.[560]

Комуникација путем кибер простора, пак, омогућава слање нецензурисаних информација (чији садржај може бити намењен одређеној циљној групи), без обзира на то да ли је реч о пласирању истинитих или неистинитих информација. Ову погодност користе субверзивне друштвене групе у циљу изграђивања одређеног имиџа у јавности и пред противницима. Са могућностима мултимедијалне комуникације, Интернет функционише у исто време и као радио-станица, телевизија и новине, омогућавајући доступност информација свуда у свету, са незнатним логистичким трошковима и без могућности цензуре од стране националних влада. Није случајност да се, на пример, политичка расправа у Саудијској Арабији и

[560] Putignano D. S.: *La criminalità informatica: cyberterrorismo*, Facoltà di Giurisprudenza, Università degli Studi di Bari, 2002, стр. 63.

земљама Залива, половином деведесетих година прошлог века, постепено преместила са традиционалних медија (који су у овом региону изложени оштрој контроли држава) у кибер простор.[561]

Путем кибер простора терористи у основи теже да допру до три различита аудиторијума:

1) постојећих и потенцијалних бораца и подржавалаца;
2) међународног јавног мњења, које није директно умешано у конфликт и упознато са разлозима терористичких активности, али које може бити заинтересовано за кључна питања конфликта;
3) непријатељске, тј. противничке јавности.

У ове сврхе се првенствено користе web сајтови. Сајтови терористичких организација обично су подељени у секције у којима су представљени разноврсни садржаји: историјат организације, политичко-социјалне идеје и идеолошки и политички циљеви организације, најзначајније иницијативе и спроведене акције, као и биографије лидера организације, оснивачâ и заслужних чланова, тј. „хероја“. Често је у структури сајта присутна и „информативна секција“, у којој се посетиоци могу упознати са актуелним вестима и прочитати политичке коментаре уредника.

Са циљем допирања до широке међународне јавности многи сајтови нуде могућност приказа интегралног текста на више светских језика. Интересантно је поменути да се текстуални садржај на домицилном језику разликује од верзије намењене међународном аудиторијуму по томе што је, у другој верзији, изостављена насилничка реторика из оригиналне верзије. Иако се често употребљавају изрази „оружана борба“ и „отпор“, не емфатизује се и не помињу се насилничке активности организације, иако је доста простора посвећено аргументисању моралне исправности и легалности коришћења насиља.

Властита употреба насилних средстава представљена је као нужност, као једини инструмент који стоји на располагању слабијем у супротстављању моћном и потлачавајућем непријатељу. Но, коришћење насилних средстава од стране непријатеља, дакле, оружани одговор на терористичку активност, дефинише се

[561] Eedle P.: “Al Qaeda takes fight for ’Hearts And Minds’ to the web”, *Jane’s Intelligence Review*, 2002, http://www.freerepublic.com

терминима „масакр“, „убиство“ и „геноцид“. Терористичка организација се описује као константно надзирана, спутавана у својој тежњи да се слободно изрази, док су њени лидери у сталној животној опасности. Чланови организације приказани су као борци за слободу или за Бога (као у случају исламског џихада), принуђени да користе силу да би се одбранили од непријатеља који подјармљује права и понос групе или народа који претендују да заступају.

Ова врста комуникације, која настоји да евоцира слику слабе организације, принуђене на избеглиштво од немерљиво надмоћније силе, смера да представи терористе као жртве и да пребаци одговорност за почињено насиље на противника. Додатно оснаживање овакве поруке постиже се реторичким коришћењем језика ненасиља и наводном расположеношћу за мирно решење сукоба дипломатским средствима. Постоје и изузеци, нарочито у погледу група и организација исламског џихада, које су обично одлучније да убеђивачком реториком утичу на јавност која их фаворизује, али и да непријатељску подвргну притиску.[562]

Последњих година је евидентиран велики пораст броја сајтова којима управљају исламске групе и симпатизери. Тешко је одредити тачан број, али се процењује да их има неколико стотина. Садржаји који су на њима заступљени обухватају теме од информативних до теолошких, уз реторику која промовише идеје „праведног рата“ и „мучеништва“. Сајтови који припадају признатим организацијама направљени су професионално и приказују фундаменталистичку верзију догађаја који се тичу Блиског истока и света уопште. Сајтови садрже чланке и коментаре идеолошких лидера, које прате фотографије западњачких злодела. Поједини сајтови нуде детаљне описе насилних акција, а на почетној страници приказују, видно истакнут, електронски бројач палих бораца („мученика“), погинулих непријатеља, као и колаборациониста. Најчешће се користи арапски језик, мада многи сајтови укључују и секције на енглеском језику, унутар којих се разматрају филозофска и теолошка питања, са циљем преобраћања посетилаца у ислам.

---

[562] Piccitto D.: *Terrorismo: dal fondamentalismo religioso ad Internet*, Facoltà di lettere e filosofia, Facoltà di Scienze Politiche, Università degli Studi di Perugia, 2005, стр. 140.

Можемо констатовати да тероризам, у својој суштини, садржи елементе психолошког рата.[563] Савремени терористи су, за разлику од „традиционалних“, у стању да користе технолошка достигнућа трећег миленијума у циљу успешног вођења својих активности. Интернет, као средство комуникације које је тешко цензурисати и којим се могу ширити мултимедијални садржаји независно од њихове веродостојности, терористи користе као психолошко оружје у кампањама психолошког рата ради увећања властите моћи и ефеката спроведених дејстава.

Међу различитим начинима за спровођење психолошких операција најчешћи су коришћење дезинформација или претњи, ради ширења осећања страха, немоћи или безнађа. Случај ликвидације америчког држављанина Николаса Берга (Nicholas Berg)[564] један је од препознатљивих примера такве праксе. Видео-снимак обезглављивања америчког грађанина прво се појавио у кибер простору, на сајту „Muntada al Ansar“-а, чије је седиште било у Малезији.[565] Пре него што је сајт укинут, снимак погубљења преузела је телевизија „Ал џазира“ и јавно га емитовала. У финалним сценама снимка који носи наслов „*Абу Мусаб ал-Заркави*[566] *приказан док масакрира америчког војника*“ могао се видети један од пет терориста како чита следећи текст: „Мајкама и супругама америчких војника поручујемо да смо понудили да разменимо овог таоца са заробљеницима Abu Ghraib-а[567] и да је Бушова

---

[563] Према дефиницији Министарства одбране САД, психолошки рат (psychological warfare) јесте планирано коришћење пропаганде и осталих психолошких операција са циљем да се утиче на мишљење, емоције, понашање и деловање страних противничких група, у функцији достизања националних циљева.

[564] Америчког бизнисмена Николаса Берга заробила је, и пред видео-камером убила, терористичка група повезана са „Ал каидом“ у Ираку, маја 2004. године. Његово убиство су осудиле многе исламске вође, наводећи да је противно исламу и штетно за муслиманску ситуацију.

[565] Сајт „Muntada al Ansar“-а словио је за центар разврставања порука „Ал каиде“ и осталих исламских терористичких група. Адреса сајта била је: http://www.al-ansar.biz/

[566] Абу Мусаб ал-Заркави (Abu Musab al-Zarqawi, 20. 10. 1966. – 7. 6. 2006.) био је вехабијски милитант, родом из Јордана, командант ирачких герилаца и вођа „Ал каиде“ у Ираку. Заркави је преузео одговорност за низ терористичких напада, укључујући бомбашке нападе на цивиле, као и одрубљивање главе заробљеном америчком таоцу Николасу Бергу. Абу Мусаб ал-Заркави се сматра заслужним за ширење секташког насиља у Ираку, односно коришћење бомбаша-самоубица против шиитских цивила у Ираку у настојању да се изазове одмазда према сунитима, односно грађански рат, и тако потпуно дестабилизује проамеричка влада у Ираку. Ал-Заркави је последњих година стекао репутацију најтраженијег терористе на свету, засенивши чак и Осаму Бин Ладена. Америчка влада је његову главу уценила на 25 милиона долара. Пре тога је у Јордану био у одсуству осуђен на смрт. Према наводима команданта америчких снага у Ираку, Ал-Заркави је погинуо у ваздушном нападу у близини Багдада 2006. године. Према: BBCSerbian.com, http://www.bbc.co.uk/serbian/news/2006/06/060608_zarqawi_gallery.shtml.

[567] Затвор у близини Багдада у којем су ирачки ратни заробљеници подвргавани мучењу и малтретирању од стране америчке војске.

администрација то одбила...“ „Част људи и жена затвора Abu Ghraib не може се наплатити крвљу.“[568]

„Ал каида“ обједињава мултимедијалну пропаганду са напредним комуникационим технологијама ради организовања софистицираног психолошког рата. Без обзира на бројне ударе које је претрпела након 11. септембра 2001. године и растурање њених оперативних база у Авганистану и Далеком истоку, организација је и даље у стању да води импресивну психолошку кампању преко својих сајтова. Са ових сајтова она стално упућује претње новим нападима на америчке циљеве. Велика пажња коју медији посвећују овим претњама доприноси порасту осећања страха и несигурности не само у Америци, већ и широм света.

„Ал каида“ је и уништење Светског трговинског центра пропратила честим слањем порука са својих сајтова и тако проузроковала не само психолошку већ и конкретну штету америчкој економији. У прилог наведеној тврдњи можемо навести чињенице слабљења долара, пада берзанског тржишта и губитка поверења Американаца и света у америчку економију. У једној од порука које су се појавиле на Интернету, Бин Ладен је изјавио: „Америка се повлачи […] мучење њене економије се наставља, али су неопходни даљи ударци. Млади морају да пронађу нове чворове америчке економије и да их погоде.“[569]

Психолошки рат који воде исламске терористичке организације често је усмерен и на одређене групе унутар самог исламског света. На пример, одмах после напада 11. септембра неколицина арапских и египатских радикалних исламиста који су критиковали „Ал каиду“ описани су, на сајту alneda.com, као хипокрити. Реакција терористичке организације била је још жешћа када је једна група од 150 академаца и стручњака из Саудијске Арабије објавила манифест под насловом: „Како можемо коегзистирати“ (*How we can coexist*), у којем је тврдила да ислам и Запад деле одређене универзалне вредности. Путем својих сајтова (alneda.com и drasat.com) „Ал каида“ је одговорила да ислам и Запад не деле ниједну вредност, да не постоји сличност између два света, да је ислам супериоран и да ништа није супериорно у

---

[568] Weimann G.: *Terror Groups Exploit Internet for Communications, Recruiting, Training*, JINSA Policy Forum, http://www.jinsa.org

[569] Bergen P. L.: “Holy War, Inc. Inside the secret world of Osama bin Laden”, *The Free Press*, New York, 2002, p. 253.

односу на њега: „Чак је и муслиман који је роб бољи од милион неверничких џентлмена...“ „Муслимани имају дужност да ислам рашире сабљом.“ Тврдња Манифеста постала је предмет једне фатве,[570] којој је била посвећена посебна секција сајта alneda.com. Притисак који су вршили чланци и фатва био је толико јак да су одређени учесници у писању чланка били приморани да повуку претходне изјаве. Циљ идеолошке кампање је тиме у потпуности постигнут.[571]

4.3.6.2. Мобилисање и обука потенцијалних терориста преко Интернета

Пропагандна активност се, добрим делом, спроводи са циљем привлачења пажње оних који имају заједничке интересе са терористичком организацијом или, пак, сличан систем вредности. Пошто је пропагандом привучена пажња симпатизера, у следећем кораку им се додељују једноставнији задаци (активности) унутар организације, као и неопходни инструменти за почетну обуку, нарочито у околностима када није могуће користити праве кампове за обуку.

Сајтови и форуми користе се за размену информација и контаката приликом пријављивања у јединицу, као и за дистрибуцију видео-снимака који приказују разне фазе обуке и борилачке сцене из актуелних или минулих сукоба. Такође је на сајтовима усвојена и пракса објављивања биографија или интервјуа са познатим муџахединима. Материјал презентован на терористичким сајтовима, осим тога што делује мотивишуће на нове чланове, има циљ да докаже континуитет борбе (као у случају чеченских сепаратистичких напада против руских војних снага) – борба се наставља упркос контролисаним информацијама које пласирају медији противничких држава.

Жене и деца су, често, циљна група у информационим кампањама. Мајкама се сугеришу различити начини на које могу васпитавати своју децу да би их

---

[570] Фатва (арапски: فتـــوى) значи саветовање, које се врши са експертом за исламско право – шарију. То су углавном муфтије. Код шиитâ фатву врше високи чланови верске хијерархије, нпр. ајатоласи. Саветовање може да потврди или оповргне правила која важе у животу појединца (законски стан, наследство) или у вери (канонско право). Фатва спада у подручје теологије и мора се позивати на одређену тачку шеријата. Код суунитâ фатва има знатно мању тежину него код шиитâ – схвата се као мишљење и није пресудна.

[571] Eedle P., *op. cit*.

припремиле за борачку будућност и на тај начин допринеле џихаду.[572] Међу потенцијалним члановима нарочито се траже они који припадају одређеном културном кругу и који имају специфична техничка и научна знања. Није реткост да се, нарочито на високим оперативним нивоима армије џихада, налазе солидни стручњаци, са потврђеним информатичким способностима. Међу протагонистима значајнијих терористичких атентата из деведесетих година налазе се биолози, хемичари, инжењери, физичари и информатички експерти. Доказано је да је Осама Бин Ладен лично регрутовао еминентне специјалисте у подручју медицине, инжењерства, хемије, физике, информатике и телекомуникација.[573]

Основна средства обуке путем Интернета јесу практични приручници са упутствима за израду бомби и експлозива, хемијских реагенаса и отрова, или пак инструкцијама за извршење киднаповања или егзекуције на разне начине. Они сегменти приручника који се односе на кибер простор елаборирају технике шифровања информација и електронских порука ради избегавања пресретања од стране противничких обавештајних служби. На великом броју сајтова могу се пронаћи публикације попут *Терористичког приручника* (*The terrorist's handbook*) и *Кувара за анархисте* (*The anarchist cookbook*), које садрже детаљне инструкције о томе како извести нападе различитим експлозивним средствима. На Мрежи је, такође, могуће набавити такозвану *Енциклопедију џихада*[574] која представља, у исто време, комплетан приручник за терористе и политичко-религиозни манифест „Ал каиде".

---

[572] Scalese A., *op. cit*., p. 64.

[573] Hudson R.: *The sociology and psychology of terrorism: who becomes a terrorist and why?*, http://www.fas.org

[574] Енциклопедија џихада је откривена 1988. године у једном претресу који је извршила манчестерска полиција. Обима је хиљаду страница, подељених у једанаест књига. Енциклопедија, између осталог, садржи детаљна упутства за израду и постављање експлозивних направа, пружање прве помоћи, коришћење свих врста ватреног оружја, начине комуникације унутар разних муџахединских група, принципе и смернице за извођење класичних герилских, али и биотерористичких операција. Међу бројним стратегијама налази се и она за регрутовање младих муџахедина, будућих „спавача", унутар држава које су потенцијалне мете. Спавачи су у стању да изврше напад и након десет година од регрутовања, на циљеве који су изабрани и по симболичком и психолошком значају, као и на основу практичног ефекта који би изазвало њихово уништење. Међу циљевима предложеним у Енциклопедији налазе се: Кип слободе у Њујорку, Ајфелов торањ, нуклеарне централе, аеродроми, луке, небодери-симболи (тринаест година након откривања Енциклопедије обистинио се напад на Куле близнакиње), зоне са високом концентрацијом људи итд.

Још једна онлајн публикација „Ал каиде“ јесте *Сабља* (*Al Battar*). Десето издање, које је изашло у мају 2004. године, било је посвећено отмицама са фокусом на методе, потенцијалне жртве и тактике преговарања, а садржало је чак и упутства за снимање одсецања главе киднапованих и објављивање снимка на Интернету. Ова публикација је објављена нешто пре сезоне отмица и убистава талаца у Ираку.[575] Сматра се да су онлајн приручници посебно добили на значају након уништења талибанских кампова за обуку „Ал каиде“ у Авганистану.

4.3.6.3. Финансирање терористичких организација и међусобна комункација

Као и многе друге политичке организације, терористичке групе користе Интернет за сакупљање новчаних фондова. Најчешће коришћени метод финансирања састоји се од каналисања фондова који произлазе из легалних (донације и привредне активности, на пример) или нелегалних активности (преваре помоћу кредитних картица, трговине дрогом и дијамантима), најчешће уз посредовање легитимних хуманитарних организација.[576]

Донације, осим оних спонтаних, изискују се и од потенцијалних подржавалаца препознатих на основу личних информација унетих у онлајн упитнике и електронске поруџбенице, које терористи са пажњом сакупљају и анализирају. Захтеве за донацију најчешће шаљу електронском поштом признате хуманитарне организације, које немају директне везе са терористима. Еклатантан пример злоупотребе Интернета за сакупљање фондова јесте случај америчке хуманитарне организације „Benevolence International Foundation Inc. – BIF“, са седиштем у Чикагу. Сајт чеченских терориста qoqaz.net (није више активан) током 2000. године позивао је симпатизере да изврше онлајн донације двема хуманитарним организацијама, од којих је једна била BIF. Између јануара и априла 2000. године BIF је прикупила и преместила око 700.000 долара на банковне рачуне повезане са чеченским сепаратистима у Грузији, Азербејџану, Русији и Литванији.[577] Деветнаестог марта

---

[575] Northeast Intelligence Network – Terrorism News, Information and Analysis: Kidnapping & Hostage Taking (from Al Battar, Issue 10), http://www.homelandsecurityus.com

[576] *How is Al Qaeda funded?*, Council on Foreign Relations, http://www.terrorismanswers.org

[577] Islamic Charity Indicted, http://www.cbsnews.com, http://news.findlaw.com

2002. године откривена је и улога ове организације у опремању и обуци терориста у Босни и Херцеговини.[578]

Информационе технологије и Интернет, дакле, омогућавају терористичким групама лако и брзо прикупљање и преусмеравање финансија. Тешкоће које постоје у контроли новчаних токова и непостојање одговарајуће стратегије супротстављања доводи експерте у пољу тероризма до закључка да ће се овај феномен у будућности ширити.

Интернет и, уопште, информационо-комуникационе технологије постале су терористима неопходне и за остваривање и одржавање међусобне комуникације. Изузетно брз проток информација омогућава „раштрканим" члановима терористичких организација готово тренутну комуникацију и координацију. Услуга коришћења глобалне комуникационе мреже јесте, при том, бесплатна, а различитост и количина информација које се њоме могу разменити бесконачне су. Интернет повезује не само чланове једне организације, већ и елементе различитих организација.

Бројни терористички сајтови који промовишу идеју џихада представљају мрежу у Мрежи којом се служе терористи из различитих земаља за размену не само идеја и савета, већ и практичних инструкција за стварање терористичких ћелија и извођење напада. Неке од терористичких организација заступљених у кибер простору имале су изражену улогу у координацији и промоцији „Ал каиде". Према извештају америчког Института за мир (*United States Institute of Peace*), assam.com је био задужен за подручје Авганистана и Палестине, qassam.net је био линкован на „Ал каиду" и на „Хамас", 7hj.7hj.com је подучавао посетиоце како да хакују владине Интернет ресурсе, aloswa.org је објављивао цитате Бин Ладена, док је drasat.com нудио линкове на десетине сајтова који су објављивали саопштења „Ал каиде".[579]

Још један разлог додатно утиче на опредељеност терориста за комуникацију путем Интернета. У односу на традиционалне системе за јавну комуникацију (фиксни, мобилни или сателитски телефон), које је могуће прислушкивати, али и

---

[578] Видети шире у: Трифуновић Д., Стојаковић Г., Врачар М.: *Тероризам и вехабизам*, Филип Вишњић, Београд, 2011, стр. 161-214.

[579] United States Institute of Peace, http://www.usip.org/pubs/specialreports/sr116.html

лоцирати комуниканте, Интернет нуди серију инструмената који, ако се користе на прави начин, гарантују готово апсолутну конспиративност комуникације. У ову сврху користе се различити методи али, за разлику од представа које у јавности стварају мас-медији жељни сензационализма, ретко се користе технолошки софистицирани начини, јер привлаче пажњу безбедносних служби.[580] Управо из тог разлога, најчешће се преферира једноставност традиционалних, али ефикасних начина шифроване комуникације која се обавља разменом електронских порука између чланова исте ћелије.[581]

Порука размењена електронском поштом међу терористима који су 11. септембра отели авионе, како сматрају у америчком Институту за мир, означавала је мете напада. Последња инструкција Мохамеда Ате (Mohammed Atta) пред извршење терористичког акта гласила је: „Семестар почиње за три недеље. Добили смо деветнаест потврда за студирање на факултету права, факултету урбаног планирања, академији ликовних уметности и факултету машинства.“ Касно се увидело да се „деветнаест потврда“ односило на отмичаре, а поменута четири факултета на број циљаних авиона за извршење напада, тј. на четири мете.[582] Ова порука је пример како размена једноставно кодиране информације са јавног места и помоћу електронске поште (отмичари авиона су имали адресе *Hotmail*-а) може послужити сврси.

Један од напреднијих метода који искоришћава мултимедијалну природу Интернета подразумева пласирање скривених порука у на први поглед неважне фајлове који садрже слике, музику или слично, техникама стеганографије.[583]

---

[580] Шифроване поруке које путују према серверу ISP сигурно су сумњивије од наизглед баналног текста обичне поруке који крије другачије значење, познато само примаоцу.

[581] На пример, чланови исте ћелије могу да користе само једно корисничко име и лозинку (тј. један кориснички налог) за приступ серверу електронске поште на web-у (као што су Hotmail, Yahoo или Gmail). На овај начин сваки од чланова може да пренесе поруку осталим члановима и без слања поруке електронске поште – једноставним меморисањем текста у одељак drafts. Будући да ниједна порука није путовала Интернетом, у електронској архиви ISP-а не постоји траг о обављеној комуникацији.

[582] Thomas T.: “Al Qaeda and the Internet: The Danger of ’Cyberplanning‘”, *Parameters*, Vol. 33, 2003.

[583] Термин стеганографија (грч. stéganos + grafeîn = скривено писање), у информатичком контексту, означава технике које се користе за сакривање тајних података у фајлове. Један од најчешће коришћених метода јесте прикривање тајних података у мање важним bit-овима неког фајла (фотографије, аудио- или видео-записа). О овим техникама и могућностима заштите видети више у: Џигурски О.: *Могућности заштите од стеганографије*, Зборник Факултета безбедности, Београд, 2008.

Приступ Интернету се, по правилу, обавља са јавних места (из кафеа, универзитетских мрежа, библиотека и других простора), чиме се постиже додатна гаранција анонимности. Комуникација између врха терористичке организације и ћелија изабраних за акцију може да поприми и облик манифеста објављеног на сајту.

Тако је, на пример, у децембру 2003. године на домену норвешког Интернет-провајдера објављен документ на арапском језику. Проглас, приписан „Ал каиди", под насловом *Џихад у Ираку: наде и опасности*, износио је став да би терористички напади, изведени на територији земаља савезника Америке, њих изложили притиску, те би оне могле да повуку своје трупе из Ирака. Документ је нарочито упућивао на Шпанију, тј. њену унутрашњу предизборну политичку сцену, као најбољу мету. Три месеца касније, 11. марта 2004. године, напади „Ал каиде" на четири воза у Мадриду проузроковали су смрт 191 особе. Ови напади су, на неки начин, условили резултат предстојећих избора. Победила је левица, која је у предизборној кампањи као један од приоритета заговарала повлачење војних снага из Ирака.[584]

Поједине терористичке организације се користе специфичним тактикама комуникације у кибер простору заснованим на мигрирању својих сајтова. Сајт alneda.com, за који се верује да припада „Ал каиди", забрањен је 2002. године пошто су Интернет-провајдери у Малезији и САД открили да служи као огласник „Ал каиде". Ипак, исти садржај се под различитим именима до данас појављује на Интернету, користећи туђе сајтове. Рита Кац (Rita Katz), директор Института за потрагу за међународним терористичким ентитетима (SITE Institute), износи податак да су овакви феномени веома чести: „Није реч само о једном или два сајта, него о стотинама сајтова који су врло битни за 'Ал каидину' комуникацију."[585]

Популарни описни назив за сајт који је кришом „угнежден" на туђи сајт јесте „интернетски паразит". Паразитски сајтови врло динамично мигрирају, мењајући форму. Сајт „Ал каиде", на пример, „васкрсава" чак на дневној бази у форми сајта, дискусионих форума (chat forum[s]), огласа (message board) итд. Метод којим се Alneda инфилтрира у друге сајтове подразумева „разбијање" шифре

---

[584] *Qa'idat al-Jihad, Iraq, and Madrid – The First Tile in the Domino Effect?*, The International Policy Institute for Counter-Terrorism, http://www.ict.org.il/Articles/tabid/66/Articlsid/557/currentpage/15/Default.aspx

[585] SITE Institute, http://www.siteinstitute.org/

администратора и корисника, те коришћење слабости сервера да се заобиђу безбедносне мере.[586]

Стручњаци из америчког института SITE тврде да није реч само о миграцији сајта, него и текстуалних форми онлајн комуникације, као што су дискусионе групе које интензивно мигрирају са једног Интернет-форума на други.[587]

4.3.6.4. Обавештајна активност терориста

Интернет представља неисцрпан извор осетљивих информација, које су често битне за безбедност државе и становништва. У приручнику за обуку „Ал каиде", откривеном у Авганистану, написано је да је коришћењем јавно доступних ресурса, без употребе нелегалних средстава, могуће прикупити барем 80% корисних информација о непријатељу.[588] То доказује да су терористи временом схватили важност такозваних отворених обавештајних извора. Ова врста обавештајне активности заснива се на прикупљању јавно доступних података из новина, часописа, књига, радијских и телевизијских емисија, телефонских именика, Интернета итд. Само путем Интернета терористи имају слободан приступ пројектима, фотографијама, мапама и осталим кључним подацима о потенцијалним циљевима. Често се са фотографија публикованих на Интернету могу добити информације о примењеним мерама заштите на одређеном објекту. На пример, у заплењеном рачунару „Ал каиде" пронађени су подаци „скинути" са Интернета о структурним и инжењерским карактеристикама једне хидроцентрале. Ови подаци су, помоћу програма за тродимензионалну симулацију, веома лако могли да буду употребљени за планирање акције са катастрофалним последицама.[589]

---

[586] Америчко-израелска организација Internet Haganah задужена је да прати кретање сајтова за које се мисли да припадају „Ал каиди" и сличним организацијама. Према њиховим сазнањима, Alneda се током 2003. године појављивала „укопана" унутар сајта једног четрнаестогодишњака, затим сајта компаније за безбедност софтвера, те страницама посвећеним режисеру хорор-филмова Клајву Баркеру (Clive Barker) и холандске фирме за консалтинг Educa. Једна од скоријих локација на којој се налазио сајт била је регистрована у америчкој савезној држави Њу Џерси, (www.conrado.net/_vit_inf/). Линк више није активан, а тренутна локација сајта „Ал каиде" није позната. Према: Internet Haganah, http://internet-haganah.com/haganah

[587] SITE Institute, op. cit.

[588] Интервју Доналда Рамсфелда (Donald Rumsfeld), америчког секретара одбране, од 15. јануара 2003. Извор: Inside Defense, http://www.insidedefense.com

[589] Putignano D. S., *op. cit*., p. 67.

Терористима су у кибер простору на располагању многи инструменти који олакшавају прикупљање релевантних података: Интернет-претраживачи, листе дистрибуираних порука електронске поште, форуми или сајтови намењени вођењу дискусија (chat rooms). Интернет-претраживачи су нарочито погодни за брз и анониман приступ јавним информацијама издатим у дневној и периодичној штампи. Прикупљање исте количине једнако вредних података традиционалним путем, у хемеротекама, било би практично немогуће. Уз одређена информатичка знања и вештине, појединцима и организацијама је омогућен приступ и оним информацијама које спадају у категорију интерних, поверљивих и тајних, дакле поузданих информација.

На размишљање наводи податак да су се планери, приликом припремања напада од 11. септембра, користили искључиво информацијама које су биле јавно доступне у кибер простору. На основу реда вожње, модела авиона (капацитета горива), броја резервисаних путничких места и полне структуре путника терористи су били у стању не само да одаберу летове које ће преусмерити, већ и да осигурају стизање авиона до циља, постигну максимизацију штете, али и да процене интензитет евентуалног отпора путника у авионима.

Према доступним подацима из досадашњих истраживања терористи су, користећи се кибер простором, извршили прикупљање података о следећим потенцијалним циљевима у САД:[590]

- Центру за контролу и превенцију болести у Атланти, који се, између осталог, бави развојем националних одбрамбених стратегија против биолошких напада;
- телематској[591] мрежи националних финансија, која подржава ток банкарских података;
- информационим системима који контролишу рад уређајâ у саставу електричних централа, хидротехничких брана и система за прераду воде;
- телекомуникационој мрежи и телефонском сервису хитне помоћи 911;
- председничким и војним командним положајима и њиховим локацијама.

---

[590] Squitieri T.: *Cyberspace full of targets*, http://www.usatoday.com

[591] Телематика је наука о слању, примању и чувању информација уз помоћ телекомуникационих уређаја.

Информације о свим наведеним објектима и системима биле су, са импресивном количином детаља, доступне на Интернету.

4.3.7. Кибер тероризам

Тероризам је, као вид диверзантске борбе, познат од давнина. Међутим, данас он поприма низ нових обележја. Најновији технолошки развој и измењене политичке, економске и војне прилике у свету довели су до низа стратешких и тактичких новина у терористичком облику ратовања, асиметричном виду рата који постепено замењује класична ратна дејства. И најразвијеније земље света страхују од нових облика испољавања тероризма, али и од нових средстава која би терористи могли у будућности да употребе. Владе многих држава, али и јавност уопште, стрепе од могућности употребе радиоактивног материјала, удара на нуклеарна постројења, крађе или трговине нуклеарним оружјем или плутонијумом за производњу оружја.[592]

Отворено се испољава и стрепња да ће се у овом веку знатно повећати употреба технолошких средстава од стране терориста. Самим тим, безбедносни сценарији новог миленијума уврстили су у своје агенде и ризик од кибер тероризма, новог облика испољавања тероризма, заснованог на употреби информационо-комуникационе технологије као средства за извођење терористичког напада. С обзиром на то да технолошки високоразвијене земље у великој мери зависе, у свим привредним и државним активностима, од осетљивих рачунарских и телекомуникационих система, ови системи су од стране експерата перципирани као могући и терористима интересантни циљеви. Кибер терористички напад може бити изведен једноставним средствима (довољан је рачунар и неки од малициозних кодова), са малим бројем људи, а да при томе нанесе велику штету држави, њеној привреди или становништву. Последице могу бити чак и фаталне уколико се угрозе критичне информационе инфраструктуре, попут система за контролу копненог и ваздушног саобраћаја, хидроцентрала, нуклеарних електрана, безбедносних и здравствених служби, или пак система за дистрибуцију електричне енергије.

---

[592] Милашиновић Р.: „Могућности успостављања мира у свету и превенција конфликата“, *Кризни менаџмент I – превенција кризе*, хрестоматија, Факултет безбедности, Београд, 2006, стр. 92.

Кибер тероризам је у многим западним земљама већ уврштен међу проблеме националне безбедности, иако се у академској јавности још води дискусија о томе да ли је кибер тероризам манифестована или потенцијална претња и, уколико је ова последња, колико је реална.

Спору у великој мери доприноси чињеница да овај феномен за сада није теоријски довољно дефинисан. Додатну тешкоћу представља и околност да је анализа претње кибер тероризма везана за јавно доступне информације из такозваних отворених извора, јер се готово ништа не зна о истраживањима националних и наднационалних обавештајних агенција, нарочито када се говори о намерама, мотивацијама и способностима непријатеља. Однос медија према феномену кибер тероризма, такође, увећава збрку – различити видови криминалних активности у кибер простору често се, иако неоправдано, називају кибер тероризмом. Узроци овоме вероватно леже делом у неразумевању проблема, а делом у чињеници да сензационалистички тон и мистификација доприносе повећању тиража. Реторичка драматизација, која се у медијима често користи, оставља у јавности утисак да проблем постаје све присутнији.

Различитост погледа на кибер тероризам има порекло у различитим поимањима фундаменталних питања везаних за овај феномен. Плуралитет теоријских елаборација произлази из бројних несугласица о основним питањима: адекватне дефиниције кибер тероризма, опасности у погледу последица, потенцијалне користи коју остварују терористи, и ефеката кибер терористичког напада.

Дивергентни приступи су, ипак, сагласни у перцепцији да неки облик опасности од кибер тероризма постоји, иако се не слажу у томе колики је степен саме опасности. Становишта су сагласна и у погледу атрактивности потенцијалних мета, које обухватају широк дијапазон корисника глобалне рачунарске мреже.

Поменути недостатак сагласности међу стручњацима доводи у питање и оправданост подвођења ове претње под један од аспеката кибер ратовања. Класификација претње кибер тероризма биће могућа тек када се поменути спор реши, тј. када теоријски корпус безбедносних наука у овој области буде у одређеној мери употпуњен. Да би се начинио први корак у том правцу, потребно је поћи од основног проблема – непостојања сагласности по питању дефиниције појма *кибер тероризам*.

4.3.7.1. Појмовно одређење кибер тероризма

Тероризам представља комплексан феномен, до чије се општеприхваћене дефиниције још није дошло ни на међународом нивоу, услед мноштва потенцијалних актера и различитих криминалних активности којима се они могу служити за остваривање циљева.

У савременој литератури чињени су покушаји да се класификују све познатије дефиниције тероризма. Тако су, рецимо, Шмит (Schmidt) и Џонгман (Jongman) анализирали 109 дефиниција тероризма и идентификовали 22 елемента који се најчешће помињу у овим дефиницијама.[593] За разлику од поменутих аутора, који су мерили учесталост понављања одређених термина у разноликим дефиницијама тероризма, покушавајући да пронађу заједнички скуп елемената, неки други аутори су издвојили неколико, према њима, кључних елемената за дефинисање тероризма. Џесика Стерн сматра да су суштински елементи појма тероризма „усмереност на цивилна лица и намерно изазивање страха међу становништвом или другом циљном групом“.[594] Касезе (Cassese), слично томе, издваја три елемента за дефинисање појма међународног тероризма: инкриминисаност дела којим је терористички акт почињен, употреба силе или претња употребом силе да би се изазвао страх код одређене циљне групе и политичка, верска или друга идеолошка мотивација која превазилази приватне циљеве једне особе или више њих.[595]

Шо (Shaw) предлаже једноставну дефиницију тероризма: „употреба терора да би се постигао неки политички циљ“.[596] Ово је, ипак, чини се, сувише сумарна

---

[593] Ти елементи су: употреба насиља; политичко насиље; изазивање страха или ужаса, претња, психолошки ефект и очекиване реакције; разликовање жртве и шире мете напада; циљано, планирано и организовано деловање, метод борбе, стратегија, тактика; кршење прихваћених правила; одсуство хуманитарних разлога; уцена, принуда и навођење на послушност; жеља за публицитетом; самовоља, безличност, насумичност, одсуство дискриминације; жртве цивили, неборци, лица без везе са самом ствари; застрашивање; невиност жртава; извршилац, група, покрет или организација; симболичка природа; непредвидљивост појаве насиља; тајност и прикривеност, понављање кампања насиља; криминални, злочиначки карактер; захтеви постављени трећим странама. Schmidt A., Jongman A.: *Political Terrorism*, North Holland Publishing Co., Amsterdam, 1988, pp. 5–6.

[594] Стерн Џ.: *Екстремни терористи*, Alexandria press, Београд, 2004, стр. 8.

[595] Cassese A.: *International Law*, Oxford University Press, New York, 2005, p. 450.

[596] Shaw M.: *International Law*, Cambridge University Press, Cambridge, 2004, pp. 1048–1053.

одредница за један тако компликован феномен. Димитријевић издваја четири кључна елемента терористичког феномена: „Терористички акти су по правилу насилни; они су политички мотивисани; потенцијалне жртве ових аката најчешће немају никакве везе са политиком; коначно, циљ оваквих дела је да изазову осећање страха и несигурности.“[597]

Генерална скупштина УН је 1994. године донела резолуцију у којој је дата дефиниција тероризма у модерном смислу.[598] Ова резолуција дефинише тероризам као „кривично дело замишљено или срачунато на побуђивање стања страха у јавности, међу групом људи или код одређених особа, са политичким циљем, које се не може оправдати политичком, филозофском, расном, етничком, религиозном или било којом другом природом на коју се може позвати“. Иста дефиниција је поновљена и у резолуцији 51/120 из 1996. године. Ова дефиниција тероризма, иако нема правно обавезујући карактер, представља прву институционалну дефиницију тероризма дату у оквиру УН.

У периоду од 2000. до 2006. године донето је чак 28 резолуција УН о тероризму. Већ овај податак илуструје тврдњу о томе да тероризам тек у овом периоду постаје својеврстан центар пажње светске јавности и глобални феномен. У оквиру Савета безбедности основани су комитети са циљем рада на спречавању терористичких активности. За поједине активности везане за сузбијање и превенцију тероризма ангажоване су специјализоване агенције и друга тела УН, попут Међународног монетарног фонда и Светске банке, који су задужени за пружање помоћи у спречавању финансирања тероризма и прања новца стеченог организованим криминалом, или Међународне агенције за атомску енергију, која учествује у процесу спречавања наоружавања терориста.[599]

Евидентно је, дакле, да се последњих деценија доживљај тероризма у међународној заједници значајно мењао. Тероризам је постао предмет интересовања

---

[597] Димитријевић В., Стојановић Р., *Међународни односи*, Службени лист СРЈ, Београд, 1996, стр. 340–341.

[598] *Measures to eliminate international terrorism*, UN Document A/RES/49/60, http://www.un.org/documents/ga/res/49/a49r060.htm

[599] Према: Милошевић М.: *Социјални и психолошки фактори криминалне мотивације терористa*, Универзитет у Београду – Факултет безбедности, Београд, 2009, стр. 18.

УН после терористичке акције на Олимпијским играма у Минхену 1972. године; обрт у приступу овом феномену започео је деведесетих, а дефинитивно је уследио после септембарских догађаја у САД 2001. године, када, према многим ауторима, започиње ера „постмодерног тероризма“.[600] У почетку је у УН превладавало мишљење да пре свега треба радити на сузбијању државног и међународног тероризма, али је временом пажња светске заједнице преусмерена на акте које изводе терористичке групе. Ово становиште је последњих година у потпуности однело превагу. Ипак, ово не значи да је у међународној јавности постигнут консензус око поимања тероризма. Несугласице између различитих региона и држава и даље су изражене, чак и у већој мери него раније. Другим речима, иако се тероризам углавном осуђује као злочин, још не постоји заједнички став о питањима шта је то тероризам и ко се може сматрати терористом.[601]

С обзиром на пажњу која се у светској јавности, националним и међународним институцијама придаје проблему превенције и сузбијања овог облика криминалитета, изненађујуће је да у релевантној научној литератури не постоји довољан степен сагласности око елемената појма тероризма. Такође, приступи дефинисању овог појма различити су и узимају у обзир само поједине аспекте ове појаве – социјалне, политиколошке, правне или безбедносне.

Тероризам је, свакако, феномен који се може изучавати са више аспеката. Два елемента су, међутим, заступљена у највећем броју дефиниција тероризма: политичност феномена и систематско посезање за организованим насиљем. Тероризам је, дакле, на првоме месту политички чин, на основу којег је увек могуће препознати мотивацију идеолошке природе. Крајњи политички циљ је есенцијалан, с обиром на то да нам омогућава да раздвојимо терористички акт од других кривичних дела са сличним ефектима. Тероризам карактерише и тежња ка изазивању стања панике и дисфункције друштвеног система.

Коришћење насилних техника за извршење напада, наравно, није типично само за тероризам, али унутар њега оне попримају посебну конотацију. За терористе

---

[600] Ganor B.: *The Counter Terrorism Puzzle*, Interdisciplinary Center of Herzlia and Transaction Publishers, Herzlia, 2005, pp. 15–17; Hoffman B.: “Modern Terrorism Trends – Reevaluation After 9/11”, y: Ganor & Boaz (eds.), *Post Modern Terrorism*, Interdisciplinary Center of Herzlia, Herzlia, 2005, pp. 35–43.

[601] О појмовном одређењу тероризма видети шире у: Милошевић М., *op. cit*.

насилне технике имају готово увек симболички карактер. Оне се користе ради шокирања јавности и постизања конкретних циљева. Одатле, можемо констатовати, штампа и средства јавног информисања имају за терористе велику важност. Они су неопходни за ширење панике и страха међу становништвом, тј. за повећање ефекта извршених терористичких (зло)дела. У том смислу не чини нам се погрешном тежња појединих аутора да дефиницију тероризма прошире на више основних елемента, међу којима би се оправдано могао наћи и „утицај на широки аудиторијум".

Националне легислативе, у широким цртама, прате општија теоријска одређења тероризма. Проблематика дефинисања терористе, терористичког акта и терористичког циља у националном законодавству не представља посебан проблем, с обзиром на то да се за параметре узимају појединци, групе и организације који у одређеном историјском тренутку упућују јасну претњу против конкретне државе.[602]

Једна од потпунијих дефиниција тероризма формулисана је у САД, и гласи: „Тероризам је политички мотивисано умишљајно насиље против не-бораца које спроводе субнационалне групе и актери, обично усмерено да утиче на јавност."[603] Као што се може видети, ова дефиниција обухвата све напред поменуте суштинске елементе феномена.

Британски *Terrorism Act 2000*, пак, третира тему на шири и систематичнији начин. Он дефинише тероризам као „акцију или претњу акцијом која има циљ да утиче на владу или да застраши становништво или један његов део", у случају да је „акција или претња акцијом предузета из политичких, религиозних или идеолошких побуда". Терористички чин мора да подразумева „изазивање тешког насиља над особом" или „тешко оштећење имовине" или „да стави у опасност живот особе, под којом се не подразумева извршилац насиља" или „да створи озбиљан ризик за здравље и безбедност становништва или једног његовог дела", тј. да акција буде „испрограмирана тако да тешко наруши или прекине функционисање неког електронског система".[604] Могућност коју предвиђа *Terrorism Act 2000*, да се један терористички чин може концентрисати на ометање или прекид електронског

---

[602] Милошевић М., *op. cit*., стр. 20.

[603] Наведено у одељку 140(d)(2) Foreign Relations Authorization Act, Fiscal Years 1988 and 1989 (22 U.S.C., § 2656f(d)(2)), http://www.state.gov

[604] Дефиниције преузете из: *UK Terrorism act 2000*, http://www.opsi.gov.uk

система, јасно указује, у законодавном подручју, на страх везан за нову врсту и нове начине испољавања тероризма – кибер тероризам.

Једну од најопштијих дефиниција кибер тероризма понудила је Дороти Денинг. Ова ауторка одређује кибер тероризам као сваку терористичку активност у сфери кибер простора. Појам кибер тероризма, према овој дефиницији, означава „нападе или претње нападом против рачунара, мрежа или информација које се у њима чувају, ради застрашивања и приморавања влада и друштава на извршавање политичких, религијских или идеолошких захтева“.[605] Осим тога, да би се квалификовао као кибер тероризам, напад „мора садржати насиље против лица или добара, или барем изазвати довољно штете да створи страх. Напади који проузрокују смрт или физичке озледе, експлозије или тешке економске губитке могу бити примери кибер тероризма. Тежак напад против критичних информационих инфраструктура може се сматрати актом кибер тероризма у односу на величину његових последица.“[606] Супротно, „напади који угрожавају сервис који није од виталне важности представљају ‘скупу сметњу’, али их не би требало сматрати манифестацијом кибер тероризма“.[607]

Према дефиницији Центра за истраживање компјутерског криминалитета (Computer Crime Research Center), која полази од намера нападача, кибер тероризам је дефинисан као „било каква намерна употреба информационе технологије од стране терористичких група и њихових извршилаца са циљем да изазове штету“.[608] Друга дефиниција, за разлику од претходне, сматра кибер терористичким актом, једноставно, употребу кибер простора од стране терористе, чак и када није директно извршена са циљем да створи евидентну физичку штету: „пример кибер терористичке активности може бити и коришћење информационе технологије за организацију и извршење напада, поспешивање активности група и спровођење психолошких операција“.[609]

---

[605] Denning D.: *Is Cyber Terror Next?*, http://www.ssrc.org/sept11/essays/denning.htm, 2001.
[606] *Ibid*.
[607] *Ibid*.
[608] Krasavin S.: *What is Cyberterrorism?*, Computer Crime Research Center, http://www.crime-research.org
[609] *Ibid*.

Ако се проблему приступи са позиције анализе ефеката напада, неки аналитичари сматрају да се под кибер тероризам може сврстати и конвенционални физички напад који уништава информатизоване чворове критичних инфраструктура, попут Интернета, телекомуникација или мрежа за дистрибуцију електричне енергије.[610]

Према операционалној дефиницији FBI, кибер тероризам представља „напад са умишљајем, политички мотивисан, против информација, информационих система, програма и података, извршен од субнационалних група и извршилаца, који се претвара у насиље против не-бораца".[611] Занимљиво је да ова дефиниција ни на који начин не обухвата имовину или добра (сем рачунарâ и/или информација) или могућност да кибер тероризам буде коришћен као инструмент притиска против влада и друштава.

Међу многим одређењима кибер тероризма која би се могла цитирати посебно је интересантна Вилсонова (Wilson) дефиниција, јер концепт намере или ефекте терористичког акта обједињава са претходно изнетим ставовима. Према његовој дефиницији, кибер тероризам је „коришћење рачунара, као оружја и као циља, од стране група, интернационалних или субнационалних извршилаца или извршилаца са политичком мотивацијом, који прете насиљем или чине насиље и узрокују страх са циљем утицања на јавност или наметања промене политике одређеној влади."[612]

Бројност дефиниција, само у једној земљи, јасно указује на потешкоћу да се феномен разјасни на теоријском нивоу, што свакако има импликације и на његово „препознавање" у пракси. С једне стране, немогућност да се са сигурношћу одреде идентитет, намере и политичке мотивације нападача чини изузетно тешком квалификацију кибер тероризма као информатичког напада или напада на информационе инфраструктуре. Са друге стране, потребно је из мноштва различитих

---

610 Verton D.: *A Definition of Cyber-terrorism*, http://www.computerworld.com

611 Pollitt M.: "Cyberterrorism Fact or Fancy?", Proceedings of the 20th National Information Systems Security Conference, 1997, pp. 285–289.

612 Wilson C.: *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service – The Library of Congress, http://fpc.state.gov

дефиниција, понуђених у доступној литератури, издвојити фундаменталне атрибуте овог феномена.

Анализе и студије које су до сада спроведене свакако су обимно документовале потенцијалну рањивост критичних информационих инфраструктура, али су често претеривале са алармантним тоном када је реч о претњама везаним за те рањивости.[613] И нарочито, недостајала им је дубља анализа способности и неопходних ресурса не-државних актера за започињање кибер терористичке активности и ефективне исплативости у смислу користи и ризика. Један од изузетака је извештај објављен 1999. године од стране Центра за изучавање тероризма и неконвенционалног ратовања (Center for the Study of Terrorism and Irregular Warfare) у Калифорнији, под насловом *Кибер терор: перспективе и импликације*.[614] Овај извештај је до данас остао једна од поузданих и најдетаљнијих студија о овом питању. За разлику од претходних анализа рађених у оквиру Центра, последња посвећује нарочиту пажњу мотивацијама, организационим предусловима и техничким баријерама које треба премостити да би се извео напад против кибер инфраструктуре.

Према овој студији, кибер тероризам представља исто што и тероризам, и значи „коришћење информације као оружја, метода и циља напада за постизање терористичких циљева“. Даље, посебно се потцртава тврдња да се са́мо коришћење кибер простора и, уопштено, информационих технологија за подршку терористичким активностима не може сматрати кибер тероризмом. Комуницирање путем електронске поште у фази организације напада, навигација Мрежом у потрази за информацијама о могућим циљевима итд. не представљају, дакле, кибер терористички чин. Кибер терористички акт може бити самосталан, то јест одвојена врста акције или пратећи акт традиционалног тероризма, са циљем повећања његовог ефекта.[615]

---

[613] “Digital Pearl Harbor”, “Electronic Waterloo”, “Cyber Doom” само су неки од назива који се користе за описивање кибер тероризма или, уопште, кибер претње.

[614] Nelson B., Choi R., Iacobucci M. et al.: *Cyberterror: Prospects and Implications*, Center for the Study of Terrorism and Irregular Warfare, Monterey, 1999.

[615] Након напада 11. септембра 2001. формулисан је сценарио о кибер нападу који би, паралелно са физичким нападом, онемогућио функционисање телефонских бројева за хитне интервенције – у циљу увећања психолошког ефекта.

Иако било који акт кибер тероризма најчешће резултује делимичним или потпуним компромитовањем информације у односу на њене аспекте (приватност, интегритет и расположивост), не важи обратно. Другим речима, нарушавање безбедности помоћу информационих система или нападом на информационе системе, уколико се спроводи за не-терористичке циљеве не може се сматрати кибер тероризмом. Уколико пођемо од премисе да тероризам представља обједињење насилне, криминалне и политичке активности, можемо извести закључак да је управо политичка природа тероризма та која га чини различитим од криминалних активности мотивисаних економском зарадом или личним анимозитетом. По аналогији са претходно реченим, информатички напад или напад против информационог система, да би се сматрао кибер тероризмом, првенствено мора спадати у категорију тероризма. Ова спецификација, наизглед банална, неопходна је за разликовање кибер тероризма од кибер криминала, две појаве које се врло често мешају.

Озбиљност претње кибер тероризма може се просуђивати са два аспекта: 1) мотивисаности и оспособљености терористе за извршење напада и 2) рањивости мете, односно величине потенцијалне штете.[616]

4.3.7.2. Мотивациони фактори

Разлози који утичу на појединце или групе да се определе за тероризам као средство за остваривање циљева јесу бројни и разноврсни. Вероватно постоји онолико мотивација за тероризам колико и његових дефиниција. У претходном поглављу смо назначили да су уобичајени мотиви терористе политичке, идеолошке или религијске природе. Од ових, политичка мотивисаност је најизраженија, будући да се појављује у највећем броју дефиниција. Уколико прихватимо став да је кибер тероризам конвергенција тероризма и кибер простора, онда би исти они покретачки принципи који се везују за традиционални тероризам морали важити и за кибер тероризам.

---

[616] Denning D.: *Cyberterrorism – Testimony before the Special Oversight Panel on Terrorism*, Committee on Armed Services, US House of Representatives, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Анализа Центра за изучавање тероризма и неконвенционалног ратовања идентификује четири детерминишућа фактора за мотиве због којих се терористичка група може определити за стратегију кибер тероризма:[617]

- Глобална умреженост повећава број циљева који се могу достићи путем кибер простора.
- Зависност развијеног друштва од информационих технологија, са једне стране, доноси нове рањивости, а, са друге, максимизује могуће ефекте кибер терористичких акција.
- Недовољна сарадња на међународном нивоу и неусклађеност националних законика у пољу кибер криминала дају потенцијалним агресорима имунитет. У случајевима када је могућа идентификација извршилаца остаје отворено питање надлежности над деликтом – да ли је надлежна држава из које је напад извршен или држава у којој су се последице напада испољиле.
- Издаци за припрему и извршење кибер терористичког напада, у односу на остале стратегије, знатно су нижи.

Виртуелни простор очигледно пружа својеврсне предности у односу на физички простор. На првоме месту, он „постмодерним терористима“ омогућава извођење прикривених операција са удаљених локација. Лишава их потребе за коришћењем кинетичког, нуклеарног, биолошког и хемијског наоружања. Ослобађа их ризика који су везани за процес прибављања овог наоружања, као и ризика од неуспеха конвенционалних напада. Такође, кибер терористички напади могу постићи исто толико публицитета као и физички напади.[618] Када се говори о ексцитирајућим факторима, важно је указати и на чињеницу да је кибер простор „малим играчима“ дао моћ да стварају велике поремећаје, помоћу шароликог арсенала малициозних програма. Другим речима, мале, али технички и технолошки

[617] Nelson B., Choi R., Iacobucci M. et al.: *Cyberterror: Prospects and Implications*, Center for the Study of Terrorism and Irregular Warfare, Monterey, 1999.

[618] Denning D.: *Cyberterrorism – Testimony before the Special Oversight Panel on Terrorism*, Committee on Armed Services, US House of Representatives, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

оспособљене терористичке групе могу допрети до светске сцене и створити поремећај и деструкцију великих размера.[619]

Са друге стране, требало би споменути и инхибишуће факторе. Анализа Центра за изучавање тероризма и неконвенционалног ратовања износи аргументе који терористе могу одвратити од стратегије кибер тероризма:

- Терористи на располагању имају многе стратешке опције. Гледано из те перспективе, корисност кибер тероризма могла би бити маргинална.
- Кибер напади могу да изазову прекиде појединих сервиса, али немају могућност да изазову деструкцију на ширем, светском нивоу.[620]
- Основне последице кибер напада могу бити финансијски губици, губици поверљивих или приватних информација, губици репутације и поверења, али у највећем броју случајева последице напада не угрожавају људски живот. Наравно, може се замислити сценарио у којем општи прекид виталних сервиса индиректно доводи до људских жртава. Међутим, и у том случају остаје отворено питање у којој је мери физичко и психолошко оштећење изазвано нападима кибер тероризма упоредиво са ефектима традиционалних терористичких метода.
- Нарастајућа свест о рањивости кибер инфраструктуре наводи кориснике информационо-комуникационих технологија да континуирано побољшавају властите системе одбране. То значи да ће приправност потенцијалне жртве на нападе и њена оспособљеност да се брани у будућности изискивати и веће издатке за агресора.
- Ефекти кибер терористичког напада тешко су предвидиви, не само у погледу физичке штете већ и према његовом утицају на јавно мњење. Идеја да се може извршити притисак на противника само претњом прекида сервиса делује, барем у већини замисливих сценарија, неозбиљно. Прекид услуга се чини као неадекватна алтернатива деструкцији. С обзиром на такве околности, терористичке оганизације, нарочито оне са ограниченим ресурсима у смислу знања и финансија, вероватно не би одабрале стратегију кибер тероризма.

---

[619] *Cyber Threats and Information Security: Meeting the 21st Century Challenge*, A report for the CSIS Homeland Defense Project, Washington D.C.: Center for Strategic and International Studies, 2001, http://www.csis.org/component/option,com_csis_experts/task,view/id,154/

[620] Кибер напади се често сврставају у такозвано оружје за стварање масовних поремећаја (*енгл*. mass disruption weapon), за разлику од оружја за масовно уништење (*енгл*. weapons of mass destruction – WMD), које се везује за традиционални тероризам.

Анализа мотивационих фактора не би требало да пренебрегава техничко-технолошки аспект проблема. Посматрано из ове перспективе, може се констатовати да постоје додатни дестимулишући фактори за примену кибер терористичке стратегије. Наиме, извођење напада у кибер простору није, у технолошком смислу, нимало једноставно. Чињеница да су напади техничког типа, у последњих неколико година, попримили епидемијске размере говори о томе да је ова техника измакла контроли. Поучени тим искуством, смемо се запитати да ли би кибер терористи могли да контролишу процес напада и да одрже штету на одређеном, предвиђеном нивоу.

Осим тога, кибер напади, у односу на физичке нападе, имају мање „разумевања“ за каприце терористичких вођа, јер су везани за временска ограничења – захтевају дуг временски период за спровођење припремне фазе која обухвата активности на истраживању мреже и освајању (не)ауторизованог приступа. По свој прилици, још је, у логистичком смислу, једноставније уништити зграду експлозивном направом, него запосести све противничке рачунаре техником DoS или неким другим нападом техничког типа. Ово би могли бити разлози зашто је, до сада, било толико мало збивања на кибер терористичком фронту.

4.3.7.3. Организациона структура и техничко-технолошка оспособљеност терориста

Природа кибер амбијента пружа кибер терористима могућност диференцирања од типичних терориста. Постојање различитих врста кибер напада и техника за њихово извршење указује и на плуралитет могућих организационих форми кибер терориста. У теоријским елаборацијама посвећеним феномену кибер тероризма најчешће се разматрају четири могуће организационе форме терориста у кибер простору.

На првоме месту, говори се о индивидуалним кибер терористима. Многе од познатих вируса раширених у кибер простору створили су појединци. Индивидуе који стварају малициозне програме најчешће то чине због авантуре и интелектуалног

изазова, а не у сврху изазивања физичког насиља.[621] Међутим, сувисло је претпоставити да може доћи до споја хакерских способности и психопатолошких црта у једној личности. Код деструктивно настројених појединаца изражена је патолошка жеља за изазивањем смрти, материјалне штете и страха међу становништвом.[622] Спој знања и патологије, метафорички говорећи, произвео би соло кибер терористу. Профил индивидуалног кибер терористе одговарао би, дакле, психолошком профилу терористе попут Меквеја,[623] с тим што би подразумевао и поседовање информатичког знања. Претња индивидуалним кибер терористичким нападом не може се оценити као изузетно висока, будући да недостаје емпиријска евиденција која би је поткрепила, али, опет, не и неостварива.

Теоријска размарања проблема кибер тероризма посебну пажњу придају формацијама малих терористичких група састављених од технички добро обучених чланова. Здруживањем у групе, удруживањем знања и способности екстремисти би били у стању да спроводе добро координиране кибер терористичке операције. Такве групе се могу сматрати озбиљнијом претњом у односу на индивидуалне кибер терористе, јер су доказале своје капацитете за извођење криминалних акција.[624] Оспособљеност малих терористичких група за самостално развијање софтверских апликација изазива у безбедносним круговима страх да би ове група могле прећи на деструктивније циљеве.

Велике терористичке организације попут „Ал каиде“, са документованим историјатом физичке агресивности, представљају трећу категорију потенцијалних актера на кибер терористичком колосеку. Као што смо раније показали, већина њих је присутна у кибер простору, где спроводи разноврсне активности.[625] Резултати

---

[621] Denning D.*: Information Warfare and Security*, Addison-Wesley, 1999.

[622] У скорашњој историји САД такви су били, на пример, терористи „усамљеници“: Казински, Меквеј и Џон Мухамед. Реч је о појединцима који су изводили терористичке нападе на територији САД у последњој деценији XX века и почетком XXI века.

[623] Меквеј (Timothy James McVeigh, 23. 6. 1968. – 11. 6. 2001), амерички држављанин проглашен кривим за једанаест федералних кривичних дела, те погубљен због изазивања бомбашког напада у граду Оклахоми 1995. године. Бомбашки напад, који је резултовао смрћу 168 људи, сматра се најгорим случајем домаћег тероризма у историји САД, као и најгорим терористичким чином у америчкој историји све до напада 11. септембра 2001. на Светски трговински центар у Њујорку. Према: http://www.clarkprosecutor.org/html/death/US/mcveigh717.htm

[624] Видети одељак „Инсајдери као фактор угрожавања безбедности пословања“.

[625] Видети одељак „Тероризам“.

истраживања, спроведеног у оквиру Америчког војног универзитета, показали су да је кибер терористичка претња „Ал каиде“ усмерена против Обавештајне агенције Министарства одбране (Defense Intelligence Agency – DIA). Спроведена процена ризика узела је у обзир следеће индикаторе: постојање намере, способности актера, историјске чињенице и потенцијалне мете, и закључила да организација „Ал каида“ представља веома озбиљну кибер претњу за САД.[626] Ипак, овој анализи се може упутити озбиљан приговор – „Ал каида“ до сада није у пракси доказала кибер способности, осим тога што се Осама бин Ладен разметљиво хвалисао „муслиманским научницима“ у својим редовима. Иако се могућност кибер напада не може искључити, чини се да је кибер претња „Ал каиде“ и других терористичких организација изражена скоро у истој мери као и у претходном случају. Судећи по до сада коришћеној несофистицираној технологији, сва је прилика да ће религиозно-фундаменталистичке групе наставити да се придржавају традиционалних метода.

У последњу категорију можемо сврстати групе које су спонзорисане или подржаване од стране влада за вођење информационог рата против непријатељских држава. Између ових група се може правити разлика на основу њиховог порекла и оспособљености. Поједине државе формирају, на званичном нивоу, јединице за кибер ратовање, са циљем извршавања офанзивних и дефанзивних задатака.[627] Прецизно говорећи, њих не би требало сврставати у категорију кибер терористичких група, али су оне на скали степеновања потенцијалне штете изузетно сличне. Може се констатовати да, у тренутним околностима, активности ових војних јединица имплицитно бивају спутаване публицитетом који доносе учестале међународне расправе о овом феномену. Захваљујући томе се не спроводе напади на противничке системе, барем не јавно.

Амерички годишњи извештај о војној снази Народне Републике Кине из 2003. године[628] евидентира у кибер простору и присуство хакера мотивисаних националистичким идеологијама, такозваних хактивиста, који творе други,

---

[626] Ashley B.: *Anatomy of Cyberterrorism: Is America Vulnerable?*, Research Paper, Air War College, Air University, Maxwell AFB, 2003.

[627] Видети одељак „Војни аспект кибер ратовања“.

[628] *Annual Report On The Military Power Of The People's Republic Of China*, IWS – The Information Warfare Site, http://www.iwar.org.uk/iwar/resources/news/china-io-2003.htm

неофицијални, организациони ниво.[629] Ове самопроглашене патриоте узимају на себе одговорност за нападе на информационе системе земаља са којима су у конфликту. Пратећи хронологију међународних инцидената, може се закључити да су, осим Кинезâ, хактивизму веома склони и Руси, Тајванци, Израелци, Индијци, Пакистанци, Американци, али и Срби.[630] Најчешће су хактивистичке активности инкриминисане националним законодавствима, али у пракси матичне државе не санкционишу овај вид активности докле год оне не почну да прелазе линију „националног интереса“.[631]

Оспособљеност терористичких група за извођење кибер напада јесте један од најважнијих параметара за процену кибер терористичке претње. Претходно поменута студија Центра за изучавање тероризма и неконвенционалног ратовања дефинише три нивоа оспособљености терориста:

- Једноставан – неструктурисан ниво. Групу на овом нивоу карактеришу базичне способности за спровођење аката хакинга против појединачних система и коришћење већ постојећих кибер инструмената.
- Напредни – структурисан ниво. Организација на овом нивоу има способност да изведе софистициране нападе против више мрежа или система и да промени или створи једноставне инструменте за извршење напада. Квалификују је и елементарне способности за анализу циљева, команду, контролу и обучавање.
- Комплексан – координиран ниво. Предвиђа способност координације напада који могу изазвати генералне прекиде сервиса чак и добро заштићених система. Организација је на овом нивоу оспособљености у стању да створи софистициране инструменте напада и поседује комплетну способност анализе циљева, команде, контроле и обучавања. Време које је потребно једној организацији да достигне комплексно координирани ниво Центар процењује на шест или десет година. Међу терористичким групама које су анализиране (религиозне, *new age*, етно-националисти, сепаратисти, револуционари и екстремна десница) сматра се да само религиозне (нарочито исламски фундаменталисти) могу да остваре максималан ниво оспособљености, с обзиром на околност да је то у складу са њима својственом применом насиља.

---

[629] Видети одељак „Хактивисти“.

[630] Dunnigan J., *op. cit*.

[631] Devost M.: “Hackers as a National Resource”, у: *Information Warfare – Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, Winn Schwartau (Ed.), Thunder’s Mouth Press, New York, 1996.

Најозбиљнију претњу кибер тероризма представљали би они напади чији актери не би могли да буду откривени. Нападачима који су лако уочљиви недостаје софицираност или организованост за спровођење координираног напада. Озбиљнији напади у кибер простору увек су камуфлирани на одговарајући начин, комплексни и изведени од стране нападача који су расподељени у групе. Нападачи могу да, у припремној фази, годинама дискретно истражују циљани систем, не би ли пронашли његову „слабу тачку“, пре него што приступе реализацији главне операције.[632]

4.3.7.4. Циљеви напада

У односу на суштину феномена кибер тероризма било би оправдано извести закључак да би кибер терористички напад превасходно морао циљати критичну информациону инфраструктуру како би довео до деструкције и смрти. На пример, уколико би информатички напад био усмерен на изазивање дисфункције система за контролу авио-саобраћаја, резултовао би великим људским жртвама. Извештаји FBI-ја говоре о ангажованости припадника „Ал каиде“ на истраживању информација везаних за инфраструктуру система процесног управљања (SCADA), система који управља процесима водоснабдевања и постројењима за отпадне воде у САД. Уколико су информације из извештаја Федералног бироа веродостојне, у скоријој будућности би могло доћи до преузимања даљинске контроле над системима SCADA од стране терориста и изазивања озбиљне штете – изливања водних акумулација или, пак, контаминације пијаће воде.[633]

Други сценарији антиципирају конвергенцију физичких напада са кибер нападима на критичне инфраструктуре. Могуће је замислити ситуацију у којој је самоубилачки бомбашки напад праћен логистичком подршком кибер терористичке групе. Ова група би имала циљ да онемогући обавештавање безбедносних и здравствених служби о догађају, изазивањем прекида у напајању електричном енергијом или функционисања телекомуникационих веза.

---

[632] *Cybercrime… Cyberterrorism… Cyberwarfare… Averting an Electronic Waterloo*, CSIS Task Force Report, Washington D.C., 1998.

[633] Ashley B., *op. cit*.

Према неким теоријским концепцијама, кибер терористички напад би могао да буде базиран на осујећењу расположивости Интернета или бар на изазивању поремећаја у његовом функционисању. Напад извршен октобра 2002. године на девет важних сервера, језгара Интернета, показао је да су овакви сценарији заиста могући.[634] Ипак, за извршење таквих акција била би потребна велика количина координата, стручног знања и нападачког арсенала. Осујећење Интернета би довело до потпуне блокаде информационог друштва, што Интернет чини вишестрано интересантном метом. Ипак, кибер терористи који би желели да онеспособе глобалну мрежу морали би, такође, знати да би таквим чином и себи ускратили средство за реализацију будућих кибер напада. Из тог разлога би сценарији кибер терористичких напада морали да буду редефинисани – Интернет би нападачи требало да перципирају као последње место које би колабирало, а не као прво.

На основу доступних информација можемо закључити да су техничке и организационе способности терористичких организација, неопходне за извршење операција које превазилазе „ометајуће актове хакинга“, ван домета познатих терористичких организација. Чињеница да, до сада, није дошло до ерупције недискриминисаног насиља у кибер простору наговештава недостатак знања и/или средстава или, пак, мотивације код терориста. Кибер тероризам, према томе, можемо оквалификовати као феномен који припада будућности.

Без обзира на изостанак манифестације овог појавног облика терористичке активности, не би било рационално потценити претњу. Терористички кругови се постепено попуњавају регрутима нове, млађе генерације, којима информациона технологија не представља непознаницу. Наредна генерација терориста, која одраста у дигиталном свету и има на располагању моћније и једноставније инструменте напада од данашњих, могла би да у кибер тероризму уочи већи потенцијал од оног који ми видимо данас. Она ће имати виши ниво информатичког знања и оспособљености. Прогресивна интеграција виртуелног и реалног света у свим аспектима друштвеног живота, као и настанак „интелигентних“ техничких уређаја,

[634] Kheng Lee Gregory Tan, *Confronting cyberterrorism with cyber deception*, Master's Thesis, Naval Postgraduate School, Monterey, California, 2003, p. 21.

попут аутомобила, кућних апарата и других уређаја повезивих са Интернетом, могли би да кибер тероризам учине још привлачнијом опцијом.

Иако терористи нису још користили кибер простор као бојно поље, неоспорно је да га користе као инструмент за подршку сопственим активностима. У том смислу, озбиљно се мора схватити и могућност повезивања и удруживања различитих субјеката претње заступљених на Интернету. Према одређеним тврдњама, талентовани хактивисти у разним крајевима света били би спремни да продају своје експертизе у замену за одговарајућу надокнаду или „исправну“ политичку промену.[635]

На крају овог разматрања можемо констатовати да, колико год се претња кибер тероризма чинила као прецењена, мере које се данас предузимају ради супротстављања нису губици ни времена, ни енергије, ни новца. Превентивне активности у пољу заштите од потенцијалне претње кибер тероризма свакако да оснажују мере које се предузимају у борби против онога што је тренутно права рак-рана кибер простора – његова злоупотреба у криминалне сврхе.

[635] DK Matai, председник „Mi2g“, лондонске фирме која пружа услуге сервиса за кибер безбедност, тврди како „постоје докази да руски хакери нуде своје услуге радикалним исламским групама“. Према: Blau J.: “The battle against cyberterror”, *Network World*, http://www.networkworld.com/. Не треба, међутим, сметнути с ума чињеницу да они који пружају услуге у пољу кибер безбедности имају интерес да ситуацију прикажу као изузетно опасну.

5. ТЕНДЕНЦИЈЕ КИБЕР РАТОВАЊА И МОГУЋНОСТИ СУПРОТСТАВЉАЊА И ЗАШТИТЕ

Проблеми који настају из компјутеризације друштва почели су још седамдесетих година прошлог века да изазивају забринутост влада и одговарајућих институција, али и наднационалних субјеката међународних односа. Прва међу њима била је влада Шведске, која је израдила студију о опасностима што угрожавају друштво због концентрације и ширења компјутеризованих података и због прекограничног тока таквих података. Студија под насловом *Рањивост компјутеризованог друштва* завршена је 1979. године под покровитељством Комитета за осетљивост рачунарских система (Committee on the Vulnerability of Computer Systems) и изражавала је озбиљну забринутост у вези са развојем компјутеризованих система и величине њиховог утицаја на друштво.

Затим је у Шпанији 1981. године одржано међународно саветовање у организацији шпанске владе и Организације за економску сарадњу и развој (*OECD*), а већ 1982. године у решавање овог проблема укључила се и Европска економска заједница (*EEC*). Комисија *EEC* је исте године формирала групу европских научника са задатком да изради студију о осетљивости (рањивости) европских друштава. Финални извештај, рађен на основу ситуације у Белгији, Француској, Италији, Великој Британији и Немачкој, био је поднет 1983. године и садржао је серију препорука и програма акција на нивоу Заједнице.

У оквиру Савета Европе (*CoE*) формиран је 1985. године комитет који се бавио питањима угрожености друштва због аутоматизације информационих система. Један број рефлексија на криминалитет у области рачунарских технологија такође је био разматран и на седмом Конгресу УН, одржаном 1985. године у Милану.[636] Током 1985. године и у Норвешкој је израђен извештај назван *Рањивост друштва зависног од рачунара* (The Vulnerability of a Computer Dependent Society), у којем је закључено

[636] Петровић С.*: Компјутерски криминал*, МУП Србије, Београд, 2001, стр. 8.

да је „ситуација врло озбиљна“ са становишта друштвене и националне безбедности.[637]

Проблем је такође био веома актуелан у САД. Тако је 1981. године Служба за технологију америчког Конгреса разматрала проблем осетљивости националних информационих система („Computer Based National Information Systems: Technology and Public Policy Issues“); док се извештај Савеза америчких друштава за обраду информација (American Federation of Information Processing Societies – AFIPS) из 1984. године претежно бавио питањима националне безбедности и рањивости америчких рачунарских инсталација.[638]

Питање рањивости информационих система и, посредно, њеног утицаја на рањивост друштва привремено је након Хладног рата прешло у други план, услед смањења директних претњи територијалној безбедности, али је већ половином деведесетих година прошлог века поново заокупило пажњу светских креатора политике, на челу са САД. Перцепција новог и опасног ризика за америчку националну безбедност, по неким мишљењима, секундарна је последица властитог развоја војних стратегија и офанзивних способности на подручју информационих операција. У основи те перцепције постојала је свест да и потенцијални непријатељи САД-а могу развити аналогне способности.[639]

Данас више нико не доводи у питање чињеницу да многе државе развијају офанзивне стратегије кибер ратовања. Осим њих, и цивилни сектор се доказао у злоупотреби ИК технологија. Број информатичких напада на глобалном нивоу свакодневно се повећава као и обим штете узроковане нападима. Због тога питања контроле, превенције и супротстављања кибер нападима представљају неке од акутних безбедносних изазова, како на националном и субнационалном нивоу тако и на регионалном и гобалном нивоу.

---

[637] *Ibid*., стр. 6.

[638] *Ibid*., стр. 7.

[639] Eriksson E. A.: “Information Warfare: Hype or Reality?”, *The Non-proliferation Review*, Spring-Summer 1999, http://cns.miis.edu

5.1. Тенденције кибер ратовања

Из досадашњег излагања лако се може извести закључак да је степен злоупотребе ИК технологија висок, да је спектар начина угрожавања безбедности кибер простора широк, као што је разноврстан и број субјеката, тј. протагониста кибер ратовања. Међу експертима у области ИК технологија опште је прихваћено мишљење да ће се степен злоупотребе рачунара и информационо-комуникационих технологија и даље увећавати.

Томе у прилог иду показатељи о непрекидном увећању бројности корисника Интернета, количине малициозних кодова у оптицају као и њиховог све деструктивнијег потенцијала. Са друге стране, не треба пренебрегнути ни мотивисаност националних армија за развијање офанзивних стратегија кибер ратовања. Сви актери у кибер простору, од индивидуалних корисника до националних држава и војних савеза имају интереса да искористе, а по потреби и злоупотребе, пун потенцијал ИК технологија.

У данашње време светска популација је бројнија и интегрисанија него икада раније. Она у многим аспектима превазилази традиционалне границе држава-нација. Превазилажење географске разноликости може се постићи само у интегрисаном свету, кроз технолошко напредовање у копненом, ваздушном и водном превозу, као и путем општег технолошког развоја и, посебно, у сфери комуникација.

Овај пораст светске интеграције, посебно дигиталне интеграције, постаје очигледан након испитивања светске популације и броја тренутних Интернет корисника и оних који се предвиђају у будућности, као што то показује Табела 12.

Табела бр. 12: *Број корисника Интернета*

	Година		
	1990.	2005.	2015.
Процењена светска популација	5.3 милијарде	6.4 милијарде	7.2 милијарде
Процењен број корисника Интернета	2.6 милиона	1 милијарда	2 милијарде
Проценат корисника у односу на светску популацију	<1%	15.6%	27.8%

Извор: ITU, www.itu.int

Број Интернет корисника у будућности могао би бити на још вишем ступњу од предвиђеног. Он би могао да премаши приказане процене услед глобалног тренда у бежичном приступању Интернету као и појефтињења рачунара и рачунарске опреме на тржишту. То би, свакако, повећало ризик од кибер ратовања.

Роберт Меткалф (Robert Metcalfe), инжењер електротехнике познат по изуму *ethernet* технологије, поставио је хипотезу да се квалитет рачунарске мреже повећава сразмерно са бројем њених корисника.[640] Са друге стране, можемо тврдити да се исто дешава и са претњама, вулнерабилношћу, ризицима и нападима. Степен ризика од злоупотребе се увећава са бројем корисника мреже исто као што се повећава и њен квалитет. Виртуелни простор представља место где појединац, или неколицина људи, могу да науде многима.

Штавише, док се виртуелна заједница увећава, скраћује се време неопходно за одговор на кибер претње, ризике и нападе.

Вирусу *Nimda*, у 1990. години, је требало само 22 минута да постане вирус број један свих времена.[641] У јануару 2003. године, црв *Slammer* је инфицирао 75.000 рачунара за приближно десет минута (при чему је дуплирао број сваких 8,5 секунди у првом минуту заразе) и постао црв са најбржом репродукцијом свих времена.[642] Већ 2004. године, појавом вируса *Sasser* свет је суочен са, како је сковано, „нултим даном одзивног времена“ будући да овај вирус допире до сваке чворне тачке Интернета за мање од сат времена, при чему се штета коју причињава процењује на 3,5 милијарди долара.[643]

Са повећањем броја и интензитета напада расту и негативне финансијске последице по кориснике Интернета.

---

[640] Green H.: “We all knew better”, *BusinessWeek Online*, http://www.businessweek.com/magazine/toc/03_34/B38460333futuretech.htm

[641] *Virus stats*, CSA/TruSecure, http://www.ICSAlabs.com

[642] *History of viruses*, Pearson Education, Inc., http://www.factmonster.com/pages/copyright.html

[643] *Maximizing Email Security ROI*, CipherTrust, http://www.ciphertrust.com/resourses/articles/articles/roi_2_virus.php

Табела бр. 13: *Финансијска штета узрокована нападима вируса*

Штета узрокована вирусима на светском нивоу	
Година	Штета у милијардама US долара
2005	14.2
2004	17.5
2003	13.0
2002	11.1.
2001	13.2.
2000	17.1
1999	13.0
1998	6.1
1997	3.3.
1996	1.8
1995	0.5

Извор: *Computer Economics*, http://www.computereconomics.com/article.cfm?id=1090

Са друге стране трошкови нападача, чак и оних који спадају у професионалне кибер криминалце, су релативно мали. Они су углавном сведени на трошкове развоја малициозних кодова и/или спровођења дигиталног напада (евентуалног закупа bot мреже) будући да је Интернет доступан свима који поседују жељу и неопходно знање за извршење напада.

Па ипак, нису само финансијски разлози ти који поспешују кибер ратовање, и који ће, по свој прилици, и у будућности то чинити. Често су у питању и други интереси, попут политичких, војних, обавештајних, корпоративних итсл.

Опште узев, можемо тврдити да на ескалацију кибер ратовања, као и свих других видова друштвених конфликата, могу утицати економски, политички структурни и културно-перцептуални фактори. У наставку рада покушаћемо да укажемо на неке од глобалних проблема који могу довести до јачања антагонизама на регионалном и глобалном нивоу, те повећања конфликтног потенцијала између корпоративних субјеката, држава или пак, појединаца из различитих региона света.

5.1.1. Проблем непостојања ваљаних правних механизама надзора и контроле кибер простора

Проблем нерешеног формално-правног власништва над кибер простором тренутно јесте један од суштинских извора неповерења између држава. Овај проблем је доспео у први план *Декларације о принципима* – завршног документа прве фазе Светског самита о информационом друштву, одржаног у Женеви 2003. године.

Декларација је, прецизно говорећи, истакла следеће кључне тачке:[644]

1. Декларација установљава да су ИКТ суштинска основа за свеобухватно информационо друштво и подржава идеју универзалне, доступне, непристрасне, фер и финансијски прихватљиве ИКТ инфраструктуре и сервиса, као кључни циљ учесника који ће помоћи да се она изгради.

2. Поспешивање поверења и вере у ИКТ, укључујући информациону и мрежну безбедност, аутентификацију, заштиту приватности и заштиту корисникâ, подвлачи се као предуслов за развој информационог друштва.

3. ИКТ су такође значајно средство управљања – владавине. Декларација подвлачи потребу да се створи погодно окружење на националном и међународном нивоу, засновано на владавини закона са подржавајућом, транспарентном, конкурентски оријентисаном, технолошки неутралном и предвидивом политиком и регулаторним оквиром.

4. Ако је универзални приступ основа правог информационог друштва, грађење капацитета је њен мотор. Декларација установљава да само кроз инспирисање и едукацију нација којима нису блиски Интернет и његове моћне импликације може „сазрети воће“ универзалне доступности.

5. Препознаје се и да се ресурси морају каналисати ка маргинализованим и осетљивим друштвеним групама, како би се осигурало прихватање ИКТ и како би се оне оснажиле.

6. Декларација реафирмише универзалност и недељивост свих људских права као фундаменталних слобода у информационом друштву, те подржава демократију и добро управљање.

7. У погледу интелектуалне својине, Декларација једнако подвлачи значај подршке иновативности и креативности, као и потребу за разменом знања како би се поспешиле иновација и креативност.

[644] ITU, http://www.itu.int/wsis/documents/background.asp?lang=en&c_type=res

8. Кључни принципи укључују поштовање културне и језичке разноликости, као и традиције и религије, посебно на Интернету, што значи вишејезички, разнолик и културно одговарајући садржај.

9. У погледу Интернет-менаџмента, истакнуто је да ће и техничке теме и правила јавне политике укључити све заинтересоване инвеститоре и организације. Али, глобално управљање Интернетом исувише је комплексно да би се детаљно разрешило. Постигнут је договор да се пре друге фазе самита у 2005. години формира отворена, доступна радна група о управљању Интернетом, која ће истраживати и сачињавати предлоге за акције.

10. Такође су подржани принципи слободе штампе, независности, плурализма и медијске разноврсности.

11. Декларација даје безусловну подршку премошћавању дигиталног јаза, кроз интернационалну сарадњу свих потписника.

Друга фаза Самита о информационом друштву одржана је у Тунису од 16. до 18. новембра 2005. И овај скуп је, као и претходни, подржала Америка кроз окриље више невладиних институција и међународних организација. Један од разлога америчке подршке оваквом скупу свакако треба тражити у појачаној перцепцији значаја и утицаја који имају технологија и светска мрежа – Интернет, нарочито после 11. септембра 2001.

На скупу је учествовало око 170 држава и велики број лидера, на челу са генералним секретаром УН Кофијем Ананом. Међутим, већина од педесетак државника учесника Самита била је из афричких и арапских земаља, док скупу у Тунису није присуствовао ниједан шеф државе или владе из развијених западних земаља.[645] Главна тема скупа требало је да буде реструктурација друштва са циљем да се омогући и побољша приступ информационој и комуникационој инфраструктури и технологијама, као и приступ информацијама и знању, повећа поузданост и безбедност у примени ових технологија и створе повољни услови за њихову ширу примену.

---

[645] ITU, http://www.itu.int/wsis/tunis/newsroom/index.html

Светски медији су данима пред отварање самита писали о хаосу који може настати на састанку у Тунису, услед жеље великог броја земаља да се на дневни ред Самита стави питање управљања Интернетом и финансијским механизмима за информационо-комуникационе технологије. Наиме, неке државе, попут Кине, Индије, Бразила и Ирана, већ су годинама тражиле да се преиспита политика управљања Интернетом. Од окончања првог дела Самита (2003) оне су се залагале за оснивање новог међународног органа који би био надлежан за доделу Интернет-адреса и омогућавање повезивања рачунара преко јединственог стандарда, тј. за пренос контроле над Интернетом са независне Корпорације за додељивање имена и бројева на Интернету (ICANN), на чије одлуке Американци имају право вета, на неко мултилатерално тело (нпр. УН).

Американци су се бранили тврдњама како би већа умешаност влада заступљених у организацији УН (међу којима су и оне „нимало склоне демократији и слободи“) претила да угрози слободу, која је и основни разлог невероватног успеха Интернета. Осим тога, Американци су сматрали да су се добро показали током година у којима су контролисали Интернет, те да нема смисла преносити на УН свакодневни технички део посла који обавља некомерцијално тело приватног сектора ICANN.

У свом одговору Американцима Кина, Индија и Бразил су запретили да ће, у случају да њихови захтеви не буду узети у обзир, покренути сопствене мреже, са другачијим приступним кодом, што би у пракси довело до „распарчавања“ Интернета и ставило у питање његову универзалност, на којој почивају његова огромна популарност и успех.

Европска унија, која се никада раније није противила потпуној америчкој контроли над Интернетом, уочила је опасност од фрагментације Интернета и дала свој предлог, којим се америчка доминација над мрежом не доводи у питање. ЕУ се овим предлогом такође дистанцирала од групе држава које прижељкују могућност да надзиру садржај Интернета. Европска унија је, у ствари, предложила стварање „форума јавних политика“, на којем би се разговарало о питањима значајним за Интернет, али који не би имао одлучујућу моћ. ЕУ је указала да уговор који везује

ICANN за Министарство трговине САД истиче 2006. године, што отвара могућности за преговоре. Кординатор преговорâ, Јанис Карклинс[646] из Финске, замолио је владе земаља у спору да пажљивије погледају предлог европског компромисног решења како би се трогодишњи сукоб окончао на задовољство свих страна.

У смиривање тензија умешао се и генерални секретар УН, објављујући пред почетак самита ауторски текст у немачком листу *Франкфуртер рундшау*,[647] у којем је стајало да се са приближавањем самита у Тунису множе гласови оних који имају „погрешне информације". У датом чланку Анан је, подсећајући на добре и лоше стране Интернета, написао да је, за кратко време колико постоји, Интернет постао средство драматичних и револуционарних промена у здравству, образовању, новинарству, политици, али и да „постоје оправдане сумње због злоупотреба од терориста, десних екстремиста, као и оних који шире порнографију", те додао „да треба захвалити САД што су развиле Интернет и учиниле га доступним свету. Из историјских разлога, Америка поседује највећи ауторитет над некима од најважнијих ресурса Интернета и многи кажу да тај ауторитет убудуће треба да буде подељен са међународном заједницом и САД, које су своју контролну функцију до сада обављале фер и часно, увиђајући и саме да остале владе имају легитимне сумње". Анан је у свом ауторском тексту посебно истакао како је „једна од погрешних представа да УН желе да 'преузму' Интернет или да га контролишу", наглашавајући да ништа није даље од истине него та тврдња. „УН желе само да омогуће глобално ширење и то је централна тема сусрета на врху."[648]

САД су најпре биле одлучне у борби против било какве промене у начину контроле Интернета. Амерички државни секретар Кондолиза Рајс позвала је једним писмом Велику Британију да своје председавање Европском унијом искористи за одбацивање захтева за поделом контроле над Интернетом. Међутим, неколико сати пре званичног отварања скупа Американци су пристали на компромис. Прихваћено решење је било најближе европском предлогу. Договорено је да се питање коришћења и контроле Интернета детаљније разматра на неком будућем

---

[646] ITU, http://www.itu.int/wsis/preparatory2/karklins.html

[647] *Frankfurter Rundschau*, http://www.f-r.de/ressorts/nac...ik/thema_des_tages/?cnt=753624

[648] Према: Марковић А.: „Утисци са WSIS 2005", http://www.elitesecurity.org/t147318-Utisci-sa-WSIS-The-World-Summit-on-the-Information-Society-Tunis-to-November

међународном форуму. До тада се управљање адресним системом Интернета оставља у надлежности САД, а свим питањима која буду искрсла бавиће се посебна међународна комисија, названа Управљачки форум Интернета (Internet Governance Forum), чије одлуке неће бити обавезујуће ни за САД ни за ICANN (који данас сачињавају представници тридесетак држава света. Они надзиру рад тог тела, али у пракси имају искључиво саветодавну улогу).[649] Другим речима, Сједињене Америчке Државе успеле су да задрже неприкосновену контролу над управљањем Интернетом.

Осим потпуне контроле над Интернетом, САД располажу техничким средствима која им омогућавају да блокирају сваки сајт на планети. Американци, међутим, „никада нису употребили ни злоупотребили ове могућности, нити су покушали да утичу на садржај података који се пуштају преко Мреже, и тиме су обезбедили потпуну независност овог новог моћног медија и средства за комуникацију“, писало је у образложењу донете компромисне одлуке.[650]

Самит су званично отворили председник Туниса и генерални секретар Уједињених нација Кофи Анан, који је бираним речима нагласио даљу потребу за наставком дијалога о начинима за контролу и управљање Интернетом. Тачније, обраћајући се учесницима самита, Анан је рекао да УН нису надлежне за та питања и предложио је да за светску електронску мрежу и даље остане надлежна непрофитна Корпорација за додељивање бројева и назива̂ на Интернету. Генерални секретар УН дипломатски је оценио да је кључно наставити разговоре о датом питању, напомињући да би у њих требало да буде укључено што више држава.

5.1.2. Национални и регионални развојни диспаритети – „дигитални јаз“

Основна тема самита, пак, требало је да буде превазилажење огромног јаза који постоји између богатих и сиромашних земаља у односу на приступ Интернету. Приликом отварања, Генерални секретар УН је истакао да би сиромашним земљама

---

[649] САД, иначе, не пропуштају прилику да истакну како је ICANN америчка корпорација са седиштем у Калифорнији, али је њен председник Аустралијанац, а већина запослених и чланова управног савета заправо нису Американци.

[650] ITU, http://www.itu.int/wsis/tunis/scripts/list.asp

требало омогућити користи од ИКТ, које би могле да побољшају ниво њиховог социјалног и привредног развоја.

Могућност приступа Интернету одређена је дистрибуцијом неопходних услова за развој одговарајуће инфраструктуре и, по правилу је везана за економску моћ да се одговарајућа технологија имплементира у одређеној средини. Међутим, осим економских услова који обезбеђују умрежавање, велику препреку у дифузији Интернета представља и дејство других фактора. Пре свега, проблем лежи у чињеници да је већински део садржаја светске мреже на енглеском језику. У правом смислу те речи, нечија могућност да ефикасно користи ресурсе Интернета одређена је управо његовим степеном познавања енглеског језика. Дистрибуција језика на којима су постављене информације на Интернету и дистрибуција матерњих језика корисника Интернета налазе се у диспропорцији. Поред ових фактора, утицај на проширење дигиталног јаза врши и недостатак одговарајуће обуке за употребу рачунара. Коначно, највећу опасност по проширење дигиталног јаза представља нешто што је још увек део саме природе процеса развоја Интернета, а то је брзина којом се овај процес развија. Са протоком времена, дигитални јаз се продубљује „сам од себе“, тако што се развијају нова и моћнија технолошка решења која почивају на све захтевнијим основама и траже нова улагања у инфраструктуру. На тај начин, средине које нису умрежене као развијени део западне цивилизације све више заостају, уместо да постепено сустижу запад.

О неједнаком степену развоја држава у домену ИКТ илустративно говори Извештај о телекомуникационом развоју у свету (WTDR), објављен уочи прве фазе Самита. Саставни део Извештаја, који издаје Међународна телекомуникациона унија (ITU), чини Индекс дигиталног приступа (DAI), који рангира државе на основу приступа информационим и комуникационим технологијама, и сматра се важним референтним документом за владе, међународне организације посвећене развоју, невладине организације и приватне предузетнике како би проценили ниво информационих и комуникационих технологија у појединим земљама.

Индекс дигиталног приступа се разликује од других сличних прегледа, зато што укључује неколико нових категорија, као што су образовање и могућност приступа Интернету. На списку се налази 178 земаља, које су класификоване у четири категорије у смислу дигиталне „имовине“: висока, виша, средња и ниска.

Како је показао Индекс дигиталног приступа, изузев Канаде, која је на 10. месту, осталих девет водећих земаља искључиво је из Азије и Европе, док су САД на 11. месту.

Водеће ИКТ привреде су Шведска, Данска, Исланд, Кореја, Норвешка, Холандија, Хонгконг, Финска, Тајланд и Канада. Остале европске земље међу првих двадесет пет јесу Велика Британија, Швајцарска, Луксембург, Аустрија, Немачка, Белгија, Италија, Француска и Словенија.

У следећој, категорији налазе се углавном земље централне и источне Европе, Кариба, из региона Персијског залива и латиноамеричке државе са настајућим тржиштима. Многе од њих су користиле ИКТ као средство развоја, а политике националних влада помогле су им да остваре завидан ниво иметка у ИКТ. Међу таквима су значајни пројекти попут *Dubai Internet City*-ја у Уједињеним Арапским Емиратима, земљи која је највише рангирана у арапском свету, и *Cyber City*-ја на Маурицијусу, који је, са суседном острвском државом у Индијском океану (Мадагаскаром), највише пласирана афричка земља. Кореја, Тајван, Сингапур и Хонгконг идентификовани су као „четири азијска тигра“, јер су остварили највећи напредак у ИКТ.[651]

Сенегалски председник Абдулаје Ваде је, насупрот томе, током излагања на самиту подсетио да је Африка „искључена“ из савременог света комуникација, с обзиром на то да само њујоршка четврт Менхетн има више телефонских линија од целог афричког континента. Према статистици Међународне уније за телекомуникације јаз између богатих и сиромашних земаља је више него очигледан: од 6,2 милијарде становника на свету две милијарде никада у животу нису користиле телефон, а тек нешто више од 1,2 милијарде особа има фиксни телефон. Иако 80 одсто светског становништва живи у подручјима покривеним мрежом мобилне телефоније, само једна четвртина користи мобилни телефон, а четири милијарде особа ниједном се нису послужиле мобилним телефоном.

[651] Према: ITU, http://www.itu.int.

На самиту је усвојена „Агенда за информационо друштво“, која би требало да представља пут за смањивање технолошког јаза између Севера и Југа.[652] И поред тога што је на самиту потврђено постојање „дигиталног јаза“, ни овог пута нису утврђени извори средстава за помоћ дигитално неразвијеним земљама. Проблем смањења разлика у коришћењу информационе технологије између богатих и сиромашних држава и даље остаје отворен. Представници индустријски развијених земаља, на опште разочарање света у развоју, нису пристали на обавезни финансијски допринос Фонду солидарности, који је задржао „факултативни карактер“. У оквиру тог Фонда, установљеног у првој фази самита у Женеви 2003. године, прикупљено је око осам милиона евра, али су се његови промотори надали да би могли годишње прикупити знатно већа средства и сиромашне земље снабдети информационим технологијама по нижој цени.

Утицај перцепције ове неједнаке дистрибуције приступа основном светском информационом ресурсу на формирање ставова према Интернету немогуће је искључити. Мале културе са недовољно развијеном економијом неће бити у стању да на адекватан начин испрате све тенденције у развоју Интернета, од којих су посебно значајне оне у развоју информационе економије (e-banking, e-commerce и сл.) и електронског управљања (e-governement). Чак и ако развијени део западне цивилизације, већ увелико умрежен и са још увек растућом стопом употребе Интернета, одлучи да финансира пројекте из области умрежавања у сиромашним земљама, проблем неће бити решен због ограниченог приступа Интернету самих грађана. Видимо како је проблематика неједнаке дистрибуције приступа повезана са економском, политичком и проблематиком репрезентације култура на мрежи.[653]

5.1.3. Расподела моћи у кибер простору – борба за доминацију

Самит је показао да је централно питање „информационог доба“, у ствари, питање начина владавине кибер простором, тј. расподеле моћи унутар кибер простора. Чињеница је да од настанка „информационог доба“ развијене државе,

---

[652] ITU, http://www.itu.int/wsis/docume..._multi.asp?lang=en&id=2266|2267

[653] Миловановић Г.: *Концепт информационог друштва и друштвени ефекти интернета*, Центар за проучавање информационих технологија, Београдска отворена школа, Београд.

велике привредне корпорације, интересне групе, међународне организације и појединци покушавају да промовишу и контролишу проток информација у кибер простору. Мислимо на различите врсте информација, од интелектуалне својине и научних истраживања, до политичког деловања, брендирања или културних симбола.

У борби за превласт над основним ресурсом инфорационог доба – информацијом – једну од водећих улога имају транснационалне корпорације развијених земаља, које су и главни носиоци процеса глобализације и новог поимања економије. Информација, односно знање, као основни производни ресурс, пружа транснационалним корпорацијама много шире могућности у привређивању. У тежњи за умањивањем производних трошкова и повећањем оствареног профита, транснационалне корпорације, а на првоме месту оне које се баве информационом технологијом и комуникацијама, те́же да остваре контролу над научноистраживачком делатношћу. Транснационалне корпорације настоје да на тај начин остваре доминацију у модерним гранама привреде заснованим на знању, које доносе новододату вредност неупоредиво већу од профита традиционалних привредних грана.

Међутим, жеља за постизањем економске превласти на планетарном нивоу није једини мотивациони фактор у тежњи за остваривањем контроле над кибер простором. На друге субјекте међународне заједнице подстицајно делују идеје да се контролом кибер простора може утицати не само на динамику националног развоја, већ и на ток глобалног развоја као и на међународне односе уопште. На тај начин различити субјекти, присутни у кибер простору, постају протагонисти, али и жртве најновијих метода дистрибуције и манипулације информацијама. Исход битке око протока информација дефинисаће, напослетку, ко ће држати моћ у глобалној информационој култури и економији.

Проблем односа између моћи и легалитета и легитимитета власти у кибер простору отвара велики број питања. Да ли ће информатизовано друштво моћи да се одупре жељи за моћи држава, појединаца и група? Да ли ће моћи да се заустави већ сада веома изражена тенденција корпоративног преузимања Интернета. Колико регулација Интернета иде у прилог повлашћеној богатој, просвећеној и образованијој класи, и колико ће се учинити на премошћавању економских и социо-културних диспаритета? Како пронаћи модус организације, систематизације,

законске регулације и координације глобалног управљања Интернетом, али и осталим познатим и будућим облицима преноса информација? По свој прилици, одговоре на ова питања, услед њихове комплексности, у ближој перспективи неће бити могуће дати.

Одржавање самита у Тунису било је иницирано и подржано од стране технолошки најнапреднијих држава света, између осталог, и услед перцепције једног посебног проблема који је на самиту формулисан у форми безбедности кибер простора. Реч је о страху од последица које може изазвати изражена зависност глобално умреженог друштва од савремених ИК технологија, будући да су распрострањеност ИК технолошких инструмената у развијеним земљама, њихова расположивост на глобалном нивоу, економска приступачност, ефективна корисност и лакоћа употребе такви да је њиховом релативно поузданом и континуираном функционисању препуштено обављање основних функција друштва. Учесници самита су се сложили да је потребно основати међународни форум у оквиру којег ће разматрати питања од значаја за безбедност кибер простора, попут кибер криминала, непожељне електронске поште и рачунарских вируса који се шире преко глобалне мреже.

5.2. Могућности превенције и супротстављања конфликтима у кибер простору

У информационим системима сконцентрисана је огромна количина података и информација који, по својој природи, могу да изражавају материјалну вредност, али исто тако могу да представљају личну, пословну, професионалну, војну или државну тајну. Управо из тог разлога, било какво угрожавање информационих система може нанети знатну штету индивидуалним корисницима, друштвеним субјектима и информационом друштву у целини. Непрестано повећање учесталости напада, као и метода и средстава кибер ратовања, његов специфични карактер и препозната друштвена опасност у све већој мери постају врло озбиљан друштвени проблем, и то не само у националним већ и у међународним размерама.

Глобална рачунарска мрежа и транснационални проток података и информација укинули су класичне државне границе. Услед распрострањености и децентрализованости Мреже, активности злонамерних актера у кибер простору постале су међународни проблем и отвориле питања заштите не само властитих већ

и туђих информационих система, спровођења међународних истрага, екстрадиције и кажњавања извршилаца.[654] Последњих година су, у том смислу, изражене интензивне активности на формирању широког одбрамбеног фронта, сачињеног од свих заинтересованих субјеката, у циљу супротстављања безбедносним претњама и смањењу ризика од њиховог манифестовања. У супротстављању безбедносним претњама у кибер простору на располагању су, уопштено узев, три типа механизама који могу помоћи да се успешно одговори на ове изазове: алати за заштиту, етика и законска регулатива.[655]

Досадашња искуства у супротстављању безбедносним претњама у кибер простору указују на потребу стварања кохерентног делатног оквира који подразумева примену како превентивних, тако и репресивних мера у стварању безбедног кибер амбијента. Превентивне активности, на првоме месту, подразумевају осмишљавање различитих механизама и стратегија заштите информационих система и њихову имплементацију, али и доношење законских мера, како на националном тако и на међународном нивоу, као и њихово усклађивање са обавештајним активностима у покушају супротстављања кибер претњама.

Глобално гледајући, неопходни предуслови за успешну реализацију наведених замисли морали би се обезбедити на три нивоа: локалном (нивоу корисникâ информационих система), националном и међународном.[656] Адекватан систем заштите, примерен сваком од наведених нивоа, морао би да има двојаку функцију: да одврати од злоупотребе рачунара, односно спречи његову злоупотребу, и да, у случају да је злоупотреба извршена, омогући брзо откривање и доказивање учињеног дела.

---

[654] У пракси је чест случај да, на пример, злонамерни актер извршава деликт из једне државе, преко провајдера у другој држави, користећи као средство рачунар „отет“ у трећој држави, а да последице наступе у четвртој, хиљадама километара удаљеној држави. Извор: презентација проф. др Мирјане Дракулић на међународном семинару *Компјутерски и cyber криминал – како се борити против њега?*, одржаном у Центру „Сава“, Београд, 21. 11. 2007.

[655] Петровић С.: *Полицијска информатика*, Криминалистичко-полицијска академија, Београд, 2007, стр. 171.

[656] *Ibid*., стр. 172.

5.2.1. Мере и стратегије заштите информационих система

Под заштитом информационих система подразумева се примарни, базични ниво заштите. Овај ниво се односи на заштиту информационих система, информација и информационих мрежа у приватном власништву грађана и свим битним државним и приватним организацијама. Информације, информациони системи и мреже представљају важну имовину која има материјалну и употребну вредност за сваког појединца и сваку организацију. Информација и информациона инфраструктура могу бити од пресудне важности за очување: националне безбедности, приватности појединаца али и конкурентности предузећа и других аспеката пословања (готовинских токова, исплативости, правне усаглашености и пословног угледа). Заштитом информација од широког опсега претњи се, са аспекта корпоративне безбедности, осигурава континуитет пословања, са циљем да се губици у пословању сведу на минимум.

Са аспекта националне безбедности, у циљу супротстављања активностима кибер ратовања, неопходно је спроводити заштитне мере на следећа три нивоа:

- *Оперативни ниво* – подразумева примену најсавременијих средстава за заштиту података и информатичких ресурса, код свих корисника ИК технологија. Осим тога, потребно је спроводити честа тестирања информационих система и одмах уклањати уочене безбедносне проблеме.
- *Производни ниво* – развити средства за мониторинг и аутоматску проверу безбедности код произвођача информатичких средстава. Спроводити ригорозна тестирања хардвера и софтвера информационих система на безбедносне пропусте.
- *Државни ниво* – реализовати критичне државне информационе системе као високо безбедне моделе. Увести политику заштите информација и информационих система и мрежа која би се спроводила на сва три наведена нивоа.[657]

Индивидуални корисници, као и приватни и државни сектор, суочавају се са широким опсегом безбедносних претњи у кибер простору – преварама, шпијунажом, саботажама, вандализмима итд. Технике напада се усавршавају, а сами напади постају све учесталији, амбициознији и софистицираније.

---

[657] Цигурски О.: *Информационе технологије у борби против тероризма*, Зборник Факултета цивилне одбране, Београд, 2005, стр. 179.

Да би се поменуте претње предупредиле, на примарном нивоу заштите морају се у обзир узети различити аспекти заштите. На основу досадашњих искустава, тзв. *добре праксе*, може се рећи да је пожељно примењивати модел вишеслојне заштите. Он представља вид проактивног деловања и обухвата неколико аспеката:

- Физички (онемогућава физички приступ - физичко обезбеђење);
- Технички (техничко обезбеђење - електронско обезбеђење; заштита од електромагнетног зрачења; идентификација, верификација и ауторизација приступа; системи за детекцију и спречавање напада; криптографија);
- Организациони (организациона структура, дефинисање радног процеса, развој софтверских система, праћење смерница и стандардâ, планирање итд);
- Кадровски (планирање и избор кадрова, руковођење, стручно усавршавање и безбедносно образовање итд.) и
- Нормативни (закони, упутства, планови и друга регулатива која обавезује и прописује извршење неке радње и начин изршења те радње).

Схема бр. 7: *Модел вишеслојне заштите*

Сфере физичке и техничке заштите се, уобичајено, називају *техничким аспектом* заштите, док се организациона, кадровска и нормативна сфера подводе под *друштвени аспект* заштите. Оба аспекта су подједнако значајна и само се њиховом комбинацијом, и синергијским ефектом, може постићи задовољавајући ниво заштите информационих система.

5.2.1.1. Технички аспект заштите

Физичка и техничка сфера заштите представљају прву линију одбране информационих система. Овај аспект заштите подразумева коришћење мера које имају за циљ регулисање начина и техничких поступака којима се може умањити ризик од злонамерног нарушавања функционалности информационих система. У циљу спречавања приступа (физичког и путем мреже) штићеном систему, у употреби су различити технички уређаји и средства али и разноврсни информатички алати.

Приликом планирања физичког обезбеђења користи се неколико метода. Контрола приступа је термин који се користи када се говори о механизму који регулише приступ рачунарима, софтверу и другим ресурсима. Сервери који чувају важне податке, рутери и друге битне мрежне компоненте требало би да се налазе у закључаним орманима, или обезбеђеним рачунарским центрима. Добро обезбеђен центар или орман представља физичку препреку за сваку особу која није овлашћена да приступи серверу.

Инсталација са добром физичком безбедношћу требало би да користи концентричне прстенове прогресивних физичких препрека, при чему се најосетљивији ресурси постављају у централни прстен. Брава са шифром на вратима рачунарског центра је и даље незаменљива, али је препоручљиво и постављање видео-интерфона. Локација сервера и других кључних компонената унутар рачунског центра би требало да буде заштићена још једним закључаним вратима под надзором. Уколико је потребно јаче обезбеђење, могу се увести магнетне картице, видео камере и стражари. Нико не би требало да улази у рачунарски центар, а да то не буде документовано. Унутрашњи прстенови обезбеђеног подручја би требало да пружају заштиту са свих шест страна просторије, што значи сва четири зида, плафона и пода. У неким случајевима се ове мере могу појачати алармним системима и камерама. Стандардни механизми за отварање врата попут металних кључева, магнетних картица и лозинки могу да буду недовољни за просторије које захтевају посебно обезбеђење. У том случају треба применити комбинацију биометријских провера: проверу отиска прста, геометрију руке, скенирање дужице,

скенирање мрежњаче или фацијални термограм. На пример, систем може да користи скенирање руке за брзу проверу идентитета а отисак прста за детаљну проверу.[658]

Бежично умрежавање је поред експлозије умрежених система, донело и нове безбедносне изазове. Локација је један од главних фактора који утичу на безбедност бежичних комуникација. Када се бирају и инсталирају компоненте за бежично умрежавање, а поготово тачке приступа, треба пажљиво извршити тестове како би се утврдио оперативни опсег уређаја. Антена би требало да буде постављена у центар зграде, што даље од спољашњих зидова. У случајевима када се преносе поверљиви подаци, потребно је да се снага преноса свих бежичних уређаја обавља на минимуму који дозвољава ефикасно обављање операција, тако да је потенцијалним шпијунима ван зграде отежано повезивање на мрежу и прислушкивање. Други фактор који може утицати на подизање безбедности бежичних мрежа је заклањање оперативног подручја. Тиме се мрежа штити од DoS напада, којима је изузетно подложна. Технологија мобилних комуникација има практично неограничен домет, и сада постоји много производа који преносивим рачунарима омогућавају да се повежу са мрежом која се налази било где у свету. Поред тога Bluetooth уређаји кратког домета могу се искористити за повезивање лаптопа са мрежом мобилног провајдера Интернет услуга. Због тога, увек треба имати у виду да је опасност од ове технологије далеко већа, јер није потребно да шпијун буде у близини мрежних инсталација да би добио приступ ресурсима. У тесној вези са физичком безбедношћу је питање чувања резервних копија података. У свету се отварају специјализоване установе за такве намене.

У циљу подизања нивоа заштите мрежних уређаја и матичних рачунара на виши ниво, препоручљиво је поштовање следећих правила:

- Онемогућити непотребне програме и процесе - што више инсталираних програма и што више покренутих процеса, већа је вероватноћа да ће малициозни код искористити слабост система;

[658] Ковачевић Ж.: *Компјутерска шпијунажа и заштита*, мастер рад, Факултет безбедности, Београд, 2010, стр. 80.

- Онемогућити непотребне сервисе - постоји много сервиса који се не користе или се користе алтернативно, а који представљају безебедносну претњу, или у најбаналнијем случају успоравају систем;
- Онемогућити непотребне протоколе;
- Проверити, тестирати и инсталирати све безбедносне исправке које дистрибутер објави (upgrade, service pack, patch, hot fix);
- Користити скенере слабих тачака, да би се таква места открила и заштитила;
- Онемогућити неселективни режим мрежних адаптера (осим у случају прегледа слабих тачака и надзора мреже, када овај режим мора бити омогућен).

Поред уклањања свих непотребних компоненти и примене надоградњи, у заштити оперативних система поред већ наведених мера треба укључити и следеће:

- Поставити сложене лозинке за све корисничке налоге и често их мењати;
- Одредити правила за блокирање налога;
- Уклонити и онемогућити непотребне модеме;
- Омогућити надгледање, записивање, проверавање и детекцију;
- Одржавати резервне копије и дупликате диска.

Треба се одлучити за безбедан систем датотека који омогућава подешавање дозвола на нивоу датотека и фолдера. Дозволе треба конфигурисати по принципу најмање привилегије.

Спровођење мера очвршћавања серверских апликација је такође од великог значаја за безбедност система. Ове мере постављају следеће захтеве:

- Истражити све проблеме који су специфични за коришћени сервер и његове апликације, информисати о безбедносним надоградњама, омогућити шифровање, одржавати резервне копије информација и користити алате за претраживање рањивих тачака;
- Општа препорука за све web сервере је: смањити број могућих сервиса, обезбедити доступне сервисе, јавне веб сервере изоловати од интерне мреже тако да се поставе у периферијску мрежу, интерне веб сервере заштитити тако да им се блокира порт 80 на интерној мрежној баријери, директоријуме на веб серверу обезбедити на одговарајући начин.
- Код сервера за е-пошту користити програме за откривање вируса, релеј за е-пошту или сервер-мрежне баријере, умањити оптерећење, проверавати да ли постоји нежељени садржај и обезбедити да отворени SMTP релеји буду затворени.

- Користити одвојене DNS сервере за разрешавање имена на интерној и периферијској мрежи, ограничити информације које се постављају на DNS, ограничити и обезбедити трансфер зоне, обезбедити динамичко ажурирање и када је год то могуће користити безбедни DNS.
- DHCP безбедност се заснива на: проверавању да ли постоје лажни DHCP сервери, конфигурисању информација о DHCP серверу на DHCP клијенту, ограничењу издавања адреса на познате MAC адресе, и блокирању DHCP портова на мрежној баријери.
- Сервери датотека и штампача, треба да буду заштићени тако да на мрежној баријери буде блокиран приступ заједничким ресурсима и сродним информацијама. При томе, треба да буду коришћени највиши нивои обезбеђења и провере аутентичности приликом приступа дељеним ресурсима. За сервере база података треба користити меморисане процедуре, конфигурисати овлашћени и забранити неовлашћени приступ, шифровати преносе поверљивих података, блокирати портове базе података на мрежној баријери и извршавати пробне упите на серверима да би се проверила безбедност.[659]

Приликом разматрања безбедности информација и уређаја који их преносе, у обзир се морају узети и заменљиви медијуми као што су магнетне траке, CD-ROM, DVD, феш меморије итсл. Ови медијуми се могу употребити за копирање података са сервера или за чување резервних копија или архивирање. У том смислу, потребно је осмислити мере како би се спречило изношење поверљивих података из предузећа на овим медијумима. Ако се на њима чувају поверљиви подаци, треба знати како их заштитити, који је најбољи начин за чување медијума да би информације остале нетакнуте и како ефикасно избрисати садржај са медијума када је то неопходно.

Употреба готових софтверских алата за заштиту, доступних на тржишту (попут антивирусних програма, *firewall*-филтера итсл.), свакако је од великог значаја на основном нивоу заштите. Информатички уско специјализовани методи и технике за откривање и супротстављање кибер нападима укључују коришћење специјалних софтверских апликација за заштиту персоналних рачунара и рачунарских мрежа,

[659] *Ibid*., стр. 79.

употребу криптографских и енкриптичких метода, техника и система, као и система за откривање и спречавање упада.[660]

Са аспекта националне безбедности, посебна пажња се мора посветити заштити система за аутоматизацију и управљање индустријским процесима (DCS, SCADA). У ову сврху могу се користити тзв. *embedded системи*[661], тј. системи посебне намене који су прављени мимо уобичајених стандарда и познатих, комерцијалних, пројектних решења присутних на тржишту.

Embedded системи су рачунарски системи специјалне намене (са јако израженом интеграцијом хардвера и софтвера), уграђени у оквиру другог система, за кога обезбеђују бољу функционалност и перформансе.[662] Насупрот рачунару опште немене, какав је персонални рачунар, embedded систем обавља један или већи број унапред дефинисаних задатака, обично са веома специфичним захтевима.[663]

Embedded системи поседују и неколико других карактеристика које их чине различитим у односу на рачунарске системе опште намене:

---

[660] Системи за откривање и спречавање упада се деле на системе за детекцију напада (*енгл*. Intrusion Detection System - IDS) и системе за превенцију напада (*енгл*. Intrusion Prevention System - IPS). Детектовање напада је процес надгледања и процене догађаја у рачунару и мрежног саобраћаја, са циљем да се открију знаци напада. Систем за детекцију напада је хардверски уређај са софтвером, или софтвер, који се користи за откривање неовчашћених активности на мрежи. Уређај се може имплементирати на појединачне рачунаре, сервере, на мрежној периферији или целој мрежи. Системи за превенцију напада су знатно напреднији од система за детекцију напада. Они су фокусирани на то шта напад ради, што је у основи непроменљиво. Основне функције система су: идентификација неовлашћених активности на основу потписа и детектованих аномалија, вођење евиденције и слање аларма администраторима у реалном времену, прикупљање форензичких података и спречавање напада. И ови системи могу бити смештени на рачунару или мрежи. О системима за откривање и спречавање упада видети више у: The Honeynet Alliance, Know Your Enemy Whitepapers, http://www.honeynet.org/papers/kye.html; Rehman R.: *Intrusion Detection Systems with Snort*, Prentice Hall PTR, 2003; Spitzner L.: *Honeypots: Tracking hackers*, Addison Wesley, 2002; Endorf C., Schultz E., Mellander J.: *Intrusion Detection & Prevention*, McGraw-Hill, 2004; Chirillo J.: *Hack Attacks Revealed – A Complete Reference with Custom Security Hacking Toolkit*, John Wiley & Sons, New York, 2001.

[661] Енглески термин *embedded* се преводи као угнеждени, уграђени или усађени али се најчешће користи у изворном облику.

[662] Бараћ Д.: *Real-time оперативни системи за мале embedded системе*, Универзитет у Нишу, Електронски факултет, Ниш, 2010, стр.4.

[663] Тако, на пример, мобилни срчани монитор/дефибрилатор је наменски систем који надгледа рад срца и од кога се не очекује да извршава апликације за процесуирање текста, па се због тога знатно разликује од персоналног рачунара који може да извршава велики број разних сложених апликација.

- Embedded системи су пројектовани да раде у екстремним амбијенталним условима. Ови системи се данас уграђују такорећи свуда: у авионима, колима, медицинским уређајима, сателитима, процесној индустрији, кућним апаратима итд. Амбијентални услови често диктирају строге захтеве у погледу високе поузданости у раду, микропотрошње, рада у реалном времену, једноставности управљања итд.
- Рад embedded система подржан је од стране широког дијапазона процесора и процесорских архитектура, док се за програмирање на персоналним рачунарима најчешће користи само једна платформа (x86 Intel). Пројектанти embedded система користе данас више од 140 различитих микропроцесора који се нуде од стране више од 40 различитих компанија које производе ове чипове. С обзиром на развој тржишта, све већу продају „паметних" уређаја, аутоматску контролу процеса у аутомобилима, авионима итд., све је већа и потреба за овом врстом процесора.
- Ако embedded систем користи оперативни систем то обично мора бити RTOS (Real Time Operating System).
- Импликације софтверских грешака су значајно озбиљније код embedded система у односу на десктоп системе.
- Embedded системи имају уграђено далеко мањи број системских ресурса (компонената) у поређењу са десктоп системима.
- Embedded системи чувају сав свој објектни кôд у ROM-у. Због ниске цене, микро-потрошње и других специфичности постоје ограничења у погледу уграђеног меморијског простора. Такође, с обзиром на то да је RAM простор ограничен, постоје и специфични захтеви који се односе на аспекте тестирања и отклањања грешака у раду оваквих система. Микропроцесори у овим системима обично имају имплементирана наменска кола за отклањање грешака (watchdog тајмери, self-test кола итд).[664]

Због своје атипичности у односу на комерцијалне системе (високе поузданости у раду, малог броја компонената, микропотрошње, рада у реалном времену, једноставности управљања, бројности процесорских архитектура итд.), embedded системи могу наћи примену у обављању појединих, наменских, процеса и задатака у системима процесног управљања. Препуштање појединих задатака embedded системима може знатно умањити шансу да потенцијални нападач продре у

[664] Према: Бараћ Д., *op. cit.*

системе који управљају индустријским процесима (DCS, SCADA), користећи њихове типичне рањивости (стандардне технолошке архитектуре хардвера и софтвера, као и стандардне протоколе глобалне мреже).

5.2.1.2. Друштвени аспект заштите

Будући да многи информациони системи нису пројектовани тако да се могу штитити техничким средствима (чији је домет, такође, ограничен), ефикасна заштита се мора базирати на одговарајућим управљачким политикама и процедурама у погледу: дефинисања радног процеса, развоја софтверских система, праћења смерница и стандардâ, планирања и избора кадрова, руковођења, стручног усавршавања и безбедносног образовања, као и доношења нормативних аката, и друге регулативе која обавезује и прописује извршење неке радње и начин изршења те радње.

Са *организационог аспекта* посебно је значајна имплементација међународних и националних безбедносних стандарда[665] у овој области. У последњој деценији XX века, и првој деценији овог века публиковани су, или прерађени, бројни национални и међународни стандарди који се односе на управљање безбедношћу података у рачунарским системима. Ови стандарди се, према намени, могу поделити на: стандарде за безбедност производа, стандарде за безбедност процеса и стандарде безбедности система.[666]

Чување информација, као мере знања и суштинског ресурса је добило свој оквир у серији стандарда *ISO 27000,* где су специфицирани захтеви које треба да поштује организација да би остварила систем за заштиту информација.

Темеље за успостављање овог стандарда поставио је почетком деведесетих Британски институт за стандардизацију (BSI). Иницијална верзија текста стандарда за систем управљања безбедношћу информација *BS 7799,* усвојена је 1995. а прва званична ревизија обављена је 1998. Пратећи брз развој рачунарских мрежа и Интернета, BSI објављује и други део стандарда *BS 7799-2.* Међународна

---

[665] Стандард представља скуп правила намењених обезбеђењу високог нивоа управљања сигурношћу података (информација).

[666] Кукрика М.: *Управљање сигурношћу информација*, INFOhome Press, Београд, 2002, стр. 102-103.

организација за стандардизацију (*енгл*. International Standardization Organization – ISO) прихвата ове стандарде под своје окриље и они у јуну 2005. године објављују другу верзију стандарда *ISO 17799 Информационе технологије - безбедност технике - Начела за управљање безбедношћу информација.* Стандард *ISO 17799* обрађује проблематику дефинисања политике рачунарске безбедности. Стандард пружа драгоцену помоћ менаџменту компаније да сагледа и разуме проблематику управљања безбедношћу података.[667] Тај стандард је, 2007. године, замењен стандардом *ISO 27002*.[668]

У октобру 2005. године објављен је стандард *ISO 27001* под називом *Системи управљања безбедношћу информација – Захтеви* (*енгл*. Information Security Management System /ISMS/ requirements).[669] Овај стандард је базиран на британском стандарду *BS 7799-2*. Он дефинише захтеве које мора да испуни систем за управљање безбедношћу података, да би га акредитована организација могла сертификовати.[670] Стандард *ISO 27001* је конципиран у следећих пет поглавља:

1. Систем за управљање безбедношћу информација (ISMS);
2. Одговорност руководства;
3. Интерна провера *ISMS*;
4. Преиспитивање *ISMS* од стране руководства;
5. Унапређење *ISMS*;

Основни појмови везани за систем безбедности информација дати су у тачки три стандарда. Развој овог стандарда је тесно повезан са стандардом *ISO 9001*, са којим је компатибилан, и од кога је преузео и P-D-C-A циклус сталног унапређења.

Политика система менаџмента за безбедност информација, заједно са циљевима система менаџмента за безбедност информација и дефинисаним мерама на унапређењу система у погледу побољшања безбедности информација чине P -

---

[667] *Ibid*., стр. 107.

[668] *ISO 27002,* http://www.iso27001/security.com/html/iso27002.html

[669] Српска верзија овог стандарда под ознаком SRPS ISO/IEC 27001 *Информационе технологије - Технике безбедности - Системи менаџмента безбедношћу информација – Захтеви*, објављена је 3. новембра 2011. Према: Институт за стандардизацију Србије, http://www.iss.rs/news/news_33.html

[670] *ISO 27001*, ISMS requirements, http://www.iso27001/security.com/html/iso27002.html

планирај циклус за безбедност информација према стандарду *ISO 27001*. На основу исказаних захтева корисника, и кроз успостављање политике *ISMS,* организација улази у фазу успостављања, односно планирања система за управљање безбедношћу информација. У овој фази спроводе се активности на дефинисању критеријума за оцену ризика, дефинише се прилаз и методологија за оцену ризика и дефинишу нивои прихватљивости ризика.

Следећа фаза је спровођење планираног, односно акција на примени оног што је постављено као циљ. То је део D - *уради*, који подразумева структуру и одговорности, обуку, свест и компетентност, документацију и контролу докумената, контролу над операцијама и спремност на реаговање у ванредним ситуацијама. Трећа фаза је преиспитивање *ISMS-a* на основу дефинисаних процедура за преиспитивање, мерење ефективности управљачких механизама, спровођење интерних провера, ажурирање планова за снижавање ризика и др. Циклус C - *проверавање* се састоји од праћења и мерења, вредновања усаглашености, корективних и превентивних акција, управљања записима и интерних провера система. Четврта фаза је A - *делуј*, и остварује се кроз преиспитивање од стране руководства које заокружује цео циклус, и враћа га на планирање, што све треба да резултира континуираним побољшањем.

Поред поменутих стандарда објављени су, са аспекта управљања безбедношћу података у рачунарским системима, следећи значајни стандарди:

- *ISO 27004 – Information Security Management Metrics and Measurement*. Намењен је да помогне организацијама у мерењу и извештавању о ефикасности њихових система за управљање сигурношћу података обухваћених поступцима управљања сигурношћу (дефинисаних у *ISO 27001*) и контролама (обухваћених у *ISO 27002*).
- *ISO 27005 – Information Security Risk Management.* Објављен је 2009. године. Базира се на британском стандарду *BS 7799-3* који је објављен у марту 2006. године. Наведени стандард обухвата процену ризика, спровођење одговарајућих контрола, надгледање и поновну процену ризика у току рада или периодично, одржавање и стално унапређење система контроле итд.

Група стандарда *ISO 27000* је значајана за све организације које се баве услугама у областима које су на било који начин повезане са информационим технологијама и које имају потребу за очувањем поверљивости информација. Његова

имплементација и примена омогућавају бољу сарадњу са сличним организацијама широм света које послују по овом моделу. Овим стандардом организације демонстрирају својим корисницима да је пословна политика усмерена на стална побољшавања у систему менаџмента за безбедност информација. Значајне су користи које модел за уређење система за безбедност информација *ISO 27001* остварује код свих који га усвоје, пре свега у смислу побољшавања организационих перформанси. Овај модел представља најбољу праксу у области заштите и безбедности информација, која је преточена у захтеве стандарда. Добити од имплементације су следеће:

- Код корисника се ствара поверење у информациони систем организације;
- Обезбеђује се да организација има потпуно комплементаран систем са правном регулативом која је везана за информационе токове;
- Обезбеђује се систем који је усмеренна јасна континуална побољшања којима се обезбеђује информациона безбедност;
- Овим системом се остварује транспарентност у пружажу услуга и менаџмент на високом нивоу;
- Обезбеђује се систем који је посебно орјентисан на управљање ризиком, и кроз управљање на смањење ризика на најмању могућу меру;
- Обезбеђује се боље разумевање информационих токова у организацији;
- Смањују се трошкови;
- Остварује се лакши процес мониторинга;
- Могуће је повећати превентивно дејство кроз смањење „уских грла“ у мрежи итд.

Важно је нагласити да је планирање и избор кадрова, њихово стручно усавршавање и безбедносно образовање од изузетног значаја са аспекта заштите информационих система. У претходним одељцима рада смо нагласили да је људски фактор, у том смислу, пресудан јер безбедност у највећој мери зависи од корисника система. Сврха свих безбедносних процедура је у томе да корисници схвате значај заштите ресурса и да узму учешћа у њиховој заштити.

Упознавање корисника рачунарских система са разноврсним претњама из спектра кибер ратовања и техникама извршења напада, представља први корак у формирању безбедносне културе у овој области. Рудиментарни кораци у овој области су постигнути онда када корисници рачунара увиде да су рачунарски системи рањиви, да могу бити злоупотребљени, да информације могу бити украдене

или уништене те да за то они могу сносити одговорност. Едукација о безбедности информационих система се спроводи у појединим државама, на различитим нивоима, у зависности од степена развијености јавне свести, потреба и нивоа знања. У САД се, на пример, едукација о безбедносним претњама спроводи већ на предшколском узрасту, док се проблем заштите информационих система изучава у оквиру различитих академских специјалистичких смерова. Слично је и у Руској Федерацији где се, у оквиру акредитованих програма на више од сто факултета, изучавају следеће области:

- Криптографија;
- Компјутерска безбедност;
- Организација и технологија заштите информација;
- Заштита сложених информатизованих објеката;
- Комплексно обезбеђење информационе безбедности аутоматизованих система, и
- Информациона безбедност телекомуникационих система.[671]

5.2.1.3. Стратегије заштите

С обзиром на бројност и разноврсност средстава и техника кибер ратовања, у пракси није могуће реализовати одбрану и заштиту нападнутих система на универзално применљив начин. Из тог разлога, потребно је стратешки развијати програме који би повећали могућности за детекцију, реакцију и опоравак од кибер напада. Овакви програми би били од посебног значаја за безбедност државе и подразумевали би истраживање у три кључне области: заштита информација и информационо-комуникационих мрежа, системи C3I за брзе одговоре и фузија информација.[672]

Постизање задовољавајућег степена заштите информација и информационо-комуникационих мрежа захтева осмишљено спровођење активности на побољшању аутентификације (спречавању неауторизованих корисника да приступе систему и нанесу штету), детекције нападача (откривању упада споља и изнутра), одржавања

[671] Ковачевић Ж., *op. cit*., стр. 88.

[672] Цигурски О.: *Информационе технологије у борби против тероризма*, Зборник Факултета цивилне одбране, Београд, 2005, стр. 180.

функционалности система који је оштећен у нападу (унапређење пројектних решења која испуњавају овај захтев) и опоравку система (деконтаминација система и враћање система у првобитно стање). Осим тога, пожељно је развијати и имплементирати софтверске алате који непрекидно тестирају исправност рада информатичких средстава. Свака компутерска и мрежна компонента мора имати уграђену функционалну компоненту која је непрекидно тестира и осигурава безбедно функционисање, као и заштиту од злоупотреба.[673]

Системи C3I (*енгл*. command, control, communication, intelligence) за брзе одговоре су осимшљени са циљем повећања координисаности безбедносних служби у ванредним ситуацијама. Ови системи треба да повећају међусобну повезаност и тиме побољшају комуникацију, сарадњу и координацију различитих државних и приватних безбедносних институција. Системи C3I су базирани на употреби информатичке технологије и користе се за сортирање, вредновање, филтрирање и интеграцију информација које потичу из различитих извора.

Фузија различитих видова информација је веома битна у превенцији, детекцији и одговору на различите врсте субверзивних активности, укључујући и кибер ратовање. Унапређене могућности за прикупљање, интегрисање и интерпретацију велике количине података могу помоћи доносиоцима одлука и обавештајним службама на пољу супротстављања безбедносним претњама. Екстракција података (*енгл*. data mining) представља технологију за анализирање и селекцију одговарајућих форми података из велике количине прикупљених или текућих података.[674] Ови, екстраховани подаци (из мноштва различитих и неструктурираних формата података као што су: текст, слика, говор, видео, и то на различитим језицима), по унапред задатој форми, користе се као подршка у доношењу одлука и предузимању превентивних активности на заштити информационих система и, уопште, критичних инфраструктура.

---

[673] *Ibid*., стр. 181.

[674] Џигурски О., *op. cit*., стр. 182.

5.2.2. Компјутерска етика као вид превенције конфликата у кибер простору

Са аспекта превентивног деловања и заштите информационих система, посебну пажњу заузима изградња и развој етичких норми и принципа у домену информатике. Успостављање и развој ових норми и принципа је од изузетног значаја, јер они могу пронаћи примену у свим оним случајевима нарушавања безбедности који нису у супротности са правом али се перципирају као неприхватљиво понашање.

Посматрано из историјске перспективе, прва етичка питања у вези са компјутерима поставила су се у деценијама након Другог светског рата, мада су она у то време била нејасно дефинисана. Једно од њих било је питање да ли рачунари доводе у сумњу нашу представу о томе шта значи бити човек, будући да су способни за рационално мишљење које се сматрало искључиво људским доменом.[675] Тада су у центру етичког дискурса била расправе о вештачкој интелигенцији, а био је присутан и страх да би компјутери могли да преузму од људи доношење одлука. Међутим, може се рећи да та рана питања о рачунарима нису имала етички карактер у строгом смислу речи. Нико, у том смислу, није експилицитно тврдио да је неморално наставити са развојем компјутера зато што они угрожавају нашу представу о људском бићу.

Крајем седамдесетих година прошлог века етички проблеми постају јасније формулисани. У том периоду актуелни су били они проблеми који су се односили на питања улоге владе и великих организација, питања приватности са њима у вези, као и на питања доминације инструменталне рационалности.[676]

Са настанком персоналних рачунара пажња је преусмерена на њихов демократични аспект. Пажња бива усмерена на софтвер и на етичка питања која се јављају у вези са њим. Будући да је софтвер имао велику тржишну вредност појавила су се питања у вези са својином – да ли софтвер треба да буде у нечијем власништву и, ако треба, на који начин? Истовремено са питањима својинских права, појавила су се и питања опште и законске одговорности као и одговорности хакера.

---

[675] Џонсон Д., *op. cit*., стр. 16.
[676] *Ibid*., стр. 17.

Током деведесетих година прошлог века пажња је преусмерена на Интернет. Развој и све већа употреба Интернета довели су до, наизглед, бескрајног низа етичких питања, пошто је Интернет временом попримао све значајнију примену у различитим доменима живота. Истовремено, Интернет је покренуо и сва важна питања из прошлости попут питања приватности, демократичности, својинских права итд.[677] Глобални опсег комуникације многих са многима, анонимност и могућност репродукције су црте комуникације на Интернету које стварају низ могућих предности и потешкоћа. Пред организацијама које спроводе урађивачку политику на Интернету стоји изазов да, до максимума, остваре позитивне потенцијале ове технологије и да, истовремено, ограниче могућности за њену злоупотребу. Изазов се, између осталог, састоји у томе да се приступи решавању проблема криминала и злоупотребе на Интернету, а да се за то примене стратегије које не би умањиле моћ коју он пружа појединцима.

Разматрајући везу између технологије и етике, Дебра Џонсон долази до закључка да је, кроз историју, поље компјутерске етике напросто следило развој компјутерске технологије. У историјском смислу, дакле, поље компјутерске етике је било реактивно у односу на технологију – компјутерски етичари су пратили технолошки развој и тек накнадно реаговали на њега. Свакако да би било боље када би технологија следила етику. Тада би се, сигурно, посвећивало више пажње оним технологијама које повећавају степен заштите приватности корисника рачунарских система.

Чињеница је да развој технологије отвара нове могућности, а те нове могућности је потребно евалуирати што је задатак аксиологије, филозофске дисциплине која вредносну сферу сматра не само темељном етичком него и онтолошком и спознајном сфером. Осим тога, нове технологије стварају вакуум у прописима. Задатак компјутерске етике јесте да испуни тај вакуум. У извесном смислу, етичка питања већ сама по себи представљају вакуум у прописима, а такви вакууми настају кад год дође до развоја или неке нове примене компјутерске технологије.

Компјутерска етика спада у поље практичне етике, а управо је практична етика оно средишње поље на коме се апстрактне етичке теорије суочавају са пролемима и одлукама из стварног света. Потребно је много времена како би се

---

[677] *Ibid*., стр. 18-19.

разумео значај теорија за стварне животне ситуације, проблеме и одлуке. У извесном смислу, теорије и не можемо разумети докле год не схватимо шта оне подразумевају о стварним животним ситуацијама. Практичну етику је, због тога, најбоље схватити као домен у коме теорија и пракса „преговарају“. Јер ако се ослањамо на моралне појмове и теорије, ми морамо и да их тумачимо и да трагамо за њиховим импликацијама у конкретним ситуацијама са којима се суочавамо. У практичној етици делујемо у оба правца – и од теорије ка контексту, и од контекста ка теорији. А често једна теорија или више њих осветле неко практично питање, док у другим случајевима хватање у коштац са практичним проблемом доводи до новог теоријског увида.[678]

5.2.3. Правна регулатива конфликата у кибер простору – национална законодавства и међународноправни документи

Осмишљавање и примена примарних система заштите рачунара и рачунарских мрежа представљали су, и данас представљају, незаобилазне и неопходне активности на пољу превенције. Међутим, проблеми везани за заштиту информационих система перманентно се усложњавају, а њихове димензије се непрекидно увећавају. На данашњем степену развоја информационо-комуникационих технологија проблеми превазилазе реалне могућности њиховог успешног и целовитог разрешавања само инжењерским методима и „алатима“ расположивим у оквиру информатике. Због тога се тежиште разрешавања све више помера ка секундарном и терцијарном нивоу заштите, тј. активностима које се спроводе на националном и међународном плану.

Историјски посматрано, појачана перцепција претње за критичну информациону инфраструктуру, која се испољила у другој половини претходне деценије, узроковала је покретање иницијатива за њихову заштиту.[679] Прве иницијативе су покренуте на нивоу држава, да би се питање заштите информационе инфраструктуре убрзо промовисало и на међународном нивоу.

Паралелно са овим активностима, у међународној заједници је сазревала свест о томе да се проблему заштите информационих инфраструктура мора приступити синергијски, уз ангажовање свих расположивих превентивних и

[678] *Ibid*., стр. 25.

[679] Видети одељак „Критична информациона инфраструктура као објект кибер рата“.

репресивних средстава. У том смислу, указала се потреба за доношењем правне регулативе у овој области, чији би механизми требало да повећају вероватноћу постизања жељеног стања безбедности информационе инфраструктуре. Ово је имало последицу да правни аспект заштите информационих система, у најширем смислу, постане један од приоритетних задатака правних система, не само на националном, већ и на међународном плану.

5.2.3.1. Законска регулатива конфликата у кибер простору

Све технолошки развијене земље света предузимају мере за супротстављање деликтима у кибер простору. Правосудни системи појединих држава су веома сложени и обухватају много више од кривичних закона. То илуструје и кратак преглед кривичних и других закона који регулишу кибер криминал у појединим, развијеним, земљама.

Упоредна анализа законодавстава у Сједињеним Америчким Државама, Великој Британији, Француској, Немачкој, Италији, Јапану, Русији и Кини приказана је у Табели 14.

Табела бр. 14*: Упоредна анализа националне регулације кибер криминала*

КРИВИЧНА ДЕЛА	**НАЗИВ ДРЖАВЕ**							
	САД	**В. Британија**	**Француска**	**Немачка**	**Италија**	**Јапан**	**Русија**	**Кина**
Заштита приватности	+	+	+	+	+	+	+	+
Интелектуална својина	+	+	+	+	+	+	+	+
Дечја порнографија	+	+	+	+	+	+	+	+
Оштећење рачунарских података и програма	+	+	+	+	+	+	+	+
Рачунарска саботажа	+	+	+	+	+	+	+	+
Прављење и уношење рачунарских вируса	+	+	+	-	+	+	+	+
Рачунарска превара	+	+	+	+	+	+	-	+
Неовлашћен приступ заштићеном рачунару или рач. мрежи	+	+	+	+	+	+	+	+
Неовлашћено коришћење рачунара или рач. мреже	+	+	+	+	+	+	+	+

Извор: Вулетић Д.: *Cyber криминал и могућност његовог откривања*, докторска дисертација, Факултет политичких наука, Београд, 2008, стр. 96.

Анализом законодавства и предузетих активности, може се утврдити да су све развијене државе предузеле одређене активности у циљу стварања услова за сигурно окружење, односно регулацији кибер криминала. Међународна сарадња и процесна питања у борби против кибер криминала регулисани су Конвенцијом Савета Европе о кибер криминалу. Међународна сарадња, пак, регулисана је посебним законима у Великој Британији и Русији.

У законодавствима наведених држава приватност појединаца је регулисана посебним законима.

У свим анализираним државама, рачунарски софтвери су заштићени као ауторски радови и у том сегменту постоји значајан ниво хармонизације. Томе су значајно допринеле имплементације европске *Директиве о заштити ауторског права (2001/29/EC)* и споразуми Светске организације за интелектуалну својину (World Intellectual Property Organization - WIPO).

По питању кривичних дела везаних за рачунаре уочљиво је постојање великог степена хармонизације. Томе је у великој мери допринела и *Конвенција Савета Европе о кибер криминалу*. У законодавству Русије не постоје одредбе које се експлицитно односе на *рачунарску превару* док у законодавству Немачке не постоје одредбе које регулишу *прављење и уношење рачунарских вируса.*

Осим Русије и Немачке све остале анализиране државе имају посебне законе којима се регулише слање нежељене електронске поште.[680]

5.2.3.1.1. Сједињене Америчке Државе

Сједињене Америчке Државе су потписале Конвенцију о кибер криминалу 23. новембра 2001. године а ратификовале су је 29. септембра 2006. године.

Амерички председник Бил Клинтон је још 1998. године, у извештају о *Стратегији за контролу кибер криминала* истакао неодложност брзог доношења законског оквира против кибер криминала будући да „кибер криминалци могу да користе рачунаре да нападају наше банке или да изнуђују новац под претњом да ће

[680] Према: Вулетић Д.: *Cyber криминал и могућност његовог откривања*, Докторска дисертација, Факултет организационих наука, Београд, 2008, стр. 97.

употребити рачунарске вирусе“. Осим тога, Клинтон је нагласио да су САД у првим борбеним редовима те битке, али да „међународни кибер криминал захтева и међународни одговор и да ниједна нација не може сама контролисати кибер криминал.“[681]

Закон о приватности (*Privacy Act*) усвојен је 1974. године. Доношење овог закона било је иницирано сазревањем свести о томе да приватност појединаца може бити директно угрожена од стране федералних агенција, прикупљањем, одржавањем, употребом и дистрибуцијом података о личности.[682] 2007. године Конгрес је констатовао да је угрожавање приватности увећано и све већом злоупотребом ИК технологија. Због тога поглавље 508 Закона регулише услове и правила под којима агенције могу нарушити приватност грађана.[683]

Закон о приватности електронских комуникација (*Electronic Communications Privacy Act*) из 1986. године садржи одредбе које регулишу приступ, коришћење, прислушкивање и заштиту приватности жичних, усмених и електронских комуникација. Законом се забрањује неовлашћен приступ као и обелодањивање комуникационих садржаја. Закон спречава владине институције да захтевају податке од Интернет провајдера без одговарајуће законске процедуре.[684]

Закон о комуникационој пристојности (*Communications decency act*) из 1996. године садржи посебне одредбе које регулишу одговорност провајдера Интернет услуга. За непристојно, узнемиравајуће и незаконито коришћење телекомуникационе опреме предвиђена је новчана казна или затворска казна до две године, односно и новчана и затворска казна - одељак 501 и 502. Приватност информација корисника регулисана је у одељку 702 где се наводи, између осталог, да телекомуникациони оператер има обавезу да сачува поверљивост података о кориснику.[685]

---

[681] Вирилио П.: *Информатичка бомба*, Светови, Нови Сад, 2000, стр. 132-133.

[682] Electronic Privacy Information Center, http://www.epic.org

[683] *Privacy Act*, http://www.usaid.gov/policy/ads/500/508.pdf

[684] *Electronic Communications Privacy Act*, http://www.legal.web.aol.com/resources/legislation/ ecpa.html; www.cpsr.org/issues/privacy/ecpa86

[685] *Communications Decency Act*, http://www.cpic.org/free.speech/CDA/cda.html

Национална стратегија за обезбеђење кибер простора (*US cyberspace strategy*) из 2003. године[686] дефинише почетне циљеве за организацију и додељивање приоритета за заштиту у кибер простору. Стратегија даје смернице министарствима и агенцијама које имају своју улогу у обезбеђењу кибер простора. Такође указује на кораке које локалне власти, приватне компаније, организације и грађани треба да предузму да би побољшали колективну безбедност кибер простора. Стратегија истиче и значај сарадње државног и приватног сектора.

Међу стратегијске циљеве Националне стратегије за обезбеђење кибер простора убрајају се:

- Спречавање кибер напада на америчке критичне информационе инфраструктуре;
- Смањење рањивост на нападе у кибер простору и
- Минимизирање штете и времена потребних за опоравак након напада.

Национална стратегија за обезбеђење кибер простора јасно идентификује пет националних приоритета:

- Безбедносни систем за одговор на националном нивоу;
- Програм за смањење рањивости у кибер простору;
- Национални програм за подизање нивоа свести о угрожености кибер простора и програм обуке;
- Обезбеђивање владиног кибер простора и
- Безбедносна сарадња на националном и међународном нивоу.

Од 1980. године рачунарски софтвер у Сједињеним Америчким Државама је заштићен *Законом о заштити рачунарског софтвера ауторским правом* (*Computer Software Copyright Act*).[687] Са становишта интелектуалне својине веома је значајан и *Дигитални миленијумски закон о ауторским правима* (*Digital Millenium Copyright Act*), донет 1998. године који у суштини представља имплементацију WIPO уговора (споразума). Садржи одредбе којима се спречава приступ радовима заштићених ауторским правом, мере којима се спречава копирање радова заштићених ауторским правом као и мере којима се штити интегритет управљања информацијама заштите

[686] *US cyberspace strategy*, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
[687] *Computer Software Copyrigh Act*, http://www.ladas.com/Patents/Computer/Copyright.USA.html

ауторских права (*copyright information management*). Наведеним документом се ограничава одговорност провајдера Интернет услуга за кршење ауторских права.[688]

Усвајањем *Закона о повећању кибер безбедности* (*Cyber Security Enhancement Act - CSEA*) предвиђена је могућност изрицања казне затвора учиниоцима кибер криминала.[689]

Контролисање напада нежељених порнографских и маркетиншких порука (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 или CANSPAM Act of 2003) ступио је на снагу 1. јануара 2004. године. У Документу се закључује:

- Влада има интерес да регулише питање комерцијалне електронске поште у целој земљи;
- Пошиљаоци комерцијалне електронске поште не смеју доводити у заблуду примаоце по питању извора или садржаја такве поште и
- Примаоци комерцијалне електронске поште имају право да одбију пријем накнадне електронске поште од истог извора.[690]

Значајну улогу у борби против кибер криминала, има и Министарство правде Сједињених Америчких Држава (*Department of Justice – DoJ*).[691]

Министарство правде се састоји од великог броја бироа, уреда и управа као што су *Управа за криминал* (*Criminal Division*)*, Федерални истражни биро* (*Federal Bureau of Investigation - FBI*) и Национални централни биро Интерпола. Од посебног значаја је *Национални институт павде* (*National Institute of Justice*) који се бави истраживањима, израдом статистичких извештаја, развојем и проценом различитих алата који се користе у истрази случајева кибер криминала.

У *Федералном истражном бироу* је смештен *Национални центар за заштиту инфраструктуре* (*National Infrastructure Protection Centre - NIPC*), у

---

[688] *Digital Millenium Copyright Act*, http://www.copyright.gov/legislation/dmca.pdf

[689] *Cyber Security and Enhancement Act*, http://www.usdoj.gov/criminal/cybercrime/homeland_ CSEA.htm

[690] Термин комерцијална електронска пошта представља неку електронску поруку првенствено намењену за комерцијално оглашавање или промоцију производа или услуга. CANSPAMAct, http://www.spamlaws.com/federal/can-spam.shtml

[691] Министарство је одговорно за: примену закона и заштиту интереса САД; остваривање јавне безбедности од страних и унутрашњих претњи; руковођење у превенцији и контроли криминала на федералном нивоу; изрицање одговарајућих казни за лица која су проглашена кривим; спровођење националних имиграционих закона; обезбеђење правичног и непристрасног дељења правде за све грађане. Према: Department of Justice, http:// www.usdoj.gov

Вашингтону, с циљем да се обезбеди, на националном нивоу, прикупљање информација о опасностима које прете инфраструктури, укључујући рачунарске и друге системе. Најважнији задатак тог Центра је да изгради „мост поверења“ како би олакшао размену информација између приватног сектора и грађана у погледу пријављивања и заштитних мера. *Национални центар за заштиту инфраструктуре* обавља свој рад користећи различите информационе ресурсе. Систем *NIPC Watch* одржава целодневно присуство у *Центру за стратегијске информације и операције* (*Strategic Information and Operations Center - SIOC*) FBI, који упућује упозорења на три нивоа и обезбеђује саветодавне услуге у случају значајне опасности. Да би се осигурала потпуна координација, у *Националном центру за заштиту инфрастритктуре* запослени су представници органа реда као и других америчких служби. NIPC сарађује и са иностраним безбедносним службама на размени релевантних информација.[692]

Одреди FBI за кибер криминал, који су распоређени на шеснаест локација широм САД, такође размењују своје информације са *Националним центром за заштиту инфраструктуре.* Главну иницијативу FBI представља програм *InfraGard*.[693] Овај програм заснован је на партнерству између Министарства правде, рачунарске индустрије, академских кругова, државних и локалних служби органа реда. Намењен је за обезбеђење критичних делова инфраструктуре на националном нивоу.[694]

Федерални истражни биро прикупља податке од локалних криминалистичких агенција и служби добијањем различитих извештаја. У покушају израде *Националог прегледа кибер криминала* у САД је урађен јединствен програм извештавања (*Uniform Crime Reporting - UCR*). Локалне криминалистичке службе (преко 18 хиљада) сакупљају и месечно шаљу податке. Подаци се интегришу и објављују као *званична национална статистика криминала* (*official national crime statistics*) и приказују на сајту Бироа. Касније је програм проширен и преименован у *Национални систем извештавања о инцидентима* (*National Incident-Based Reporting*

---

[692] Вестби Џ.: *Међународни водич за борбу против компјутерског криминала*, Продуктивност АД, Београд, 2004, стр. 140-141.

[693] InfraGard, http://www.infragard.net

[694] Вестби Џ., *op.cit*., стр. 140-141.

System - NIBRS) у којем су дела разврстана у различите категорије. Систем извештавања о инцидентима специфицира податке и прослеђује их до Федералног истражног бироа.[695]

Национално одељење за компјутерски криминал (*National Computer Crime Squad - NCCS*), у оквиру FBI, спроводи истрагу компјутерских превара и злоупотреба које обухватају и упад у владине, финансијске и друге виталне рачунарске системе.

Веома важан закон у супротстављању кибер криминалу јесте и *Закон о рачунарским преварама и злоупотребама* (*Computer Fraud and Abuse Act - CFAA*).[696] Као одговор на терористичке нападе од 11. септембра 2001. године и проблеме кибер криминала, Конгрес САД је изменио делове тог Закона усвајањем *Закона о уједињењу и јачању Америке одговарајућим инструментима за спречавање и сузбијање тероризма* из 2001. године (*PatriotAct*).[697] *Изменама Закона о рачунарским преварама и злоупотребама* обухваћене су рачунарске преваре и сличне активности против заштићених рачунара, или оне које су настале њиховом употребом. „Заштићени рачунар“ је, према том Закону, „рачунар или рачунарски систем који користи финансијска институција, влада САД или који се користи у међудржавној трговини.“[698]

Према Закону о рачунарским преварама и злоупотребама, кривично дело чини:

- Приступ рачунару без одобрења, или избегавање одобрења ради приступања поверљивим информацијама које се тичу спољних односа или одбране државе.
- Приступ рачунару, без одобрења, или избегавање одобрење да би се добиле информације које се односе на финансијске или кредитне институције, о државним управама или органима или информације из заштићеног рачунара уколико се он користи за међудржавну комуникацију.

---

[695] Shinder D.: *Scene of the Cybercrime: Computer Forensic Handbook*, Syngress Publishing, Rockland, 2002, p. 37-49.

[696] *Computer Fraud and Abuse Act*, http://www.usdoj.gov/ criminal/cybercrime/1030_new.htrnl

[697] *Patriot Act*, http://thomas.loc.gov/cgi-bin/bdquery/z7dl07:HR03162:TOM:/bss/dl07qu-cry.litnil

[698] Вестби Џ., *op.cit*., стр. 51.

- Намеран приступ без одобрења било ком рачунару владе САД који није јавног типа или било ком рачунару који не користи искључиво америчка државна управа или орган али му се приступа да би се извршио утицај на његово коришћење од стране државе.
- Приступ заштићеном рачунару без одобрења и намерно вршење преваре у вредности од 5.000 америчких долара или више, за период од једне године.
- Пренос или покушај преношења програма, информација или команде без одобрења чиме се намерно наноси штета заштићеном рачунару; Намеран приступ или покушај приступа заштићеном рачунару, без одобрења, и несмотрено наношење штете. Штета представља укупан губитак од најмање 5.000 америчких долара за годину дана, при чему се узима у обзир вредност стварне штете проузроковане неовлашћеним преносом или приступом, трошкови враћања система на претходно стање, као и друге предвидљиве штете.
- Незаконита трговина информацијама које могу да се искористе да би се стекао неовлашћен приступ заштићеним рачунарима, уколико таква незаконита трговина утиче на међудржавну трговину, или дати компјутер користи влада САД.
- Пренос саопштења које прети да изазове штету заштићеном рачунару, у покушају да се изнуди новац или нека корист.[699]

За наведена дела запрећена је новчана казна, затворска казна или и једно и друго. Уколико је починилац већ био осуђиван за неко дело које је предвиђено *Законом о рачунарским преварама и злоупотребама* затворска казна може износити и до двадесет година.[700]

Свесно уношење програма, информације, кода или команде услед чега се с намером проузрокује штета на заштићеном рачунару кажњиво је према америчком кривичном закону, део 1030 *Преваре и сличне активности везане за рачунаре*.[701]

Закон о рачунарским преварама и злоупотребама је допуњен одељком 1037 - Преваре и повезане активности у вези са електронском поштом (Fraud and related

---

[699] *Computer Fraud and Abuse Act*, *op.cit*.

[700] Вестби Ц., *op.cit*., стр. 51-54.

[701] *Fraud and Related Activity in Connection with Computers*, http://www.usdoj.gov\criminal\cybercrime\1030NEW.lUm

uctivity in connection with electronic mail), за које је запрећена казна затвора до пет година, новчана казна или и једно и друго.

С циљем да олакша коришћење електронских записа и потписа у трговини, валидност и правни основ примене електронских уговора, амерички Конгрес је, 2000. године, усвојио документ *Електронски потписи у глобалној и националној трговини* (*Electronic Signatures in Global and National Commerce Act*). Конгрес је наметнуо посебне захтеве за компаније које желе да користе електронске записе или потписе у трансакцијама. Између осталог, од компаније се захтева да добије сагласност потрошача да им доставља информације у електронској форми где је закон регулисао да то буде у писаној форми.[702]

5.2.3.1.2. Руска Федерација

Законом о информацијама, информатизацији и заштити информација (*Law on Information, Informatization and Protection of Information*) из 1995. године, члан 11, подаци о личности се сврставају у категорију поверљивих информација. То значи да се забрањује прикупљање, чување, употреба или дистрибуција података о личности без сагласности лица на кога се подаци односе, без одлуке суда.[703]

Законом Руске Федерације о правној заштити рачунарских програма и база података (број 3523-1 из 1992. године односно допуњени Закон број 177-ФЛ из 2002. године) рачунарски програми и базе података заштићени су као ауторски радови.[704]

Закон о комуникацијама из 2003. године[705] представља правну основу за активности у подручју комуникација. Закон регулише надлежности владиних институција у сфери комуникација, права и одговорности особа које учествују у тим активностима или користе комуникационе услуге. Садржи одредбе које се тичу

---

[702] *Electronic Signatures in Global and National Commerce Act*, http://www.ftc.gov/os/2001/06/es-ignreport.pdf

[703] *Law on Information, Informatization and Protection of Information*, http://www.fas.org/irp/world/russia/docs/lawjnfo.htm

[704] *Law of the Russian Federation on the Legal Protection of Computer Programs and Databases*, http://www.fips.ru/ruptoen2/law/pr_db.html

[705] *Law on Communications*, http://english.minsvyaz.ru/docs/FED.doc

заштите комуникационих мрежа, повезивања са јавним телекомуникационим мрежама, контроле од стране Владе, обавезе провајдера Интернет услуга и заштите права корисника комуникационих услуга.

Кривични закон Руске Федерације, у посебној глави под насловом *Криминал у сфери компјутерске информације* регулише следеће:[706]

Члан 272 *Неовлашћени приступ компјутерској информацији.* Неовлашћено приступање законом заштићеној информацији на рачунару или мрежи, уколико на тај начин дође до уништења, блокирања, модификације или копирања информације, прекида (поремећаја) рада рачунара или рачунарске мреже, биће кажњиво, за основни облик: вредношћу 200-500 просечне цене рада, или личног дохотка или другог дохотка од два до пет месеци, или друштвено корисним радом од шест до дванаест месеци, или лишењем слободе до две године.

Уколико је дело извршено од стране групе лица у завери, организованих група или особа које су злоупотребиле службени положај, казне су у износу од 500-800 просечне цене рада, или личног дохотка или другог дохотка од пет до осам месеци. Казна може обухватити и друштвено користан рад до две године, или лишење слободе до пет година.

Члан 273 *Прављење, употреба и дистрибуција штетних рачунарских програма.* Прављење рачунарских вируса ради промене већ постојећих програма које свесно доводи до уништења, блокирања, модификације, или копирања информације, ометања рада рачунара или рачунарске мреже, као и коришћење или ширење таквих вируса или медија са таквим програмима биће кажњиво: лишењем слободе до три године, новчаном казном у вредности 200-500 просечне цене рада, или личног дохотка или другог дохотка од два до пет месеци. Уколико је дело изазвало теже последице, запрећена је казна затвора од три до седам година.

Члан 274 *Повреда прописа експлоатације рачунара, система рачунара и рачунарских мрежа.* Кршење прописа експлоатације рачунара или мреже, од стране лица које има приступ и ако је изазвало уништење, блокирање или модификацију законом чуване информације рачунара и проузроковало озбиљну штету, биће

---

[706] *The Criminal Code of the Russian Federation*, http://www.russian-criminal-code.com

кажњиво, за основни облик: забраном вршења основне делатности до пет година, или обавезним радом од 180-240 сати, или лишењем слободе до две године. Уколико је дело изазвало теже последице, запрећена је казна затвора до четири године.

Иако је било више покушаја, тј. нацрта закона да се регулише *спем* у Русији (*Регулација руског сегмента на Интернету*, *Правна регулација пружања Интернет услуга*, *Електронска трговина*) још увек није донет одговарајући закон који регулише ту област. Наведеним нацртима предлагано је да нежељена комерцијална електронска пошта мора бити прецизно и недвосмислено означена.[707]

Закон о електронском дигиталном потпису број 1-ФЗ из 2002. године, регулише употребу електронских докумената, њихов пренос путем Интернета и др. Наведеним Законом се регулише да електронски потпис не може бити употребљен за потписивање електронских докумената упућених владиним органима.[708]

Са аспекта међународне сарадње у решавању проблема кибер криминала веома је значајан *Закон Руске Федерације о учешћу у међународној размени информација* из 1996. године који је усвојен у циљу заштите националних интереса у процесу међународне размене информација као и заштите права, слобода и интереса физичких и правних лица. Законом се регулишу државна одговорност и ограничења, права власника информације, обезбеђење заштите за грађане, правна лица и државне органе од неистинитих и фалсификованих информација, као и координација, контрола и одговорност у међународној размени информација. Приступ комуникационим мрежама је регулисан у складу са *Законом о комуникацијама.*[709]

5.2.3.1.3. Народна Република Кина

Регулација управљања Интернет услугама електронске поште (*Internet Email Service Management Regulations*) регулише приватност грађана који користе услуге електронске поште путем Интернета. Наведени Закон примењује се у

---

[707] *Law and Internet: Legal aspects of SPAM in Russia*, http://www.russianlaw.net/english/ae06.htm; *Russian law makers to fight spam*, http://www.gateway2russia.com/st/art_244487.php; *Russia Says "Nyet" to Anti-Spam Law*, http://www.lockergnome.com/nexus/net/ 2005/02/03/ru-ssia-says-nyet-to-anti-spam-laws

[708] *Electronic Digital Signature Law*, http://www.byakernet.com/ecommerce/russia-t.htm

[709] *Russian Federation Federal Law on Participation in International Information Exchange*, http://www.privacyexchange.org/legal/nat/omni/nol.html

Народној Републици Кини од 30. марта 2006. године и њиме се забрањује слање комерцијалне поште без претходне сагласности примаоца, а у случају сагласности пошиљалац је дужан да прецизно назначи да је реч о комерцијалној електронској пошти као и валидне информације о контакту. Чланом 9 провајдери се обавезују да чувају поверљивост података корисника као и електронске адресе корисника. Чланом 10 провајдери се обавезују да чувају 60 дана податке о времену послате и примљене електронске поште као и електронске и IP адресе пошиљаоца и примаоца.[710]

У октобру 2000. године Министар информационе индустрије објавио је *Регулативу о управљању информационим услугама везаним за Интернет* (*Internet Information Services Management Regulations*) у циљу контроле коришћења Интернета. Наведеним законом се захтева од провајдера Интернет услуга да надгледају садржај и блокирају контроверзне материјале. Поред тога они се обавезују да чувају 60 дана садржаје као и листу корисника који су им приступали.[711]

Регулатива о рачунарским мрежама и информационој безбедности, заштита и управљање (*Computer Information Network and Internet Security, Protection and Management Regulations*), члан 7 изражава слободу и приватност мрежних корисника. Према том Закону *Биро државне безбедности* (*Public Security Bureau*) има задатак да надгледа провајдере Интернет услуга и других комерцијалних предузећа који имају кориснике с Интернет приступом. Према члану 8 појединци и институције укључени у Интернет пословање морају прихватити надгледање и управљање од стране *Бироа државне безбедности.* Биро захтева од тих структура месечне извештаје о броју корисника, броју посећених web страница, профил корисника и др. Провајдери се такође обавезују да сарађују у истрази са Бироом у случају кибер криминала.[712]

Телекомуникациона регулација (*Telecommunications Regulations*) усвојена је 11. новембра 2000. године с циљем заштите права и интереса претплатника, заштите

---

[710] *Internet Email Service Management Regulations*, http://www.cdt.org/international/censorship/20060220chinaspam.pdf

[711] *Internet Information Services Regulations*, http://www.usembassy-china.org.cn/sandt/netreg2000.html

[712] *Computer Information Network and Internet Security, Protection and Management Regulations*, http://newmedia.cityu.edu.hk/kiberlaw/gp3/pdf/law_security.pdf

телекомуникационих мрежа и информација и помоћи развоја телекомуникационе индустрије. Чланом 6 се регулише да појединцима и организацијама није допуштено да користе телекомуникационе мреже у активностима које угрожавају националну безбедност, државне интересе или законска права и интересе појединаца.[713]

Поред наведених, у Народној Републици Кини су предузете и активности са циљем раујашњења и праћења кибер криминала, односно његових појединих облика.[714]

Народна Република Кина је чланица WIPO од 1980. године. Године 1990. усвојени су *Закон о заштити ауторских права Народне Републике Кине* (*Copyright Law of the PRC*) који је допуњен 2001. године и *Примена правила за заштиту ауторских права Народне Републике Кине* (*Implementing Rules for the Copyright Law ofthe PRC*) који је допуњен 2002. године. *Регулатива о примени међународних споразума о заштити ауторских права* (*Regulations on Implementation of International Copyright Treaties*) усвојена је 1992. године. Рачунарски софтвери у Народној Републици Кини су заштићени као литерарни радови од 1991. године *Регулативом о заштити рачунарских софтвера* (*Regulations on Computer Software Protection*).[715]

Сходно *Закону о заштити ауторских права Народне Републике Кине,* од 1. марта 2005. године на снази је *Регулација о колективном управљању заштитом ауторских права* (*Regulations on Collective Management of Copyright*). Тим Документом су прецизиране активности *Организација котективног управљања заштитом ауторских права* (*Copyright Collective Management Organizations – CCMO*), тј. управљање заштитом ауторских права у корист власника као што је нпр. помоћ у парници.[716]

Мере административе заштите ауторских права на Интернету (*Measures on Administrative Protection of Internet Copyright*) у Народној Републици Кини

---

[713] *Telecommunications Regulations*, http://www.cnii.com.cn/20020808/ca91368.htm

[714] Вулетић Д., *op. cit*., стр. 114.

[715] *China's Copyright Regulations*, http://www.wipo.int/export/sites/www/about-ip/en/ipworldwide/pdf/cn.pdf

[716] *Regulations on Collective Management of Copyrights*, http://www.law-lib.com/law/ law vicw.asp?id=87904, www.ipsmart.cn/view_article.php?article_id=110&article_sortid=2&sort_ supcrid=2

усвојене су 30. априла 2005. годино, а примењују се од 30. маја 2005. године. Мере су у складу са *Законом о заштити ауторских права Народне Републике Кине,* а односе се на садржаје у Интернет информационим услугама. Уколико провајдер Интернет услуга сазна да су одређени садржаји који су предати путем Интернета заштићени ауторским правом дужан је да одмах уклони такве садржаје, а о свему сачува евиденцију 60 дана (члан 5).[717]

Регулацијом о заштити рачунарских информационих система (*Regulations on Safeguarding Computer Information Systems*) усвојеној у фебруару 1996. године, прописује се да државни органи безбедности треба да упозоре или новчано казне од 5.000 до 15.000 јуана појединце или организације ако рачунарски вируси или остали подаци, свесно убачени у систем, оштећују рачунарски систем (члан 23).[718]

Кривични закон Народне Републике Кине,[719] од 14. марта 1997. године прописује следеће:

Чланом 252 је регулисано кршење права комуникационих слобода грађана. Скривање, уништавање или отварање туђе поште кажњиво је затворском казном или условно до једне године.

Члан 285 - Ко прекрши државне прописе и упадне у рачунарски систем може се казнити затворском казном или условно, до три године.

Члан 286 - Ко прекрши државне прописе и обрише, измени, дода или поремети рачунарски систем, проузрокујући неправилан рад система и теже последице, биће кажњен казном затвора или условно, до пет година. Ко прекрши државне прописе и обрише, измени или дода податке или корисничке програме проузрокујући теже последице, намерно прави и умножава рачунарске вирусе који нарушавају нормалан рад система и проузрокује теже последице биће такође санкционисан истом казном.

---

[717] *Measures on Administrative Protection of lnternet Copyright*, http://www.chinaitlaw.org/?pl=regulations&p2=051006180113.

[718] *ReguIations on Safeguarding Computer Information System*, http://ftp.fas.org/irp/world/ china/clocs/computer_code.htm

[719] *Criminal Law of the People's Republic of China*, http://cybercrimelaw.net/laws/countries/ China.html

Члан 287 - Ко користи рачунар за превару, крађу, корупцију, проневеру државних фондова, крађу државних тајни или других облика криминала биће кажњен према одговарајућим одредбама тог закона.

5.2.3.2. Међународноправни оквири сарадње и проблем правног статуса кибер конфликата

Правна регулација кибер криминала одвија се на више колосека. Поред националне, све је заступљенија и међународна регулација кибер криминала, односно неких од његових облика. Паралелно са тим, и саморегулација покушава да се избори са овом појавом. Занимљиво је да се последњих година знатно више активности одвија на међународном плану него на националном и саморегулационом плану. То је донекле и природно, с обзиром на природу деликата у кибер простору.[720]

Још 1983. године у оквиру OECD-а усвојена је *Студија о међународној примени и хармонизацији кривичног права везаног за проблеме компјутерског криминала и злоупотреба*, три године касније публикован је документ под називом *Криминал везан за компјутере: анализа и правна политика*. Период од 1999. године обележило је континуирано издање збирки приручника за безбедност информационих система којима се успостављају правила и утврђују основе њеног постизања.

Најзначајнији и најбројнији међународни акти донети су у оквиру Европске уније. Тако је 1996. године започела *Заједничка акција против расизма и ксенофобије*, 1997. донета је *Препорука о анонимности субјеката на Интернету* и *Декларација о глобалним рачунарским мрежама*, 1998. сачињен је *Предлог о оквирима спречавања сексуалне експлоатације и трговине људским бићима*. Пар година касније доноси се и посебан акт везан за кибер криминал (*Communication on Cybercrime*).[721] *Студија о правним аспектима компјутерског криминала у*

---

[720] Приликом израде прегледа међународних правних аката аутор се руководио чланком: Дракулић М., Дракулић Р.: *Cyber криминал*, 2005, http://www.bos.org.yu/cepit/drustvo/sk/cyberkriminal.

[721] Communication from the Commission to the Council, The European Parliament, The Economic and Social Committee and Committee of the regions, Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, http://europa.eu.int

информационом друштву[722] објављена је 1998. године и она, у комбинацији са документима са Лисабонског састанка Европског савета 2000. године, представља смернице за активности везане за разумевање феномена кибер криминала.

Акциони план (*eEurope Action Plan*) из исте године везан је за активност обезбеђења сигурности мреже и успостављања сарадње земаља чланица и њиховог заједничког приступа кибер криминалу до 2002. године. Исте године доноси се и *Предлог правног оквира одлучивања везаног за нападе на информационе системе* (*Proposal for a Council Framework Decision on attacks against information systems*). Годину дана касније документ је допуњен одредницама о „недозвољеном приступу информационим системима" и „недозвољеном ометању система и података". Године 2000. донета је и *Директива о електронском пословању* (*Directive on electronic commerce*), у којој се посебна пажња посвећује проблему злоупотреба.[723] Те године се доноси и читав скуп различитих аката, од *Одлуке Савета о спречавању дечје порнографије на Интернету*, *Конвенције о међусобној помоћи у кривичној материји* до *Препоруке о стратегији за нови миленијум* у заштити и контроли компјутерског криминала.[724]

Потом следи акт којим треба да се обезбеди сигурније информационо друштво кроз безбедност информационе инфраструктуре и борбу против криминала везаног за рачунаре (*Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*). У домену процесних права, која треба да истражним и правосудним органима олакшају прикупљање и валоризовање података о учињеним делима и починиоцима, Европска унија је 2000. године донела *Конвенцију о међусобној помоћи у кривичној материји* (*Convention on Mutual Assistance in Criminal Matters*), којом се предвиђа не само сарадња већ и усклађивање правних и правосудних система земаља чланица. Ове одредбе требало би да олакшају институционализовање сарадње која се мора

---

[722] *Legal Aspects of Computer-related Crime in the Information Society – COMCRIME*, http://europa.eu.int/ISPO/legal/en/crime/crime.html

[723] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain aspects of Information Society services, in particular electronic commerce, in the Internal Market, http://europa.eu.int

[724] *The Prevention and control of organised crime: A European Union strategy for the beginning of the new millennium* (OJ 2000 C124, 3. 5. 2000).

успоставити између одговарајућих органа гоњења различитих земаља, као и међународних полицијских организација. Сарадња се очекује и са релевантним институцијама корисникâ, органâ за супервизију заштите података, као и индустрије.

Савет Европе је крајем 1998. године започео активности на доношењу *Конвенције о кибер криминалу* (*Convention on Cybercrime*), чији је предлог априла 2000. године пуштен у процедуру јавне расправе. Она је данас један од најзначајнијих докумената који су, поред европских земаља, прихватили и Јапан, САД, Канада и Јужна Африка. Конвенцију, која је ступила на снагу у јулу 2004. године, прате бројни документи донети у оквиру Савета: *Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime* (2002); *Cyber-Rights & Cyber-Liberties, Advocacy Handbook for NGOs* (2003); *Racism Protocol to the Convention on Cybercrime* (2003); *The Protocol to the Cybercrime Treaty* (2002); *Additional Protocol to the Cybercrime Convention Regarding "Criminalization of Acts of a Racist or Xenophobic Nature Committed through Computer Networks"*; *Report Revised Draft of the Protocol on Racist Speech* (2002); *Background Materials on the Racist Speech Protocol*; *Draft Protocol on Racist and Xenophobic Speech: Preliminary draft* (2001); *Second Protocol on Terrorism* (2002).

У оквиру групе Г8 од 1997. године (када је предложен *Акциони план борбе против кибер криминала*, а усвојеног 1998), на предлог експертске групе за кооперацију на пољу правде и унутрашњих послова, министри правде и унутрашњих послова у више наврата су расправљали о принципима те борбе. Између осталог, расправљало се и о нужности међународне сарадње у спровођењу истрага и хватању починилаца, као и о прихватању стандарда дефинисаних у Конвенцији Савета Европе. Ова организација је донела следеће акте: *Recommendations for Enhancing the Legal Framework to Prevent Terrorist Attacks*; *Recommendations on Special Investigative Techniques and Other Critical Measures for Combating Organized Crime and Terrorism*; *Recommendations for Sharing and Protecting National Security Intelligence Information in the Investigation and Prosecution of Terrorists and Those Who Commit Associated Offenses: Best Practices for Network Security*; *Incident Response and Reporting to Law Enforcement*; и друге.

Уједињене нације су, такође, имале бројне активности и донеле одговарајуће акте који су директно или посредно били везани за решавање проблема кибер криминала. Поред њих, одређеним аспектима или типовима овог криминала баве се

и друге међународне организације, какве су Светска организација за интелектуалну својину, Међународна привредна комора, Светска трговинска организација и Азијско-пацифичка организација за економску сарадњу.

5.2.3.2.1. Иницијативе и програми за заштиту критичне информационе инфраструктуре

Сједињене Америчке Државе су прве формализовале акције на нивоу владе на тему заштите критичних инфраструктура доневши, 1998. године, Председничку директиву о заштити критичне инфраструктуре (*President Decision Directives – PDD 63*).[725] Од тада су многе друге информатизоване државе развиле акције које су имале циљ да:

- схвате елементе критичности и рањивости различитих инфраструктура државе;
- дефинишу стратегије за смањивање тих рањивости;
- подстакну развој сензибилитета код јавних или приватних оператера у погледу проблема заштите критичних инфраструктура;
- осмисле и развију планове за кризне ситуације и послекризни опоравак;
- да подстакну развој суштински сигурних технологија;
- подрже међународну сарадњу.

Због транснационалне природе претње, проблематика заштите критичних информационих инфраструктура (Critical Information Infrastructure Protection – CIIP) већ је дуже време у центру пажње различитих међународних организација. У Паризу је марта 2003. године одржан први састанак експерата земаља Г8 на тему заштите критичних информационих инфраструктура, на којем су скицирани принципи који би требало да инспиришу политике различитих земаља ради постизања виших нивоа заштите. Са циљем да фаворизују међународну сарадњу, али и за добробит земаља које нису чланице, Г8 је публиковала *Приручник за заштиту критичних*

[725] Затим је уследило формирање Националног центра за заштиту инфраструктуре (National Infrastructure Protection Center – NIPC), Центра за анализу и размену информација везаних за критичну инфраструктуру у власништву приватног сектора (Information Sharing and Analysis Center – ISAC) и формирање Удружења експерата заинтересованих за заштиту информационих система (Infagard). Током 2003. године Бушова администрација је објавила *Националну стратегију за обезбеђење кибер простора* (National Strategy to Secure Cyberspace), документ који има за циљ обавезивање америчке владе на борбу против кибер тероризма и других кибер претњи.

информационих инфраструктура на међународном нивоу (*International CIIP Directory*), са указивањем на структуре и додирне тачке института земаља чланица ради ношења са проблематиком питања везаних за заштиту критичних информационих инфраструктура.[726]

На проблемима у пољу заштите критичне инфраструктуре рад је 2005. године започела и Европска комисија унутар истраживачких пројеката: *Технологије информационог друштва* (*Information Society Technologies – IST*) и *Припремне активности у истраживању безбедности* (*Preparatory Action on Security Research*). Ови пројекти се данас реализују уз финансијску подршку Европске комисије из буџета Седмог оквирног програма (*Framework Programmes* – FP 7). Један од три основна технолошка сектора које евидентира Европска комисија у области информационо-комуникационих технологија јесте инфраструктура мобилне, бежичне, оптичке и широкопојасне комуникације, као и информатичке и софтверске технологије. Приоритетни стратешки циљ на пољу технологија информационог друштва представља оријентација истраживања „према глобалној слици поузданости и безбедности". Комисија узима у задатак, између осталог, развој помоћних инструмената у процесу одлучивања, са циљем зашите критичних инфраструктура ради превенције претње и смањивања рањивости, узимајући у обзир зависност друштва од информационо-комуникационих технологија.

Већ у оквиру Петог оквирног програма (FP 5), унутар приоритетâ информационо-комуникационих технологија, Европска комисија је с пажњом третирала проблеме везане за критичне информационе инфраструктуре. Резултат те активности била је *Европска иницијатива поузданости* (*European Dependability Initiative – DEPPY*).[727] На овом пољу је, такође, започета серија истраживачких и развојних пројеката на тему *поузданости*[728] система и сервиса информационог друштва и, у скорије време, на тему анализе ризика и рањивости критичне информационе инфраструктуре, као и међусобне зависности ове и осталих

---

[726] Dunn M., Wigert I.*: International CIIP Handbook 2004*, Center for Security Studies, ETH Zürich, 2004.

[727] Извор: Servida A.: *Towards a Dependable Information Society: from DEPPY to FP6*, European Commission, http://groups.inf.ed.ac.uk/safecomp/Download/safecomp2002/servida_safecomp2002.pdf

[728] Поузданост (*енгл*. dependability) информационог система треба да оправда указано поверење у услуге које обезбеђује систем. Поузданост подразумева следеће атрибуте: расположивост, физичку обезбеђеност, поверљивост, интегритет и одрживост. Према: http://www.cert.org.

критичних инфраструктура. Осим тога, промовисана је међународна сарадња стварањем институције *EU–US Joint Task Force on R&D for CIP*.[729]

Током 2004. Комисија је извршила припремну акцију у пољу истраживања безбедности, са циљем да започне глобални програм након 2007. године. Припремна активност представља допринос Комисије свеобухватнијој агенди Европске уније у вези с одношењем према изазовима и претњама Европи, што је илустровано, између осталог, у документу *Европске стратегије за безбедност*, који је прихватио Савет Европе децембра 2003. године.

Европска комисија је осмислила пет пројеката у вези са заштитом од терористичких атентата, од којих се један фокусира на истраживање у пољу критичних информационих инфраструктура. Наслов пројекта је *Оптимизација безбедности и заштите умрежених система*, а његов циљ је анализа безбедности коришћења садашњих и будућих умрежених система, попут система комуникације, јавне управе, саобраћајне инфраструктуре, трговине и пословања, испитујући њихове слабе тачке и међусобну зависност ради евидентирања начина реализације безбедносних мера против физичких претњи и кибер претњи. Приоритети у овој мисији су:

- развој стандардизованих методологија и инструмената одлучивања ради процене природе потенцијалне претње и њених слабих тачака;
- демонстрација мера за побољшање заштите и безбедности јавних, приватних и државних критичних елемената инфраструктуре у проширеној Европској унији;
- развој способности откривања, превенције, одговора и упозорења ради повећања безбедности информационих система и система контроле, уз интегрисано коришћење сателитских, фиксних земаљских и бежичних система.

На политичком и регулативном нивоу Комисија је од 2001. године започела дефинисање европског односа према безбедности мрежа и информација, што је довело до стварања *Европске агенције за безбедност мрежа и информација* (ENISA). Агенција има циљ да осигура висок ниво безбедности мрежа Европске

[729] Servida A.: *Towards a Dependable Information Infrastructure for the EU*, European Commission, http://www.safety-club.org.uk/resources/128/AServida.pdf

уније, да развија културу у области безбедности мрежа и информација, и да подстиче одговорност код свих актера јавног и приватног сектора.

Значајан је и предлог Комисије Европског парламента упућен Савету, Економском и социјалном комитету и Комитету регија у јуну 2001. под насловом *Безбедност мрежа и безбедност информација: предлози за стратешки европски однос*. У овом документу су скициране потенцијалне претње и врсте могућих напада против мрежа, као и модели за противодговор. Дана 12. јула 2002. донета је директива 2002/58/CE, која се тиче третирања личних података и заштите приватности у сектору електронске комуникације. Ова норма је у потпуности заменила претходну директиву 97/66/CE. Потреба за редефинисањем претходне директиве појавила се услед еволуције технологија у протеклих пет година, те, самим тим, и повећања ризика за приватност корисника.

На оперативном нивоу Комисија је одобрила акциони план *eEurope 2005*. План дефинише две синергијске категорије интервенција. Прва се односи на јавне онлајн сервисе и на сервисе електронског пословања, а подразумева стимулисање ових сервиса, апликација и садржаја. Друга интервенција треба да подржи стварање базичне инфраструктуре за примену широкопојасне (large band) технологије и да пажљиво размотри аспекте везане за њену безбедност.

Организација за економску сарадњу и развој (OECD) објавила је 2002. године у облику Препоруке Савета *Водич за кибер безбедност*, који представља важан оријентир у овој материји. У њему су дате нове смернице, упућене нарочито предузећима, операторима и индивидуалним корисницима. Примена следећих принципа од стране свих учесника у мрежи треба да допринесе повећању безбедности кибер простора:

- „Повећати осетљивост на проблем – корисници кибер простора морају бити свесни неопходности заштите информационих система и мрежа и активности које могу да предузму ради повећања њихове безбедности.“ Разумевање проблема је неопходан корак у концепту кибер безбедности: неопходно је упознати ризике којима су изложени властити системи и мреже, као и развијати свест о томе да се безбедносни инциденти лако преносе с једног дела мреже на други, с обзиром на глобалну повезаност и међузависност система. Пажња се мора усмерити и на упознавање сопственог система и неопходних корака за повећање безбедности, и на

предузимање одговарајућих мера како би се спречило да систем буде опасан по друге системе.[730]

- „Одговорност – заинтересоване стране су одговорне за безбедност информационих система и мрежа.“ Ово је аспект који се не односи само на кориснике система већ и на „оне који системе пројектују и развијају, а кориснике снабдевају производима и услугама“, с обзиром на то да се безбедност кибер простора добрим делом заснива на солидности и поузданости производа, те зависи од понашања оних који пружају услуге широј јавности.[731]
- „Одговор – заинтересоване стране морају да делују тренутно и кооперативно ради превенције, откривања и одговора на безбедносне инциденте.“ Инциденти у кибер простору могу се брзо раширити, па је неопходно спровођење тренутне акције у кооперацији са свим заинтересованим странама из различитих земаља.
- „Етика – заинтересоване стране морају поштовати легитимне интересе осталих страна.“ У међусобно повезаном свету акција или изостанак акције једне стране може да нанесе штету другим странама. Развијање и примена одговарајућих пракси, заснованих на етички прихватљивом понашању, на пољу кибер безбедности представља морални императив.
- „Демократија – безбедност система и информационих мрежа мора бити компатибилна са основним вредностима демократског друштва.“ Безбедност се мора осигурати уз поштовање вредности демократског друштва, посебно слободне размене мисли и идеја, токова информација, поверљивости информација и комуникације, приватности, отворености и транспарентности.
- „Евалуација ризика – заинтересоване стране морају да процене ризик.“ Уопштено говорећи, анализа и евалуација ризика, у процесу управљања ризиком, омогућавају препознавање претњи и рањивости повезаних скупом „основних спољашњих и унутрашњих фактора, дакле технологија, физичког и људског фактора, политике и услуге трећих лица чија умешаност утиче на безбедност.“ Захваљујући овим инструментима може се одредити степен прихватљивости ризика и могу се усвојити одговарајуће противмере.

---

[730] На пример, успостављањем система антивирусне контроле одлазне електронске поште.

[731] Успостављање правне одговорности продаваца производа који садрже рањивости у великој мери би допринело смањењу несигурности кибер простора, сматра и експерт у овој области Брус Шнајер. Према: Schneier B.: *Liability changes everything*, http://www.schneier.com

- „Разумевање и примена безбедносних стандарда – заинтересоване стране морају да укључе безбедносне стандарде као есенцијалан елемент информационих система и мрежа.“ То значи да, у суштини, безбедност представља елемент који се мора узети у обзир од тренутка пројектовања неког система или производа.
- „Управљање безбедношћу – заинтересоване стране морају да усвоје глобални приступ управљања кибер безбедношћу.“ Менаџмент на подручју безбедности мора се заснивати на евалуацији ризика, мора бити динамичан и глобалан, како би обухватио све нивое активности заинтересованих страна и све аспекте њиховог деловања. Менаџмент мора да антиципира и да пружи одговор на хитне претње, да превенира инциденте и да на њих одговори, успостави поновну функционалност система и да их перманентно одржава и контролише. Безбедносне политике везане за информационе системе и мреже (праксе, активности и процедуре у пољу безбедности) морају бити интегрисане и координиране ради стварања кохерентног система безбедности.
- „Реевалуација – заинтересоване стране морају да испитају и поново процене безбедност информационих система и мрежа како би увеле одговарајуће промене у своје политике, праксе, акције и безбедносне процедуре.“ Нове рањивости се константно откривају, што захтева да се скуп мера и процедура везаних за кибер безбедност непрестано анализира ради верификовања њихове делотворности у новим околностима.

Организација уједињених нација је, са своје стране, више пута нагласила важност политика које имају за циљ побољшање безбедности информационе инфраструктуре. Заштита критичних инфраструктура, као засебна тема, разматрана је на 78. заседању УН, у децембру 2003. године. Том приликом је усвојена резолуција под називом „Стварање глобалне културе кибер безбедности и заштита критичне информационе инфраструктуре“ (*Creation of global culture of cyber security and the protection of critical information infrastructures* – A/RES/58/199).

Резолуција истиче како се све већа повезаност критичних инфраструктура са информационом инфраструктуром претвара у повећану рањивост комплетног система. Одатле произлази неопходност примене мера које имају за циљ формирање и припремање тимова стручног особља на плану смањења ризика, смањењу последица од евентуалних штетних догађаја и реализацији потоњих операција реактивирања угрожених система. Резолуција, дакле, позива земље чланице да током дефинисања властитих стратегија узму у обзир једанаест „Елемената за заштиту критичних информационих инфраструктура“ (*Elements for protecting critical*

information infrastructures), који, у суштини, понављају принципе које је разрадила Г8 у марту 2003. године. За разлику од препорука OECD-а, резолуција Уједињених нација је посебно упућена владама држава чланица и, нарочито, њиховим оружаним снагама.[732]

5.2.3.2.2. Проблем правног статуса кибер конфликата

Ако се у обзир узму катастрофалне последице које кибер напади могу изазвати, од виталног је значаја да државе буду оспособљене да ефикасно одбране своју критичну инфраструктуру од напада. Најефикаснији начин за одбијање кибер напада је употреба слојевитог система одбране, састављеног од мера активне и пасивне одбране.[733] У пракси, државе намерно бирају искључиво мере пасивне одбране, делимично из страха да би коришћењем мера активне одбране прекршиле међународно ратно право.

Међутим, за активности које називамо кибер ратовањем, иако се оне спроводе већ више од десет година, у међународном ратном праву још увек није пронађена адекватна дефиниција. У овом тренутку, дакле, не постоји свеобухватни међународни споразум који би регулисао кибер нападе, тј. пружио неку правну дефиницију чина кибер агресије. Заправо је целокупно поље кибер права још увек недовољно развијено.

Шеф Стратешке команде Сједињених држава, генерал ваздухопловства Кевин Чилтон (Kevin P. Chilton), најавио је још 2009. године да ће се међународно ратно право применити на ову област.[734] Још увек није познато да ли су са овим

---

[732] *The UN Resolution on CIIP*, UK National Infrastructure Security Co-Ordination Centre, *The Quarterly*, No. 2, February 2004, http://www.niscc.gov.uk

[733] Мере активне одбране су електронске мере контранапада које су осмишљене тако да узврате напад рачунарским системима који нападају и затворе канал кибер напада. Безбедносни експерти могу подесити мере активне одбране тако да аутоматски одговоре на нападе против критичних система, или их могу активирати мануелно. Највећим делом, мере активне одбране су поверљивог карактера, иако су програми који шаљу деструктивне вирусе назад ка непријатељским машинама или преплављују подацима рачунар нападача. Мере пасивне одбране су традиционалне форме рачунарске безбедности које се користе за заштиту рачунарских мрежа, као што су контроле приступа систему, контрола приступа подацима, одржавање безбедности и дизајн безбедног система.

[734] Schogol J.: "Official: No Options 'off the table' for U.S. Response to Cyber Attacks", *Stars and Stripes*, May 8, 2009, http://www.stripes.com/news/official-no-options-off-the-table-for-u-s-response-to-cyber-attacks-1.91319

ставом сагласне и друге државе, посебно Руска Федерација и Народна Република Кина.

Амит Шарма (Amit Sharma), изасланик шефа Центра за проучавање одбране и безбедности при Министарству одбране Индије, заступа другачији приступ, онај који је настао према моделу нуклеарног застрашивања: „Можете причати у недоглед о закону о оружаном сукобу, али споразум неће бити постигнут.... Једина одржива солуција је кибер застрашивање.“[735]

Према писању *Њујорк Тајмса* од 28. јуна 2009.: „Русија фаворизује међународни споразум попут оних постигнутих преговорима о хемијском наоружању, и агитовала је за такав приступ на бројним скуповима ове године као и у јавним изјавама високих званичника.

САД тврде да споразум није неопходан. Уместо тога, оне заговарају бољу сарадњу међународних агенција за спровођење закона. Уколико ове групе сарађују тако да учине кибер простор безбеднијим у погледу криминалних активности, њихов рад ће учинити кибер простор сигурнијим и у погледу војних кампања.“[736]

Због правне нерегулисаности ове области државе су, у пракси, стављене пред избор да ли ће изједначавати кибер нападе са традиционалним оружаним нападима и одговарати на њих према међународном ратном праву, или ће кибер нападе изједначавати са криминалним активностима и одговарати на њих у складу са домаћим кривичним законима и међународним конвенцијама о кибер криминалу. Став који преовладава међу државама и правним експертима је да државе морају да третирају кибер нападе као криминална дела: 1) због несигурности поводом тога да ли се кибер напад може сматрати оружаним нападом, и 2) због тога што међународно ратно право захтева од држава да припишу оружани напад некој страној влади или њеним актерима пре него што одговоре силом.

НАТО координациони центар за кибер одбрану и подршку (NATO Cooperative Cyber Defense Centre of Excellence - CCDCOE) објавио је чланак на ову тему у новембру 2008. године, под називом „Кибер напади на Грузију: извучене

---

[735] Carr J., *op. cit*., p. 31.

[736] Markoff J., Kramer A.: “U.S. and Russia Differ on a Treaty for Cyberspace”, *The New York Times*, June 28, 2009, http://www.nytimes.com/2009/06/28/world/28cyber.html

правне поуке.“ У њему аутори разматрају могућности примене међународног ратног права на кибер нападе који су се појавили током Руско-грузијског конфликта, августа 2008. године. Аутори наведеног чланка сматрају да се у основи проблема налази питање одређења садржине и обима појма *кибер агресија*. Шта би под овим појмом требало подразумевати? Да ли би овај појам обухватио сва или само нека од наведених тумачења:

- Кибер агресија подразумева нападе на владине, кључне државне или цивилне Интернет странице или мреже без пратеће војне силе;
- Кибер агресија се односи на нападе усмерене против политичких неистомишљеника унутар државе;
- Кибер агресија означава нападе на критичну инфраструктуру и мреже;
- Кибер агресија се може поистоветити са кибер шпијунажом.[737]

Да ли неко од наведених одређења адекватно дефинише чин кибер агресије? Сва? Ниједно? Да ли дефиниција кибер агресије треба да садржи одредницу да мора постојати одговорност (противничке) државе за извршени напад? Да ли се појмови *кибер агресија* и *кибер рат* могу синонимно употребљавати?

Треба нагласити да у праву не постоји појам ратног чина, било да се ради о традиционално схваћеном рату било да је реч о кибер рату или неком другом ратном конфликту. Повеља Уједињених нација одређује када суверена држава може да употреби силу у циљу самоодбране од чина агресије, али се то у потпуности односи на оружани сукоб. Други споразуми би можда могли да обезбеде бољи оквир за успостављање појмовног одређења кибер агресије.

Један покушај у том правцу учињен је у чланку Скота Шеклфорда (Scott Shackleford) iz 2009. године под називом „Од нуклеарног до Интернет рата: успостављање аналогије са кибер нападима у међународном праву”.[738]

Шеклфорд набраја неколико уговорних режима који могу послужити у конструисању међународног кибер споразума: *Споразум о нешириењу нуклеарног*

---

[737] Tikk E., et. al.: *Cyber Attacks Against Georgia: Legal Lessons Identified*, Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia, November 2008, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

[738] Shackleford S.: “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law,” *Berkeley Journal of International Law*, Vol 27, No 1, 2009, pp. 192-251.

наоружања, *Међународно космичко право*, *Систем антарктичке повеље*, *Конвенција Уједињених нација о праву мора* и *Уговори о узајамној правној помоћи*.

Уговори о нешириењу нуклеарног наоружања. Уговори о нешириењу нуклеарног наоружања настали су са циљем спречавања ширења производње нуклеарног оружја већ у почетним фазама, тј. на ступњу нуклеарног реактора. Они су последњи пут коришћени у Ирану након што је он одбио да у потпуности сарађује са Међународном агенцијом за атомску енергију (International Atomic Energy Agency - IAEA).

Уговори о нешириењу нуклеарног наоружања су делотворни јер су компоненте које учествују у стварању нуклеарног уређаја строго забрањене и пажљиво надгледане од стране IAEA као и различитих влада и њихових агенција за праћење ових активности.

Када су у питању средства кибер ратовања ствари стоје другачије. Целокупна техника која је нападачу потребна за извршење напада се навелико дистрибуира и може се набавити по веома ниској цени. Та чињеница у старту обесмишљава евентуалну примену оваквог типа споразума о нешириењу наоружања с циљем да се државе спрече у развијању способности кибер ратовања.

И поред тога што су званичници САД-а и Руске Федерације склони претеривању у изјавама по питању размера и пропорционалности одговора на кибер нападе великих размера,[739] чињеница је да ниједна страна нема јасну политику којом би се та питања регулисала.

С правом се може поставити питање да ли кибер напад може да се подигне на ниво нуклеарног напада? Не сам по себи, али кибер напад довољно великих размера који уништава главне мреже и стога изазива систематско уништавање

[739] На пример: „Русија задржава право да користи нуклеарно оружје против средстава и сила информационог ратовања а онда и против саме земље агресора" (пуковник В. И. Тсимбал, 1995); кибер ратовање је „блиски сусрет треће врсте иза ширења наоружања за масовно уништење и употребе нуклеарног, биолошког и хемијског оружја од стране терориста" (бивши директор ЦИА-е John Deutch, 1996). Према: Carr J., *op. cit*., p. 33.

безбедносних система нуклеарних електрана, би могао имати разорне последице, међу којима и губитке живота.[740]

Међународно космичко право и Систем антарктичке повеље. Кибер простор се често упоређује са свемиром пошто су оба неограничена и нерегулисана законом. Међународно космичко право не забрањује коришћење свемира као платформе за тестирање оружја, осим по питању употребе нуклеарног наоружања. Употреба ове врсте наоружања забрањена је међународним уговором као што је забрањено и одлагање таквог оружја на неко планетарно тело. Међутим, правни вакуум између ове две категорије наоружања још увек није регулисан.

Једна од препрека у примени ове аналогије на кибер ратовање огледа се у томе да мали број нација има могућност, или може очекивати да ће бити у могућности, да ратује у свемиру. Са друге стране, преко 120 нација данас има могућност вођења рата у кибер простору.

Други проблем приметан је у разлици у потенцијалу претње кибер напада у поређењу са лансирањем нуклеарног оружја из свемира. Нема таквог кибер напада који може проузроковати штету еквивалентну штети изазваној неким нуклеарним оружјем иако се, теоретски, употреба огромног ботнета који укључује милионе зомби рачунара може, бар приближно, сматрати Интернет еквивалентом нуклеарног напада.

Алтернатива забрани одређеног типа оружја у неком подручју је забрана свог оружја у датом подручју, по принципу Антарктичке повеље из 1959. године. Овим уговорним режимом, Антарктик је ван домашаја свих облика војних активности од стране било које нације и користи се само у мировне, превасходно, научно-истраживачке сврхе.

По свој прилици, ни овај уговорни режим не може послужити као модел за регулисање кибер ратовања. На првом месту због тога што је немогуће направити разлику између информатичког кода који се користи у мировне сврхе и оног који се користи у негативне сврхе.

---

[740] Подсетимо се вируса Stuxnet који је септембра 2010. године заразио рачунаре иранске нуклеарне електране Бушер. Вирус је био креиран тако да је могао да заустави рад електране и доведе до хаварије великих размера. Према: Мишић М.: „Нова фаза сајбер-ратовања“, Дневни лист *Политика*, 06.10.2010, стр. 3.

Још један проблем са антарктичком аналогијом је у томе што кибер простор нема видљивих граница нити има поузданих начина да се оне вештачки повуку.[741]

Конвенција Уједињених нација о праву мора (*The United Nations Convention on Law of the Sea - UNCLOS*). Право мора и међународних вода одређено је *Конвенцијом Уједињених нација о праву мора*. Ова Конвенција представља споразум који је усвојила *Трећа конференција Уједињених нација о праву мора* (UNCLOS III) и ступила је на снагу 1994. године.[742] По свом пространству су мора и океани, као и свемир, слични кибер простору. Сликовито би се то могло приказати на следећи начин:

Схема бр. 8: *Унутрашњи, територијални и међународни кибер простор*

741 Један од скорашњих напада на Интернет странице влада САД и Јужне Кореје потекао је са сервера на тлу САД преко VPN конекције са сервером у Уједињеном Краљевству. Сервер у Британији је био контролисан од стране командних и контролних сервера стационираних на територији других држава са којих је напад и започет. Безбедносна служба Јужне Кореје, пак, била је убеђена да је напад иницран из Северне Кореје. Ту погрешну процену подржала је целокупна штампа и један амерички конгресмен. Конгресмен је затражио од војске САД да узврати кибер напад Северној Кореји. Да је то учињено, односи у међународној заједници би данас вероватно били много заоштренији. Према: Carr J., *op. cit*., p. 34.

742 Прва конференција УН-а о праву мора (UNCLOS I) одржана је 1958. у Женеви. UNCLOS I резултирала је усвајањем четири конвенција. Иако је UNCLOS I сматрана успешном, оставила је неколико битних питања нерешеним, пре свега ширину територијалног мора.

Друга конференција УН-а о праву мора (UNCLOS II) одржана је 1960. Међутим, ова конференција није резултирала нити једним новим споразумом. Опште говорећи, земље у развоју и земље трећег света учествовале су на овој конференцији само као савезници САД-а и СССР-а, без значајнијег властитог доприноса.

Трећа конференција УН-а о праву мора сазвана је 1973. године у Њујорку, и трајала је до 1982., уз учешће 160 држава. Како би се спречио покушај да одређене групе држава доминирају преговорима, конференција је доносила одлуке консензусом, избегавајући примену система већине. Резултат UNCLOS III је Конвенција о праву мора. Конвенција је увела нови институт у међународно право мора - искључиви државни појас, који је већ постојао у обичајном међународном праву, али није био до краја дефинисан. Конвенцијом је предвиђено оснивање Међународне власти за морско дно, али и Међународног суда за право мора.

Према овој аналогији, унутрашњи кибер простор био би подручје у коме национална држава има потпуни суверенитет. Под територијалним кибер простором подразумевао би се део националног кибер простора у који се допушта неограничен приступ. Међународни кибер простор теже је дефинисати, али би се према аналогији са UNCLOS-ом односио на она подручја која нису под суверенитетом нити једне нације.

Међутим, проблеми везани за регулативу права мора су се појавили још током *Треће конференције* када су САД, Немачка и Уједињено Краљевство осујетиле покушаје Уједињених нација да успоставе стандарде трансфера технологије. Чини се да технологија стално нуди изазове споразумном режиму који покушава да регулише њен развој – наговештавајући на тај начин правне потешкоће настале као резултат кибер ратовања. Другим речима, ако трансфер технологије не буде регулисан *Конвенцијом Уједињених нација о праву мора*, неће бити нимало лако направити споразум о регулисању проблема кибер ратовања према његовом моделу.

Споразум о узајамној правној сарадњи (*MALT*). Споразуми о узајамној правној сарадњи могу послужити као универзални модел за споразуме о билатералној сарадњи међу државама, као што су удружени напори за спровођење закона, споразуми о екстрадицији итд. Изгледа да САД тренутно заговарају овај приступ док Руска Федерација преферира аналогију третирања кибер простора као оружја за масовно уништење и забрану његове употребе одговарајућим споразумним режимом.

Руси сматрају да проблем кибер ратовања треба да се регулише према моделу Споразума о хемијском наоружању или било ком другом споразуму о контроли наоружања, док САД заговарају спровођење међународног права у области кибер криминала и бољу сарадњу међу државама на том пољу. Многи кибер криминалци су, као недржавни актери (хактивисти), укључени у кибер конфликте тако да би ова стратегија резултирала двоструком добити - обезбеђивањем Интернета од кибер криминала и кибер ратовања.

Један аргумент Русије против става САД објављен је у московском журналу *Војна мисао* под називом „Војна политика Руске Федерације у области Међународне информационе безбедности: регионални аспект": „Међународни правни акти који регулишу односе који се јављају у процесу сузбијања кибер криминала и кибер тероризма не смеју да садрже норме које нарушавају тако безусловне принципе

међународног права као што су неуплитање у унутрашње послове других држава и суверенитет потоњих. Штавише, политички мотивисани кибер напади извршени по налогу владајућих структура се могу оквалификовати као војни злочин са свим предвиђеним процедурама истраге и кривичног гоњења злочинаца. Поред тога, војни кибер напади могу се посматрати и као предмет међународног јавног права. У овом случају, требало би да говоримо о увођењу ограничења на развој и употребу рачунара са намером изазивања негативних утицаја када су у питању ентитети кибер простора других држава.

У сваком случају, војна политика у области међународне информационе безбедности где ова укључује супротстављање кибер тероризму и кибер криминалу, требало би да буде усмерена ка увођењу међународних правних механизама који би омогућили спречавање неконтролисане и тајне употребе кибер оружја од стране потенцијалних агресора против Руске Федерације и њених геополитичких савезника.“[743]

Русија је формулисала своју политику у овој области пре 2007. године и она се до данас није променила. На руску позицију у овој области утицала су два разлога. Први разлог свакако јесте заштита националног суверенитета. Са друге стране, не би требало пренебрегнути корист коју Руска Федерација има од недржавних актера у кибер конфликтима. Досадашње искуство је показало да хактивисти (популација високообразованих, патротски настројених хакера који се радо боре у име своје државе на подручју кибер простора) представљају стратешко средство у руском кибер арсеналу.

Међународно ратно право. Занимљиво је да се Шеклфорд уопште не бави међународним ратним правом у овом есеју, што само показује колико се разликују мишљења правних стручњака који су фокусирани на ову област. Уместо тога, он потцртава тезу да је најбољи начин за смањење обима информационог ратовања, формулисање међународног споразума који би се бавио искључиво кибер нападима под покровитељством држава у међународном праву. Овакав споразум би подразумевао формирање сталног тела за реаговање у хитним случајевима које би било слично већ предложеном Глобалном рачунарском тиму за реаговање у кризним

[743] *Военная мысль*, Но. 3, Москва, 31. март, 2007.

ситуацијама. САД би требало да одбаце своје противљење таквом режиму споразума, сматра Шеклфорд: „Без једне такве организације, међународна заједница ће посртати од случаја до случаја бринући се да ће наредног пута, случај Естоније бити само корак који води ка мрежном рату v. 2.0. Када информационо ратовање достигне ступањ нуклеарног рата, биће неопходан нови и другачији режим, који ће у себи садржати елементе постојећег међународног права, особито међународног хуманитарног права јер, у супротном, нације су изложене ризику од систематских оштећења инфраструктуре који могу не само онеспособити друштва, већ врло вероватно и до темеља уздрмати информационо доба.“[744]

Ако се међународно ратно право користи као смерница за одређивање тога шта јесте а шта није кибер ратовање, напад мора имати одређена правила. Прво, међународно ратно право примењује се само у случају отпочињања оружаног сукоба. Затим, кибер инциденти који одговарају оружаном нападу морају бити такви да их је могуће приписати конкретној држави. Даље, постоји питање намере која за циљ има наношење штете. Да ли је кибер инцидент изазвао повреде или штете (монетарне, физичке, или виртуелне)?

Према експертима НАТО атрибуција, са становишта међународног права, може бити директна и индиректна: „Владајући принцип државне одговорности под међународним правом био је да се понашање недржавних актера – како ентитета, тако и особа – не може приписати држави, уколико сама држава није директно и експлицитно пребацила део својих задатака и функција приватном ентитету. Напуштање ове ригидне парадигме може се уочити у развоју ситуације током последњих година: нпр. Међународни кривични суд за бившу Југославију у случају Тадић 104, као и односом међународне заједнице према америчкој операцији *Трајна слобода* 2001. Ипак, тренутно становиште је да је за атрибуцију ипак потребан неки облик свеобухватне контроле од стране државе.“[745]

Правни преседани поменути у наведеном цитату завређују пажњу. Навешћемо оба са кратким сажетком о њиховом значају:

---

[744] Shackleford S., *op. cit*.
[745] Tikk E., et al., *op. cit*.

У случају Никарагве, Међународни суд правде навео је да се: „држава може сматрати одговорном за дела недржавних актера само уколико је имала ефикасну контролу над тим актерима. Стога, МСП не може сматрати да су САД одговорне за дела побуњеника (организација Контрас), јер САД нису имале ефикасну контролу над припадницима Контрас-а. Према наводима Суда, да би дела недржавних актера могла бити сматрана одговорношћу државе, морало би се доказати да је држава заиста имала ефикасну контролу над деловањем недржавних актера“.[746]

Случај Тадић снизио је праг за импутирање дела недржавних актера државама и закључио да: „државе само треба да имају свеобухватну контролу над недржавним актерима како би се држави приписао било који противзаконити чин актера. Међународни кривични суд за бившу Југославију сматрао је да је критеријум „ефикасне контроле“ Међународног суда правде био у супротности са самом логиком државне одговорности и да није доследан државној и правној пракси“.[747]

У поређењу са случајем Тадић, америчка операција *Трајна слобода* је на исти начин спустила праг за атрибуцију јер су САД покушале да импутирају одговорност за деловање Ал-Каиде Авганистану из простог разлога што је званични, талибански режим подржавао и штитио ту терористичку групу (без обзира на то да ли је Авганистан имао ефикасну или свеобухватну контролу). Међународна заједница је подржала приступ САД-а и одлучила да: „су према међународним инструментима напади на САД од 11. септембра 2001. представљали оружане нападе који су изазвали инхерентно право САД-а на самоодбрану. УН, НАТО и ОАС су такође приписали терористичке нападе Ал-Каиде талибанском режиму“.[748]

Након разматрања праксе међународног права по питању атрибуције, Тик се бави објашњавањем суштинског правног принципа, а то је *посредништво.* На пример, да ли је појединац деловао као посредник државе, и да ли се његово деловање може изједначити са деловањем државе? Такође, да ли би држава могла учинити нешто да спречи штетно деловање недржавног актера ако то жели?

---

[746] Jinks D.: “State Responsibility for the Acts of Private Armed Groups,” *Chicago Journal of International Law*, No 4, 2003, 83–95, p. 88.

[747] *Prosecutor v. Dusko Tadic - ICTY Case No. IT-94-1*, 1999, према: Jinks, *op. cit*., p. 88–89.

[748] Jinks D., *op. cit*., p. 86.

У случајевима кибер напада на Грузију и Естонију, Тик и њен тим закључили су да нема довољно доказа како би се показала умешаност државе, што је неопходан услов за аргументовање посредовања.

До сада, важно је нагласити, није постигнута општа сагласност о међународним споразумима који би разјаснили правни статус држава и недржавних актера у кибер конфликтима.

5.3. Могући правци развоја међународног ратног права у циљу развијања адекватнијих механизама супротстављања и заштите од кибер конфликата

У претходном одељку рада дотакли смо се неких правних питања из домена кибер ратовања која су предмет дебате међународне заједнице и правних стручњака. Намера нам је да се, у овом одељку рада, усредсредимо на једну стратегију која се бави улогом недржавних актера у кибер конфликтима између националних држава, то јест, приписивањем одговорности државама због њиховог неангажовања да спрече такво деловање и последицама које тиме настају.

Једна од најжустријих дебата из међународног права води се око питања у ком тренутку нападнута држава може легално одговорити на кибер напад. Међународно ратно право је састављено од добро познатих и прихваћених принципа, али примена тих принципа на кибер нападе представља тежак задатак. Потешкоће настају из чињенице да се међународно ратно право развило, већим делом, као одговор на „класичне“ међудржавне ратове. Из парадигме традиционалних оружаних сукоба релативно је једноставно проценити обим напада и открити идентитет нападача. Међутим, током кибер напада, нападнутој држави је тешко да процени обим напада, као и да закључи ко је за њега одговоран. У претходном одељку рада указали смо на чињеницу да су ове потешкоће довеле до тога да државе невољно одговарају на кибер нападе у самоодбрани јер се боје да не прекрше међународно ратно право. Због тога је кибер ратовање постало једна од најактуелнијих тема међународног ратног права.

Метју Склеров, капетан Морнарице САД, дао је запажен научни допринос истраживањима проблема које кибер напади постављају пред међународно ратно право и пружио аналитички оквир помоћу кога се њима може приступити.[749] Може се рећи да је став Склерова по овом питању јасан – према међународном праву државе имају право да:

- тумаче кибер нападе као чинове рата, а не само као кривична питања, те да у складу са тим и одговоре на њих;
- користе мере активне, а не само пасивне одбране против рачунарских система других држава, без обзира на то да ли су те државе иницирале напад или су само занемариле своју обавезу да спрече кибер нападе који долазе са њихове територије.[750]

Склеров сматра да је страх од употребе мера активне одбране спутавајући и штетан по државе из два разлога. Прво, будући да се мере активне одбране сматрају видом примене електронске силе, одбрана рачунарских система државе бива препуштена само мерама пасивне одбране, што доводи до слабљења дефанзивне позиције државе. Друго, оно приморава државе да се ослањају на домаће кривичне законе како би се одбраниле од кибер напада, што је неефикасно јер је неколико великих држава невољно да спроведе екстрадицију или кривично гоњење нападача. Прихватањем оваквог, преовлађујућег тумачења међународног ратног права, државе се могу наћи у „одбрамбеној кризи“ током кибер напада јер су принуђене да одлуче између ефикасних, али правно спорних мера активне одбране и мање ефикасних, али легалних мера пасивне одбране и кривичних закона.

Одбрамбену кризу, више од било чега другог, компликује атрибуциони захтев јер је у пракси немогуће било коме приписати одговорност за кибер напад током његовог трајања. Иако нападнута држава може лоцирати сервере у другој држави са којих су упућени кибер напади, утврђивање идентитета нападача захтева интензивну и дуготрајну истрагу током које је неопходна сарадња државе из које је напад иницран. Будући да међународно ратно право забрањује употребу силе све

---

[749] Џефри Кар сматра да Склеров (Matthew J. Sklerov) заступа своје ставове веома чврсто и убедљиво, и да они могу служити као одлична платформа за даљу дискусију, не само у влади САД већ и у свим владама и војним командама широм света. Према: Carr J., *op. cit*., p. 46.

[750] Sklerov M.: “Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent”, *Military Law Review*, No. 201, July 2009, pp. 1-86, p. 2.

док се не докаже да напад може бити приписан некој држави или њеним актерима (тим пре што пракса показује да је велики број кибер напада изведен од стране недржавних актера) не изненађује чињеница да су државе невољне да третирају кибер нападе као чинове рата и ризикују кршење међународног ратног права. Дакле, „проблем атрибуције“ окива државе и држи их у стању одбрамбене кризе, истиче Склеров.

Третирање кибер напада као кривичних дела не би било проблематично када би мере пасивне одбране и кривични закони омогућавали довољан степен заштите. Међутим, то није случај. Иако су мере пасивне заштите увек прва линија одбране и доводе до редуковања шансе за успешан наставак напада, државе се не могу ослонити на њих да у потпуности осигурају критичне информационе инфраструктуре. Осим тога, мере пасивне одбране могу урадити врло мало по питању одвраћања нападача од извршења напада. Одвраћање проистиче из кривичних закона и казни које су њима прописане. Ипак, кривични закони су се показали као неуспешни у спречавању кибер напада јер практично све јаке државе дозвољавају својим хакерима да делају без ризика од кажњавања када су њихови напади усмерени ка државама ривалима.

Како би избегле ову дилему, државе морају да прибегну мерама активне одбране, сматра капетан Склеров. Не само да би мере активне одбране у великој мери побољшале државне капацитете за борбу против кибер напада, већ би њихова примена имала и функцију одвраћања будући да нападачи не желе да се излажу контранападу.

Легално право државе да употреби мере активне одбране Склеров изводи из дужности коју државе имају у спречавању недржавних актера да користе њихову територију како би спроводили прекограничне нападе. Традиционално, ова дужност је захтевала да државе спрече противзаконита дела за које су унапред знале. Ова дужност је еволуирала као одговор на међународни тероризам и сада захтева од држава да делују против група за које се генерално зна да спроводе противзаконите деликте, аргументује Склеров. У свету кибер ратовања, дакле, ова дужност би требало да буде протумачена тако да се од држава очекује да усвоје и спроведу кривичне законе како би спречиле прекограничне кибер нападе. Захтевање да државе усвоје и спроведу кривичне законе против прекограничних кибер напада решило би тренутну кризу на један од два могућа начина: или би државе испоштовале своје

обавезе и почеле да спроводе кривичне законе против нападача, или би прекршиле своју обавезу, што би створило легални пут да државе-жртве њих сматрају одговорнима за напад без обавезе да га прво атрибуирају. У пракси, уколико држава више пута не спроведе кривичне поступке против нападача са своје територије, она ће бити проглашена за „државу уточиште криминалаца“, што ће омогућити другим државама да користе мере активне одбране против кибер напада који потичу са њене територије.

Ако се узме у обзир значај употреба мера активне одбране, било би најбоље када би међународно право одредило параметре везане за њихову правилну употребу. На крају, једна од сврха међународног права јесте да наведе државе да се понашају на предвидиве начине, прихватљиве међународној заједници. Стога, уколико међународна заједница не жели да ризикује са непредвидивим и неприхватљивим одговорима на кибер нападе, међународно право мора пружити смернице за употребу мера активне одбране.

Намера нам је да у наставку рада детаљније размотримо образложење које Склеров даје за поменуте ставове.

5.3.1. Анализа кибер напада према доктрини праведног рата

Међународно ратно право почива на две примарне групе правила: *jus ad bellum* и *jus in bello*, што су латински називи за „правни основ ратовања” односно „правни основ средстава која се користе у рату”.[751] Другим речима, постоје правила како једна држава улази у рат и, када се једном нађе у тој позицији, на који начин ратује.

---

[751] Захтеви за *jus ad bellum* су традиционални: а) држава може започети рат само ако има праведан основ, на пример самоодбрану, заштиту недужних и кажњавање преступа; б) исправна намера – не само да држава мора да има праведан основ већ мора и да уђе у рат из тог разлога, тј. мотивација је пресудна; ц) рат се мора објавити јавно и то морају учинити легитимне власти те државе; д) рат мора бити последњи излаз након што су све (реалне) мирне алтернативе истрошене; е) мора бити вероватно да рат води ка остваривању праведног циља; ф) рат не сме водити ка већим патњама и губицима од оних које покушава да спречи.

Захтеви за *jus in bello* су традиционални: мора се направити разлика између могућих циљева напада, тако да се нападају само циљеви који су непосредно умешани у рат, не сме се користити више насиља него што је потребно да би се постигао циљ и не смеју се користити средства која су сама по себи зла, као што су силовање, мучење, оружја за масовно уништавање, биолошка и хемијска оружја итд. Данас су захтеви за *jus in bello* спецификовани у четири женевске конвенције из 1949. и у два допунска протокола из 1977. године. Према: Вучинић З., *op. cit.*

Међународно ратно право подељено је, дакле, на две велике области. Област *jus ad bellum*, такође позната и као *доктрина праведног рата*, правни је режим који је на снази током транзиције из мира у рат.[752] У суштини, она одређује када државе могу законски прибећи оружаном сукобу. *Jus in bello*, такође познато и као *правила понашања у рату*, бави се стварном употребом силе током рата. Анализа питања да ли државе могу одговорити на кибер напад помоћу мера активне одбране најчешће припада области *jus ad bellum*, јер ова област поставља правила које карактеристике кибер напади морају имати како би се сматрали чиновима рата.

Кибер напади представљају загонетку за правне стручњаке. Видели смо да они постоје у мого различитих облика, те да је њихов деструктивни потенцијал ограничен једино креативношћу и спретношћу нападача који стоје иза њих. Иако се може чинити да је једноставно кибер нападе сврстати у оружане нападе, особито у светлу њихове способности да повреде или убију, правна заједница била је невољна да усвоји овај приступ јер кибер напади не представљају традиционалне оружане нападе конвенционалним наоружањем.[753] Ствар додатно отежава уврежено тумачење које државе и стручњаци имају о потреби држава да припишу кибер нападе некој држави или њеним агентима пре него што одговоре силом. Иако је тачно да кибер напади не личе на традиционалне оружане нападе, и да је кибер нападе тешко приписати, ниједна од ових карактеристика не треба да спречава државе да одговоре силом, сматра Склеров.

У циљу поткрепљивања тврдње да државе могу законски употребљавати мере активне одбране против кибер напада који долазе са територије држава које су прекршиле своју дужност да их спрече, поменути аутор приступа испитивању: различитих аналитичких модела за процену оружаних напада; значења *дужности спречавања* везане за кибер нападе и технолошких могућности тзв. „програма за детекцију напада“ да открију тачно порекло напада.

---

[752] Историјски гледано, транзиција из стања мира у стање рата налазила се под прерогативом владара. Ипак, она је доспела под окриље међународног права након Другог светског рата ратификацијом Повеље Уједињених нација. Иако Повеља Уједињених нација није једини извор за *jus ad bellum*, она је почетна тачка за све анализе *jus ad belluma*. Релевантни чланови Повеље Уједињених нација су Чланови 2(4), 39, и 51, и они сачињавају оквир за модерне *jus ad bellum* анализе. *Ibid*., стр. 108.

[753] Sklerov M., *op. cit*., p. 50.

5.3.1.1. Кибер напади насупрот оружаних напада

Државе-жртве морају бити у стању да категоришу кибер напад као оружани напад или непосредну опасност од оружаног напада пре него што одговоре мерама активне одбране јер, аргументује Склеров, оружани напади или блиска опасност од оружаних напада неопходни су услови који морају бити испуњени како би држава могла да одговори самоодбраном или превентивном самоодбраном. У идеалним околностима, постојала би јасна правила за категорисање кибер напада као оружаних напада, непосредне опасности од оружаних напада, или мањих употреба силе. Међутим, како су кибер напади релативно нов облик напада, међународни напори да се они категоришу као оружани напади још су увек у зачетку, иако су суштински правни принципи којима се регулишу оружани напади јасно одређени. Према томе, питања да ли се кибер напади могу категорисати као оружани напади и које кибер нападе треба сматрати оружаним нападима још увек су отворена у међународном праву.[754] Како би одговорио на ова питања, Склеров испитује суштинске правне принципе за регулисање оружаних напада, примењује их на кибер нападе, објашњава зашто се кибер напади могу категорисати као оружани напади и покушава да пружи неки увид у то које би кибер нападе требало сматрати оружаним нападима.

У претходним одељцима рада већ је било речи о томе да појам „оружани напад“ није дефинисан било којом међународном конвенцијом. Због тога је његово значење остало отворено за тумачење од стране држава и стручњака. Иако ово може звучати проблематично, заправо није. Оквир за анализу оружаних напада је релативно добро постављен, као што су и суштински принципи који регулишу његово значење. Међународна заједница, опште узев, прихвата тест опсега, трајања, и интензитета Жана Пиктеа[755] као почетну тачку за евалуацију тога да ли одређена употреба силе може бити сматрана оружаним нападом. Према Пиктеовом тесту, употреба силе може се сматрати оружаним нападом када је довољног опсега,

---

[754] *Ibid*., p. 51.

[755] Жан Пикте (Jean S. Pictet) (1914-2002) био је дугогодишњи потпредседник Међународног комитета Црвеног Крста и изузетан стручњак у области међународног права. Сам термин „хуманитарно право“ предложио је Пикте у својим радовима из ове области. Према: Дурсун Б.: *Основи међународног хуманитарног права*, http://www.scribd.com/doc/47408474/osnovi-medjunarodnog-humanitarnog-prava

трајања, и интензитета. Наравно, као што је то случај са многим међународним правним концептима, државе, невладине организације и стручњаци различито тумаче тест опсега, трајања, и интензитета.

Државне декларације помажу да се детаљима попуни правило које су то употребе силе довољног опсега, трајања, и интензитета да би се могле сматрати оружаним нападом. Генерална скупштина Уједињених нација усвојила је Резолуцију о дефиницији агресије 1974. године. Овом резолуцијом се захтева да напад буде „значајне озбиљности“ пре него што се може сматрати оружаним нападом.[756] Резолуција нигде не дефинише оружане нападе, али пружа примере који су у великој мери прихваћени од стране међународне заједнице. Иако је ова резолуција помогла у одређивању значења оружаних напада по питању конвенционалних напада, напредовањем технологије појавили су се напади у облицима који нису обухваћени претходним државним декларацијама и праксама. Зато, државе сматрају да неконвенционалне употребе силе могу оправдано бити третиране као оружани напади када су њихов опсег, трајање и интензитет довољно озбиљни. Резултат тога је да државе стално издају прогласе о новим методама ратовања, полако обликујући парадигму за категоризацију оружаних напада.

Стручњаци су развили неколико аналитичких модела који се баве неконвенционалним нападима, као што су кибер напади, како би помогли у олакшавању категоризације и стављању анализе опсега, трајања и интензитета у конкретније оквире. Ови модели су посебно релевантни за кибер нападе јер они прелазе линију између криминалне активности и оружаног ратовања.[757] Постоје три главна аналитичка модела која се баве неконвенционалним нападима. Први модел је инструментални приступ који проверава да ли је штета изазвана новом методом напада раније могла бити изазвана једино кинетичким нападом.[758] Други је приступ заснован на ефектима, понекад назван и последични приступ, у коме је сличност

---

[756] Вучинић З., *op. cit*., стр. 58.

[757] Sklerov M., *op. cit*., p. 54.

[758] На пример, према инструменталном приступу, кибер напад употребљен у сврхе саботирања електричне мреже јесте оружани напад. Ово се тако тумачи јер је акција обарања електричне мреже у прошлости подразумевала бацање бомбе на електричну централу или неку другу кинетичку употребу силе како би се онеспособила мрежа. Пошто се од конвенционалне муниције раније очекивало да постигне резултат, према инструменталном приступу кибер напад је стога третиран на исти начин. *Ibid*.

напада кинетичком нападу безначајна и фокус се помера на свеобухватне ефекте које кибер напад има на државу-жртву.[759] Трећи приступ се бави стриктном одговорношћу и њиме се кибер напади против критичне инфраструктуре аутоматски сматрају оружаним нападима, због тешких последица до којих може доћи онеспособљавањем ових система.[760]

Склеров је мишљења да најбољи аналитички модел за разматрање кибер напада, од три наведена приступа, пружа онај који је заснован на ефектима. Не само да анализа заснована на ефектима узима у обзир све што обухвата инструментални приступ, већ она пружа и аналитички оквир за ситуације које се не могу јасно изједначити са кинетичким нападима.[761] Анализа заснована на ефектима је такође супериорна у односу на приступ стриктне одговорности јер се одговори на кибер нападе према приступу заснованом на ефектима сматрају усклађенима са међународно прихваћеним правним нормама и обичајима, док приступ стриктне

---

[759] На пример, према приступу заснованом на ефектима, кибер напад који је манипулисао информацијама у оквиру државних банкарских и финансијских институција како би озбиљно угрозио тржиште државе сматра се оружаним нападом. Иако манипулација информацијама не подсећа на кинетички напад, што је услов према инструменталном приступу, угрожавајући ефекти које је напад имао на економију те државе су довољно озбиљна последица да би се оправдао третман ове врсте напада као оружаног напада.

[760] Важно је напоменути да овај трећи аналитички модел за разматрање кибер напада има намеру да оправда превентивну самоодбрану пре него уопште дође до било какве штете. Валтер Шарп (Walter Sharp) предложио је овај модел због брзине којом се упад у рачунар може претворити у деструктивни напад против критичне инфраструктуре. Он сматра да, када се упад догоди, постоји непосредна претња која има способност да изазове штету великог опсега, трајања и интензитета, и стога је превентивна смоодбрана оправдана. Према: Walter G. S.: *Cyberspace and the use of force*, Ageis, 1999, 129-31.

[761] На пример, кибер напад може оборити систем и учинити га нефункционалним на неки временски период или, пак, напад може изазвати експлозију у хемијској фабрици тако што ће нарушити функционалност рачунара који контролишу размере хемикалија у мешавинама. Резултати таквог напада једнаки су резултатима конвенционалних оружаних напада, који су раније могли бити остварени једино путем кинетичке силе, тако испуњавајући услове инструменталног приступа.

Нажалост, кибер напади такође могу изазвати велику штету која се не може упоредити са резултатима конвенционалних оружаних напада. На пример, координисани кибер напади могли би оборити финансијска тржишта „на колена“ без употребе било чега што макар из далека изгледа као кинетички напад. Измена огромног броја података могла би угрозити банкарство, финансијске трансакције и опште темеље економије, сејући конфузију широм државе-жртве током дужег времена. Према приступу заснованом на ефектима, опсег, трајање и интензитет овог напада био би једнак оружаном нападу, упркос чињеници да их раније није било могуће изазвати једино путем кинетичке силе.

одговорности може ту ситуацију третирати као да су државе-жртве прекршиле међународно ратно право.[762]

Од свих научника који су заступали моделе засноване на ефектима, Мајкл Шмит (Michael N. Schmitt) је развио најкориснији аналитички оквир за процену кибер напада.[763] Аналитички оквир се заснива на следећим критеријумима: јачина, непосредност, директност, инвазивност, мерљивост и претпостављена легитимност.[764] Узети заједно, они омогућавају државама да процене кибер нападе. Ниједан критеријум не носи превагу. Међутим, кибер напад који задовољава већи број наведених критеријума може бити окарактерисан као оружани напад. Од свог издавања, Шмитови критеријуми стекли су следбенике у оквиру правне заједнице – неколико еминентних стручњака заступа њихову употребу. Многи се надају да ће

---

[762] Заговорници приступа стриктне одговорности заступају аутоматски одговор на кибер нападе на критичну инфраструктуру мерама активне одбране. Ипак, аутоматско одговарање на кибер нападе на овај начин може лако навести државу-жртву да изврши контранапад на државу која је позната по томе што одувек чини све што је у њеној моћи да спречи кибер нападе и казни нападаче. Ако би држава-жртва одговорила мерама активне одбране против те државе која није уточиште криминалаца, она би прекршила принципе из доктрине праведног рата. Ово је тако због тога што не постоји начин приписивања државне одговорности једној таквој држави, директно или индиректно, чак и уколико би се кибер напад сматрао оружаним нападом. Према: Sklerov M., *op. cit*., p. 57.

[763] Schmitt M.: "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*, 37: 885, 1999, pp. 913-15.

[764] Значења ових критеријума су следећа:

1. Јачина посматра опсег и интензитет напада. Анализа према овом критеријуму испитује број убијених људи, величину нападнутог подручја и количину штете настале на имовини. Што је већа штета, то је аргумент за третирање кибер напада оружаним нападом јачи.

2. Непосредност посматра, трајање кибер напада, као и друге временске факторе. Анализа према овом критеријуму испитује колико је временски трајао кибер напад и временски период током кога су се осећали његови ефекти. Што је дуже трајање напада и његових ефеката, то је јачи аргумент да је у питању оружани напад.

3. Директност посматра насталу штету. Ако је напад био непосредни узрок штете, то појачава аргумент да је кибер напад био оружани напад. Ако је штета била изазвана у потпуности или делом другим паралелним нападима, то је слабији аргумент да је кибер напад био оружани напад.

4. Инвазивност посматра место дешавања напада. Инвазиван напад је онај који физички прелази границе држава или електронски прелази границе и изазива штету на територији државе-жртве. Што је кибер напад инвазивнији, то се пре може поистоветити са оружаним нападом.

5. Мерљивост покушава да квантификује штету насталу кибер нападом. Штета коју је могуће квантификовати генерално је озбиљније схваћена у међународној заједници. Што држава може више кванификовати штету која јој је нанета, то су веће шансе да кибер напад изгледа као оружани напад.

6. Претпостављена легитимност фокусира се на државну праксу и прихваћене норме понашања у међународној заједници. Акције могу стећи легитимитет када међународна заједница прихвати одређено понашање као легитимно. Што мање кибер напад делује као прихваћена државна пракса, то су јачи аргументи да је у питању противзаконита употреба силе или оружани напад. Према: Schmitt M., *op.cit*., p. 913.

Шмитови критеријуми помоћи у изједначавању напора држава да категоришу кибер нападе. Ипак, док Шмитови критеријуми не постану шире прихваћени, државе ће морати да категоришу кибер нападе на различите начине, у зависности од свог поимања оружаних напада као и свог концепта виталног националног интереса.[765]

Спровођење категоризације кибер напада ће, у пракси, бити веома тешко.[766] По међународном праву, одлука о одговору на напад морала би да буде донета од стране државног руководства. Стварна одлука да се употребе мере активне одбране, међутим, морала би да буде пребачена на систем администраторе који управљају рачунарским мрежама. Један од изазова са којима ће се креатори политике суочити биће превођење међународног права у концизна, разумљива правила како би их њихови систем администратори могли пратити.

Ипак, категоризација кибер напада као оружаних напада или непосредне опасности од оружаних напада је само прва препрека коју систем администратори морају прећи пре него што одговоре мерама активне заштите. Друга и подједнако важна препрека је утврђивање државне одговорности за напад.

5.3.1.2. Утврђивање државне одговорности за кибер нападе

Државе не могу одговорити силом на прекограничне кибер нападе без претходног утврђивања одговорности друге државе за напад. Иако је, историјски гледано, ово значило да је неки напад морао бити приписан држави или њеним агентима, директна контрола напада није више захтев за утврђивање државне

---

[765] Sklerov M., *op. cit*., p. 58.

[766] Склеров сматра да ће неки кибер напади сигурно бити категорисани као оружани напади и да ће бити тумачени кроз призму правних принципа самоодбране и превентивне самоодбране како би била оправдана употреба мера активне одбране: „Неки ће несумњиво критиковати овај закључак. Ипак, они који инсистирају на томе губе из вида начин на који су државе категорисале неконвенционалне нападе у прошлости. Нове методе напада често се налазе ван прихваћених дефиниција оружаних напада. Ово не значи да ти напади нису оружани напади, већ само да се ти напади не уклапају у традиционалне класификације. Даље, свако ко инсистира на томе да се кибер напади не могу подићи на ниво оружаних напада не узима у обзир један од важних аспеката међународног права – репресалије, које могу бити употребљене као алтернативна основа за одобравање мера активне одбране против кибер напада. Из тог разлога што су кибер напади, у најмању руку, противзаконита употреба силе и њихова употреба би самим тим дозволила државама другу противзакониту употребу силе, осим оружане силе, да би се државе које су уточишта нападачима одвратиле од тога да им дозволе да почине те нападе.“ *Ibid*.

одговорности. Данас, међународно право заснива државну одговорност на њеном неизвршавању међународних дужности које има.

Ова промена је посебно важна за кибер нападе јер преовлађујуће мишљење да државе морају третирати прекограничне кибер нападе као кривично питање, а не као питање националне безбедности, делује као да је засновано на историјском тумачењу државне одговорности. Ово ограничено виђење државне одговорности ставља државе у „одбрамбену кризу“ захтевајући од њих да припишу кибер нападе некој држави или њеним агентима пре него што одговоре мерама активне одбране, чак и уколико је вероватноћа да се утврди одговорност државе за напад веома слаба. Последица овога је „одбрамбена криза“ током кибер напада. Државе-жртве, сматра Склеров, полазе од неистините претпоставке да морају да одлуче између ефикасних, али противзаконитих, мера активне одбране и мање ефикасних, али законитих, мера пасивне одбране и домаћих кривичних закона.

Ако се узме у обзир промена у тумачењу државне одговорности, државе би требало да одреде да ли неки кибер напад може бити приписан држави из које је потекао. Када се кибер напад припише некој држави и та држава одбије да одреагује у складу са својим међународним дужностима, правне препреке за реаговање у самоодбрани нестају, истиче Склеров.[767]

Иако ни државна пракса нити публикације правних стручњака још увек не подржавају ово гледиште по питању кибер напада, прихваћени принципи обичајне доктрине праведног рата подржавају приписивање државне одговорности за оружане нападе изведене од стране недржавних актера када ти напади потичу из државе која дозвољава недржавним актерима да спроводе криминалне операције са њене територије. Државе које дозвољавају недржавним актерима да спроводе такве операције крше своју дужност да спречавају нападе против других држава, и познате су као државе уточишта. Ово је веома важно за државе-жртве кибер напада јер када напад води порекло из неке државе уточишта, држава-жртва може употребити мере активне одбране и спречити одбрамбену кризу.

[767] Sklerov M., *op. cit*., p. 62.

Стога је, према Склерову, важно разумети одговоре на два кључна питања:

- Шта се подразумева под дужношћу државе да спречи кибер нападе?
- Шта држава мора да уради како би се сматрало да је прекршила своју дужност превенције?

5.3.1.3. Дужност да се спрече кибер напади

Државе имају дужност да спрече кибер нападе са своје територије против других држава. Ова дужност заправо обухвата неколико активности: доношење строгих кривичних закона, спровођење енергичних истрага од стране криминалистичких агенција, кривично гоњење нападача и, током истражног и кривичног поступка, сарадња са државом-жртвом кибер напада. Ово су дужности свих држава и обавезујуће су као обичајно међународно право. Сва три извора међународног обичајног права – међународне конвенције, међународни обичаји и општи правни принципи заједнички цивилизованим државама – говоре у прилог овој дужности.

Једини међународни споразум који се бави овом тематиком је *Европска конвенција о кибер криминалу*. Иако је овај споразум само регионални уговор, ипак је веома утицајан на пољу међународног обичајног права због значаја држава које су га ратификовале.[768] Даље, он показује да државе препознају како потребу да инкриминишу кибер нападе, тако и дужност држава да спрече да њихове територије буду употребљене од стране недржавних актера за извођење кибер напада против

[768] Међународно обичајно право не захтева да државна пракса буде универзална. И опште праксе могу задовољити услове међународног обичајног права. Тест за то када државне праксе постају међународно обичајно право јесте када су праксе опсежне и када одражавају правила која се државе осећају обавезнима да следе. До данас је 26 држава ратификовало Конвенцију о кибер криминалу, од којих већина спада у водеће силе Запада, од којих 3 имају сталне мандате у Савету Европе, а од којих је 5 међу 20 држава са највећим бројем корисника Интернета у свету – Француска, Немачка, Италија, Уједињено Краљевство и САД. Заједно, ових 5 држава сачињава 25% корисника Интернета у целом свету. Даље, иако још увек нису усвојиле овај споразум, Канада, Јапан, Шпанија и Пољска су потписнице истог и очекује се да ће га ускоро ратификовати. Ове 4 државе су међу преосталих 20 са највећим бројем корисника Интернета у свету и њихова ратификација ће у великој мери изменити државну праксу како би се ускладила са стандардима постављеним у конвенцији. Погледати: Савет Европе, Конвенција о кибер криминалу, Повеља потписа и ратификација, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=18/06/04&CL=ENG (листа 46 потписница и 26 земаља које су ратификовале Конвенцију о кибер криминалу) и 20 држава са највећим бројем корисника Интернета, http://www.internetworldstats.com/top20.htm

других држава.[769] Ова Конвенција је такође важна јер преопознаје да кибер напади не могу бити спречени усред напада, те да је једини начин да они буду спречени ригорозно спровођење закона.

Међународни споразуми који инкриминишу тероризам такође пружају подршку, иако индиректно, дужности да се спрече кибер напади. Међународна заједница препознаје тероризам као претњу међународном миру и безбедности али се, као што смо раније показали, не може сложити око дефиниције. Резултат тога је да су државе усвојиле приступ којим се ван закона стављају одређени терористички чинови сваки пут када терористи усвоје нове методе напада, уместо да ставе ван закона сам тероризам.[770] Ови споразуми намећу неколико заједничких захтева државама у зависности од метода терористичких напада, као што је спровођење свих изводљивих мера у циљу спречавања тих напада, инкриминисање напада, предавање случајева надлежним властима за кривично гоњење и присиљавање држава да међусобно сарађују током кривичног поступка. Иако се ови споразуми не односе на кибер нападе, принципи садржани у њима имају утицаја на захтеве према државама по међунарнодном обичајном праву по питању тероризма. Како постоји много доказа да ће кибер напади ускоро бити главно оружје терориста, државе би требало да консултују уобичајене принципе који се налазе у овим споразумима у виду судског мишљења када се кибер напади употребљавају као терористичко оружје, истиче Склеров.

---

[769] Конвенција о кибер криминалу захтева од држава које су је усвојиле да установе кривичне прекршаје за скоро сваки могући тип кибер напада према својим домаћим правним системима (чланови 2-11). Она такође препознаје и важност кривичног гоњења нападача, и захтева од држава да прошире своју надлежност како би обухватиле све кибер нападе изведене са њихове територије или изведене од стране њихових држављана, без обзира на њихову локацију у време напада (члан 22). Осим тога, ова конвенција наглашава важност сарадње међу државама, и захтева од држава да пруже „најширу могућу узајамну помоћ у циљу истраге или кривичних поступака који се тичу кривичних дела“ (чланови 23-25). Према: *Конвенција о кибер криминалу*, http://www.entel.rs/info/software/sajber%20kriminal-konvencija%20EZ.pdf

[770] У ове споразуме спадају: *Токијска конвенција о прекршајима и одређеним другим делима почињеним у авиону* из 1963; *Хашка конвенција за сузбијање противзаконитог преузимања авиона* из 1970; *Монтреалска конвенција за сузбијање противзаконитих дела против безбедности цивилне авијације* из 1971; *Међународна конвенција против узимања талаца* из 1979; *Конвенција за сузбијање противзаконитих дела против безбедности у поморском саобраћају* из 1988; *Монтреалски протокол о сузбијању противзаконитих дела насиља на аеродромима за међународни путнички саобраћај* из 1988; *Међународна конвенција за сузбијање терористичких бомбашких напада* из 1997; *Међународна конвенција за сузбијање финансирања тероризма* из 1999; *Међународна конвенција за сузбијање дела нуклеарног тероризма* из 2005. итсл.

Начин на који државе третирају кибер нападе према својим кривичним законима такође указује на препознавање дужности да се спрече кибер напади према међународном обичајном праву. Бројне државе инкриминишу и кривично гоне извршиоце кибер напада како би их одвратиле од таквог деловања. Спровођење закона, дакле, јесте једини начин заштите сопствених рачунарских система. Ово даје на значају чињеници да, за разлику од конвенционалног напада, који може бити заустављен након што је откривен, кибер напади могу бити заустављени једино успостављањем *ex ante* препрека које би заплашиле нападаче и одвратиле их од напада. Даље, ове праксе показују да је у порасту схватање држава да кибер напади морају бити заустављени и да је начин да се то уради кроз енергично спровођење закона.

Осим тога, Склеров сматра да одговори држава на транснационалне терористичке нападе додатно подржавају препознавање дужности да се спрече кибер напади према међународном обичајном праву. Након терористичких напада 11. септембра 2001, државе широм света прогласиле су тероризам за претњу међународном миру и безбедности и пружиле различите облике подршке Сједињеним Америчким Државама у рату против Ал-Каиде. Да би се осигурало да ће тероризам увек бити правно сматран претњом међународном миру и безбедности, Савет безбедности усвојио је Резолуцију 1373, која је потврдила да су чинови међународног тероризма претње међународном миру и безбедности и која апелује на државе да раде заједно како би спречиле и сузбиле тероризам. Ова резолуција је, даље, саветовала државе да се „уздрже од пружања било какве подршке“ терористима кроз деловање или пропусте, да „не пружају уточиште“ онима који изводе терористичке акције, и да „омогуће једне другима највећи ступањ сарадње у вези са кривичним истрагама...[или] поступцима“ повезаних са тероризмом.

Одговор међународне заједнице на тероризам показује да државе имају дужност да спрече претње међународном миру и безбедности. Осим тога, он показује да пасивно мирење са претњама међународном миру и безбедности неће бити толерисано. Коначно, истиче Склеров, он показује и да државе морају да раде заједно како би спречиле и сузбиле претње међународном миру и безбедности. Што кибер напади више подсећају на тероризам, то ће се лакше уклопити у парадигму направљену да се бави транснационалним тероризмом. Ипак, без обзира на њихову

сврху, кибер напади представљају претњу међународном миру и безбедности и са њима треба поступати као и са другим признатим транснационалним претњама.[771]

Бројне декларације УН о међународном криминалу такође препознају дужност да се спрече кибер напади. Ове декларације залажу се за то да државе треба да преузму афирмативне кораке како би спречиле недржавне актере да користе њихову територију како би починили дела која ће довести до грађанских немира у другој држави.[772] Даље, ове декларације такође подржавају дужност држава да сарађују једне са другима како би се елиминисао траснационални криминал, што даје на уверљивости обавези да се сарађује са државом-жртвом током кривичне истраге и процеса кибер напада.[773]

Фокусирајући се посебно на кибер нападе, државе су и саме правиле предлоге и користиле Генералну скупштину УН да издају многе декларације о важности спречавања кибер напада. На пример, Генерална скупштина УН позвала је државе да инкриминишу кибер нападе[774] и да не дозволе да њихова територија буде употребљена као сигурно уточиште за спровођење кибер напада.[775]

Генерална скупштина је, такође, позвала државе да сарађују једне са другима током истраге и кривичних процеса за међународне кибер нападе.[776] Чак је и премијер Кине Wen Jiabao признао да би Кина требало да предузме чврсте и

---

[771] Sklerov M., *op. cit*., p. 66.

[772] Декларација о пријатељским односима, 1970., Ген. Скупштина, Рез. 2625, ¶ 1, УН званични записник ГС, 25. заседање, Анекс, предмет агенде 85, УН док. A/Рес/2625 (24. 10. 1970.); Бечка декларација о злочину и правди: Сусрет са изазовима 21. века, 2000. Ген. Скупштина Рез. 55/59, Анекс, ¶ 18, УН док. A/РЕС/55/59/Анекс (17. 01. 2001.): Чланови о одговорности држава за међународна кривична дела, 2001., УН док. A/ЦН.4/Л.602/Рев 1 (2001.).

[773] Ген. Скупштина Рез. 2615, супра ноте 23, ¶ 1; Извештај генералног секретара поводом дискусије о претњама, изазовима и променама, ¶ 17, 24, одржан пред Генералном скупштином, УН док. A/59/565 (02. 12. 2004.).

[774] Ген. Скупштина Рез. 45/121, ¶ 3, УН Док. A/РЕС/45/121 (14. 12. 1990.); Ген. скупштина Рез. 55/63, ¶ 1, УН Док. A/РЕС/55/63 (22. 01. 2001.); такође погледати Осми конгрес Уједнињених нација о превенцији криминала и третману преступника, Хавана, Куба, 17.08– 07. 09. 1990., извештај који је припремио секретаријат, на 140–43, УН Док. A/CONF.144/28/Rev.1 (1991.).

[775] Ген. скупштина Рез. 55/63, супра ноте 25, ¶ 1.

[776] Ген. скупштина Рез. 45/121, супра ноте 25, ¶ 3 (прихватање принципа усвојених на Осмом конгресу Уједињених нација о превенцији криминала и третману преступника, и позивање држава да их следе); Ген. Скупштина Рез. 55/63, супра ноте 25, ¶ 1; видети такође Осми конгрес Уједињених нација о превенцији криминала и третману преступника, Хавана, Куба, 27. 08- 07. 09.1990, УН Док. A/CONF.144/28/Rev.1 (1991).

ефикасне акције како би спречила све хакерске нападе који представљају претњу рачунарским системима.

Даље, државе почињу да схватају какву претњу међународном миру и безбедности представљају кибер напади, док неке државе и Генерална скупштина сматрају да кибер напади представљају непосредну опасност за међународни мир и безбедност.[777] Све ове декларације сведоче о препознавању дужности које државе имају да спрече кибер нападе: да донесу строге кривичне законе, енергично спроводе истраге о извршеним кибер нападима, кривично гоне нападача и обавезу да државе-домаћини сарађују са државама-жртвама током истраге и кривичног поступка.

Општи правни принципи заједнички свим цивилизованим народима такође подржавају препознавање обавезе да се спрече кибер напади. Опште је познат принцип у законодавству већине држава да појединци треба да буду одговорни за дела или пропусте који за последицу имају штету нанету другом појединцу. Док међународно право није у обавези да прати домаће законе држава, оно може бити утемељено на општим принципима заједничким свим великим правним системима у свету. Већина држава употребљава узрочност као принцип за утврђивање индивидуалне одговорности, што даје кредибилитет идеји да би државна одговорност исто требало да буде утемељена на узрочности. Стога, уколико држава не донесе строге кривичне законе, не истражује међународне кибер нападе или кривично не гони нападаче, она би требало да буде сматрана одговорном за међународне кибер нападе против друге државе јер су њени пропусти довели до стварања уточишта за нападаче.

---

[777] *Национална стратегија за безбедност кибер простора САД* из 2003; *Конвенција о кибер криминалу*; Ген. Скупштина Рез. 53/70, УНУН Док. A/RES/53/70 (04. 01.1.999.); Ген. Скупштина Рез. 54/49, ¶ 2, УН Док. A/RES/54/49 (23.1.2. 1999.); Ген. скупштина Рез. 55/28, УН Док. A/RES/55/28 (20.12.2.000.); Ген. Скупштина Рез. 56/19, УН Док. A/RES/56/19 (07. 01. 2002.); Ген. Скупштина Рез. 56/121, УН Док. A/RES/56/121 (23.01.2.002.); Ген. скупштина Рез. 57/53, УН Док. A/RES/57/53 (30. 12. 2002.); Ген. Скупштина Рез. 57/239, ¶ 1–5, УН Док. A/RES/57/239 (31. 01. 2003.); Ген. Скупштина Рез. 58/32, УН Док. A/RES/58/32 (18. 12. 2003.); Ген. скупштина Рез. 58/199, ¶ 1–6, УН Док. A/RES/58/199 (30. 01.2.004.); Ген. Скупштина Рез. 59/61, УН Док. A/RES/59/61 (16.12. 2004.); Ген. скупштина Рез. 59/220, ¶ 4, УН Док. A/RES/59/220 (11. 02. 2005.); Ген. Скупштина Рез. 60/45, УН Док. A/RES/60/45 (06. 01.2.006.); Ген. Скупштина Рез. 60/252, ¶ 8, УН Док. A/RES/60/252 (27.04.2006.); Ген. Скупштина Рез. 61/54, УН Док. A/RES/61/54 (19.12. 2006.).

Судска мишљења додатно подржавају обавезе државе да спречи кибер нападе против других држава са своје територије. У прилог овој тврдњи Склеров наводи примере из праксе Међународног суда правде.[778]

Дужност државе да спречи кибер нападе не би требало да буде утемељена на спознаји те државе о конкретном нападу (пре него што се он догоди), већ на њеним акцијама за спречавање кибер напада генерално. Државама је врло тешко да уоче кибер нападе пре извршења конкретног напада. Осим тога, њих често извршавају појединци или групе који нису под контролом државе. Кибер нападе је тешко спречити, али то не значи да државе могу кршити своју обевезу да их спречавају. Постојање строгих кривичних закона и спровођење тих закона требало би да одврате потенцијалне нападаче. Државе које не донесу такве законе, или их не спроводе, не испуњавају своју дужност да спрече кибер нападе. Другим речима, пасивност државе и незаинтересованост по питању кибер напада чине ту државу уточиштем из ког нападачи могу безбедно да оперишу. Дакле, полазећи од ових премиса Склеров изводи закључак о посредној одговорности државе за кибер нападе, на основу утврђених принципа међународног обичајног права.

Одређивање да ли се нека држава понаша као држава-уточиште у многоме зависи од чињеница. Приликом разматрања овог питања, државе-жртве морају проверити кривичне законе државе-домаћина, праксе спровођења закона и наћи архиву о сарадњи са државама-жртвама кибер напада који воде порекло са њене територије. У пракси, државе-домаћини биће процењиване према напорима које улажу да би ухватиле и кривично гониле нападаче који су починили кибер нападе, што је вероватно једини начин на који државе могу да осујете и спрече будуће нападе. Државе-жртве ће, дакле, проценити да ли је држава-домаћин испунила своје обавезе према међународним очекивањима. Државе-домаћини мораће да сарађују са државама-жртвама како би потврдиле транспарентност. Међусобна сарадња ће нужно захтевати да држава-домаћин прикаже своју кривичну истрагу држави-чланици како би држава-жртва могла исправно проценити напоре које држава-домаћин улаже.[779]

---

[778] Видети детаљније у: Sklerov M., *op. cit*., pp. 70-71.
[779] *Ibid*., p. 72.

Даље, када држави-домаћину недостају тенхнички капацитети за откривање нападача, међународно право би требало да захтева да она ради заједно са полицијским званичницима из државе-жртве како би их заједничким снагама открили.[780] Ове две мере спречиће да се државе-домаћини посматрају као некооперативне и као саучесници у нападима на друге државе. Државе које поричу умешаност у кибер напад али одбијају да прикажу своје истражне материјале држави-жртви не могу очекивати да буду третиране као да испуњавају своје међународне дужности. У суштини, државе-домаћини које одбију да сарађују са државама-жртвама изражавају своју невољност да спрече кибер нападе те се могу прогласити државама уточишта, тј. може им бити приписана одговорност од стране других држава.

У том тренутку, држава-домаћин постаје одговорна за кибер напад који је био предмет почетног захтева за истрагом, као и за све будуће кибер нападе који воде порекло са њене територије. Ово отвара врата државама-жртвама да употребе мере активне одбране против рачунарских сервера у тој држави током кибер напада.[781]

5.3.2. Избор да се употребе мере активне одбране

Иако капетан Склеров охрабрује државе да користе мере активне одбране како би заштитиле своје рачунарске мреже, државе које одаберу да их употребе суочиће се са тешкоћама које су разултат технолошких ограничења. Технолошка ограничења ће довести државе у позицију да, уколико желе да благовремено употребе мере активне одбране, морају одлучити да их употребе уз непотпуне информације. Како одговор силом на кибер нападе мора бити у складу са оба подручја ратног права – *jus ad bellum* и *jus in bello* – одлука да се употребе мере активне одбране покреће неколико других питања о рату која су резултат ових

[780] Ову позицију подржавају многобројне резолуције Генералне скупштине Уједињених нација, Европска конвенција о кибер криминалу и друга документа УН-а, која охрабрују државе да међусобно сарађују при истрагама и кривичном гоњењу криминалне злоупотребе информационих технологија.

[781] Sklerov M., *Ibid*.

техничких ограничења. Са практичног становишта, ово ће утицати на доношење одлука и на највишем и на најнижем нивоу власти.

Творци државне политике мораће да узму у обзир сва ова ограничења приликом креирања политике, док ће државни систем-администратори морати да узму у обзир ова ограничења када буду одговарали на стварне кибер нападе.

5.3.2.1. *Jus ad bellum* доктрина и анализа технолошких ограничења при идентификацији, класификацији и утврђивању извора напада

Анализа кибер напада је у великој мери поједностављена утврђивањем чињенице да ли је држава из које напади потичу прекршила своју дужност да их спречи. *Jus ad bellum* доктрина захтева да државе пажљиво анализирају кибер напад и да буду сигурне да: 1) напад представља оружани напад или непосредну опасност од оружаног напада; и 2) напад потиче из државе уточишта. Оба ова услова морају бити испуњена пре него што држава може законски одговорити употребом мера активне одбране према *jus ad bellum* доктрини.

Анализу кибер напада, по својој прилици, спроводиће систем-администратори, јер их систематизација радних места ставља у прве редове одбране. Систем-администратори могу употребљавати различите рачунарске програме како би олакшали анализу. Програми за аутоматско откривање напада и рано упозорење могу помоћи да се открију упади, класификују напади и означе упади на које треба одговорити. Програми који су на располагању администратору могу пратити порекло напада све до локације са које су покренути. Ови програми могу помоћи администраторима система да категоришу кибер нападе као „оружане нападе“ или „мање употребе силе“ и да процене да ли напади потичу из државе за коју се од раније зна да је држава-уточиште. Када се испуне адекватни правни услови, систем-администратори могу употребити мере активне одбране како би заштитили своје мреже.[782]

Нажалост, постоји велика вероватноћа да ће технолошка ограничења везана за откривање напада, категоризацију напада и праћење порекла напада додатно

[782] *Ibid*., p. 74.

закомпликовати доношење политичких одлука током анализе кибер напада. У идеалним околностима било би лако открити нападе, извршити њихову категоризацију и открити извор. Нажалост, овде то није случај.

Програми за детекцију напада и рано упозорење могу помоћи да се открију кибер напади пре него што они достигну тачку кулминације. Али чак и најбољи програми нису у стању да открију све кибер нападе. Неуспех да се напад открије у раној фази, пре него што се оконча, има и позитивну и негативну страну. Добра страна је та да државе имају довољно времена да анализирају напад, јер је претња већ прошла. Лоша страна је та да откривање порекла напада, проласком времена, постаје све теже.

Даље, чак и када се испостави да је „оружани кибер напад“ потекао са територије државе-уточишта, креатори државне политике морају добро да размисле пре него што употребе мере активне одбране, ако се то посматра као политичко питање. Што је више времена потребно да се открије напад, то је мања потреба да држава искористи мере активне одбране, посебно онда када делује да је напад потпуно завршен. Са друге стране, када се напад који је завршен посматра као део низа текућих напада, примена мера активне одбране у циљу одбијања будућих напада чини се оправданом.

Програми за детекцију напада и рано упозорење у стању су да открију многе кибер нападе док су они још увек у току. Међутим, откривање напада пре него што он кулминира, чини га тежим за класификовање. Наравно да ће систем-администратор моментално покушати да заустави напад мерама пасивне одбране, оног тренутка када га открије, али то није целокупан опис његовог посла. Администратор система мора такође да процени причињену штету, као и сваку могућу компликацију која може да настане због ње, како би се могла донети одлука о употреби мера активне одбране.[783]

Када кибер напад изазове озбиљну, непосредну, директну штету која се брзо шири и која се може одредити, он се може назвати „оружаним нападом“, иако је он,

[783] Ове одлуке ће без сумње бити засноване на смерницама које држава-жртва објави пре него што се напад и догоди. Ова правила ће поједноставити законски оквир и свести га на групу правила лако разумљивих лаику, сличних правилима вођења борбе која поштују припадници оружаних снага.

можда, још увек у току.[784] С друге стране, ако напад не изазове такву штету, администратор неће морати да процењује: 1) непосредну опасност од будуће штете; 2) могућност заустављања напада чисто одбрамбеним мерама како би се одредило да ли напад може да се класификује као непосредна опасност од оружаног напада. С обзиром на то да рачунарски кодови могу деловати брзином светлости, ово неће бити нимало лако пошто одлагање употреба мера активне одбране значи опасност од још веће штете.

Ограничења у погледу класификације напада требало би да наведу администраторе система да размисле пре него што одлуче да употребе мере активне одбране у превентивној самоодбрани. Иако сматра да је потпуно законито донети одлуку засновану на подробној анализи чињеница, Склеров је мишљења да ће такве одлуке бити веома подложне спекулацијама с обзиром на нејасну природу кибер напада. У ситуацији када се напад детектује, сврху напада биће вероватно веома тешко прозрети без растављања програмског кода на делове или претраживања историје активности нападача. Штавише, брзина којом се кибер напади спроводе натераће систем-администраторе да се баве нагађањем по логици здравог разума, иако ће вероватно приликом нагађања бити ускраћени за најважнију информацију. Имајући у виду недовољно јасну природу таквих калкулација, креатори државне политике ће можда пожелети да усмере администраторе да на кибер нападе одговоре превентивном самоодбраном само у случају крајње нужде, како би спречили ескалацију непријатељства међу државама.[785]

Кибер напади се често изводе посредством великог броја сервера и рачунарских система како би се прикрио стварни идентитет нападача. Иако програми за улажење у траг нападачима могу да продру у те посредујуће системе, све до електронског извора напада, њихова стопа успешности далеко је од идеалне. Зато програми за детекцију напада носе ризик погрешног откривања извора напада. Ово очито ствара проблем јер би напад могао да изгледа као да долази из државе из које заправо не долази. Ипак, овај проблем није тако велики како се чини. О одговорности државе требало би расуђивати на основу чињеница које су на

[784] Sklerov M., *op. cit*., p. 76.
[785] *Ibid*.

располагању, чак и ако то резултира приписивањем напада погрешној држави, истиче Склеров. Прво, док год држава процењује напад користећи максимално своје техничке могућности и информације које су јој на располагању, она је у доброј вери испунила своје међународне обавезе. Друго, државе које одбијају да испуне своју међународну обавезу спречавања могуће злоупотребе своје територије као извора кибер напада, ризикују да им буде приписана посредна одговорност за напад. На крају крајева, држава може да избегне опасност да буде мета активне одбране, чак и ако напади потичу из ње, на тај начин што ће предузети позитивне кораке да спречи кибер нападе, као што су доношење строгих кривичних закона, спровођење тих закона и сарадња са државама-жртвама како би нападачи били приведени правди.

5.3.2.2. *Jus in bello* питања која се односе на употребу мера активне одбране

Одлуке о употреби силе одређене су принципима *jus in bello*. *Jus in bello* представља пропозицију да државе немају право да користе неограничену силу против других држава током рата. У својој суштини, *jus in bello* користи четири основна принципа за регулисање понашања држава током ратовања. То су: принцип разликовања, нужности, хуманости и пропорционалности.

Разликовање је захтев да „сукобљене стране у свако доба треба да праве разлику између цивилног становништва и војника и… да ће своје војне операције усмеравати искључиво ка војним циљевима“.[786]

Принцип *нужности* ограничава количину силе коју држава може да употреби против легитимних циљева до границе „неопходне да се испуни одговарајући војни циљ”, и забрањује употребу силе која за сврху има „беспотребну људску несрећу и физичко истребљење”.[787]

Принцип *хуманости* забрањује употребу оружја направљеног „да изазове непотребно страдање”.[788]

---

[786] Допунски протокол уз Женевске конвенције од 12. августа 1949. године, и о Заштити жртава међународних оружаних сукоба од 8. јуна 1977. Према: Вучинић З., *ор. cit*., стр. 270.

[787] *Ibid*.

[788] *Хашка конвенција о законима и обичајима рата на копну* од 18. октобра 1907.

Принцип *пропорционалности* штити цивиле и њихову имовину на исти начин као што принципи нужности и хуманости штите легитимне циљеве од прекомерне употребе силе. Имајући у виду да напади на легитимне циљеве често прозрокују ненамерну штету мимо самог легитимног циља, принцип пропорционалности ограничава употребу силе на ситуације у којима очекивана војна корист надмашује очекивану колатералну штету причињену цивилима и њиховој имовини.[789]

5.3.2.2.1. Мере активне одбране - најприкладнији одговор применом силе

Иако Склеров заговара употребу мера активне одбране као одговора на кибер нападе, неизбежна последица прихватања тезе да државе имају право да на кибер нападе одговоре силом јесте да те исте државе могу да употребе силу у оној мери која је предвиђена принципом *jus in bello*. Другим речима, уколико *jus in bello* не спречи државе у коришћењу конвенционалног оружја, одговори применом силе неће бити ограничени само на мере активне одбране. Зато је потребно објашњење зашто би креатори државне политике требало да изаберу мере активне одбране као најприкладнији одговор кибер нападима.

Мере активне одбране су најприкладнији тип силе која може да се користи против кибер напада у светлу принципа *jus in bello*.[790] Прво, у смислу неопходне војне интервенције, мере активне одбране вероватно представљају сву силу која је потребна да би се испунила мисија одбране од кибер напада. Мере активне одбране могу да открију одакле напади долазе и моментално их онемогуће, док ће кинетичко оружје бити спорије и мање ефикасно у односу на информатичко откривање извора напада. Према томе, употреба кинетичког оружја током активне одбране неће бити мање ефикасна, али ће такође нарушити принцип нужности употребљавајући силу са једним јединим циљем, а то је уништење. Друго, у смислу пропорционалности, мања је вероватноћа да ће мере активне одбране изазвати несразмерно велику колатералну штету у односу на кинетичко оружје. Мере активне одбране допуштају лоцирање извора кибер напада. Иако колатерална штета може и тада настати, јер рачунарски

[789] Овај принцип изведен је из Допунског протокола I, члана 51. Према: Вучинић З., *op. cit*., стр. 272.
[790] Sklerov M., *op. cit*., p. 79.

систем из кога потичу кибер напади може имати вишеструке функције (осим уколико нападач не изводи напад помоћу кључних информационих система), употребом мера активне одбране она ипак не би требало да буде великих размера.

Штавише, како се већина кибер напада изводи од стране недржавних актера, мало је вероватно да ће велики број напада бити лансиран са рачунара који су саставни део кључне инфраструктуре те државе. Из овога следи да мере активне одбране омогућавају државама да хируршком прецизношћу узврате напад са минималним ризиком од тешке колатералне штете причињене држави-домаћину испуњавајући притом захтев о пропорционалности да се изабере оружје чијом употребом је најмање вероватно проузроковање велике колатералне или узгредне штете.

Коначно, иако не проистичу из принципа *jus in bello*, избор мера активне одбране у односу на кинетичко оружје требало би да умањи шансу ескалирања оваквих ситуација у свеобухватне оружане сукобе међу државама.

5.3.2.2.2. Анализа технолошких ограничења и jus in bello доктрине

Нажалост, упркос већој безбедности коју мере активне одбране пружају, коришћење ових мера носи одређени ризик. Технолошка ограничења могу спречити државе у извршавању прецизних напада мерама активне одбране. Што више нападач прикрива свој напад, спроводећи га помоћу великог броја сервера и система, то га је теже пратити.

Штавише, за сложена праћења потребно је доста времена, кога у кризној ситуацији нема на претек. Овим потешкоћама треба додати и чињеницу да програми за улажење у траг често нису у могућности да прецизно одреде извор напада онда када нападач прекине конекцију са Интернетом. Некада ће ове потешкоће једноставно резултирати неуспехом у покушају да се одреди извор напада. Други пут могу резултирати погрешним одређивањем система са кога је напад иницран (извора напада). Чак и када је извор напада успешно одређен, систем-администратор државе-жртве мора да мапира рачунарски систем са кога долази напад како би спознао његове функције као и могуће последице које могу настати уколико се напад заустави. Ипак, за „мапирање" рачунарског система, потребно је време, често и више времена него што једна држава има када мора да донесе политичку одлуку. Понекад

ће администратор моћи да мапира систем веома брзо, омогућавајући на тај начин естаблишменту да процени могућу колатералну штету. Међутим, некада ће држава бити приморана да изврши процену могућих последица коришћења мера активне одбране без потпуно мапираног система. Дакле, свака држава која користи мере активне одбране ризикује да случајно погоди погрешне системе, са којих не долази напад, узрокујући тиме велику колатералну штету.

Како би се осигурала законска примена мера активне одбране у складу са принципима разликовања и пропорционалности, државе морају покушати да смање ове ризике. У светлу мера активне одбране, то значи да треба учинити све што је могуће да се одреди: 1) рачунарски систем са кога долази почетни напад; и 2) очекивана колатерална штета која ће настати као резултат коришћења мере активне одбране. Када држава уради све што је изводљиво да осигура добијање тачне информације и поступа у доброј вери у складу са *jus in bello*, она је и законски заштићена од погрешних процена, чак и ако нациља цивилне системе или причини огромну колатералну штету свом војном циљу. На тај начин, државе још увек могу да делују и на основу непотпуних информација, сматра Склеров. Прави тест биће то да ли је опасност по системе државе-жртве оправдала коришћење мера активне одбране у светлу могуће колатералне штете држави-домаћину.[791]

Пре него што држава одлучи да имплементира мере активне одбране, потребно је размотрити неколико питања.

Пре свега, због кратког временског интервала кибер напада, држави ће можда бити потребно да аутоматизује мере активне одбране како би могла да благовремено реагује. Но, употреба аутоматизованих мера одбране повећаће вероватноћу нарушавања принципа разликовања и пропорционалности. Као резултат свега, мере одбране би требало аутоматизовати само у сврху откривања напада.

Друго, само зато што је коришћење мера активне одбране у наведеним околностима у складу са законом, то не значи да је таква политика и добра. Државе морају да одлуче да ли су њихова дипломатска неслагања вредна ризика. Нажалост, технолошка ограничења могу довести до тога да држава повремено направи

[791] Sklerov M., *op. cit*., p. 82.

погрешну процену и погоди цивилне системе или им причини велику колатералну штету.

Трећа ствар је да постоји могућност да су сервери са којих потичу почетни напади тесно повезани са важним системима у држави-домаћину, и у случају да се искључе, могу имати разорне последице и довести до неминовног страдања. Ова се могућност мора узети као фактор приликом процењивања нужности војне интервенције државе насупрот могућој колатералној штети нарочито уколико држава одговара мерама активне одбране без потпуног мапирања система са којег напад долази.

Четврто, државе морају пажљиво осмислити мере активне одбране. Програми мера активне одбране који су недовољно кодирани ризикују да се прошире у кибер простору, што одступа од њиховог првобитног циља, и да од програма за одбрану еволуирају у малициозни код чија штета може далеко да превазиђе потребу из које је он настао. Премда мере активне одбране представљају нову границу у кибер ратовању, њихова почетна примена биће спорна, без обзира на ситуацију. Државе могу очекивати и критику јавности као и дипломатске протесте док не дође време да мере активне одбране буду признате као легитиман начин самоодбране по међународном праву.[792]

5.4. Преглед предузетих мера и активности држава на пољу супротстављања претњама у кибер простору

На основу досадашње елаборације проблема, могли смо се уверити да је заштита умрежених информационих система од разноврсних кибер претњи, услед њихове озбиљности, сложености и значаја, већ годинама предмет студија, расправа и одлука различитих националних и међународних тела и организација. Студије и остали материјали сачињени у оквиру међународних организација и асоцијација, као и одговарајућих националних институција, предвидели су реализацију конкретних мера у оквиру сталних консултантских процеса.

[792] Sklerov M., *op. cit*., p. 83.

Успостављање сарадње између правосудних органа, индустрије, разних организација и асоцијација посебно се потенцира од 1997. године, када је у Вашингтону одржан састанак министара правде и полиције земаља Г8 и када је утврђено десет тачака *Акционог плана* борбе против кибер криминала, међу којима је посебно место посвећено сарадњи са индустријским сектором, који дизајнира, развија и производи компоненте глобалних мрежа, али и који треба да буде одговоран за изградњу и примену техничких безбедносних стандарда.

Европска унија је 1998. године наставила са „охрабривањем" производње специјализованих производа који служе за повећање безбедности рачунарских система и мрежа у оквиру *Студије о правним аспектима компјутерског криминала у информационом друштву*. Ова студија је, такође, предвидела успостављање сарадње између правосудних органа, индустрије, организација потрошача и телâ за заштиту података, али и формирање посебних јединица специјализоване полиције на националном нивоу држава чланица.[793] Успостављање специјализованих јединица за откривање, праћење и хватање злонамерних актера у кибер простору представљало је посебно значајан помак. Пример рада таквих тела представља успостављање „врућих линија" између већег броја земаља – од САД, Велике Британије, Немачке, Норвешке, Аустрије, Холандије до Ирске у оквиру тзв. *мреже Дафне*[794] и повезаних провајдера у Европском форуму.

Ни група Г8 није остала по страни у решавању практичних питања кооперације и инернационализације активности везаних за кибер криминал. Успостављена је мрежа која 24 сата током 365 дана у години обезбеђује адекватну примену принципâ борбе против криминала високих технологија. Њима се придружују и земље нечланице, чиме се круг шири, а очекивани ефекти треба да буду бољи. Успостављен је чак и експертски тим који би требало да идентификује методе и технике те дефинише стандарде које се могу примењивати у борби против

---

[793] *Legal Aspects of Computer-related Crime in the Information Society – COMCRIME*, http://europa.eu.int/ISPO/legal/en/crime/crime.html.

[794] Мрежа Дафне (Daphne Programme) – програм ЕУ за превентивну акцију у борби против насиља над децом, омладином и женама; према: Водич кроз избор правних и законодавних инструмената за управљање миграцијама на територији Европске уније, Међународна организација за миграције (IOM), 2005, http://iom.ramdisk.net/iom/images/uploads/Vodic%20kroz%20izbor%20prav-nih%20i%20zakonodavnih%20instrumenata%20za%20upravljanje%20migracijama%20na%20teritoriji%20Evr_1185965257.pdf.

кибер криминала, као и у пружању помоћи специјализованим телима за његово откривање. Тај тим чини *Међународну организацију за компјутерске доказе* (*IOCE*), као групу којој су се прикључили тимови из Европске уније и њених земаља чланица. Тако је успостављена мрежа чији је циљ олакшавање реализације програма истраживања и праћења овог криминала.

Ове активности подржали су и експерти који су се, у организацији UNESCO-а, састали у Паризу 1999. године ради договора о успостављању конкретне мреже „врућих линија“, симболички названих „електронска кула стражара“. Њима треба додати и екипе окупљене око пројекта *Excalibur*, који је развило Шведско обавештајно одељење за криминал и којим се успоставља сарадња између полицијâ Немачке, Велике Британије, Холандије и Белгије, заједно са Европолом и Интерполом.[795]

Од специјализованих јединица за откривање, праћење и хватање злонамерних актера у кибер простору захтева се перманентно усавршавање у циљу успешног супротстављања претњама. У том смислу, Европол организује сталну обуку чланова својих специјализованих група, путем семинара о специфичним врстама напада, методима и техникама откривања извора, као и начинима прикупљања и обезбеђивања доказâ. Слично се већ годинама ради у оквиру Интерпола, а ни посебна група експерата у оквиру Г8 није остала без континуираног усавршавања.

У оквиру америчког Федералног истражног бироа 2000. године радило је шеснаест специјализованих станица на територијама федералних држава, са преко 190 агената. У обављању посла агентима помажу бројни сарадници – универзитетски професори и асистенти, као и експерти који се налазе у институтима, индустрији, компанијама и разним другим организацијма и институцијама. Они се, по позиву, укључују у активности откривања деликата, рутирања и прикупљања доказа, али и за пружање консултативних услуга органима гоњења. Да би се сагледале размере овог феномена и идентификовале карактеристике појавних облика, унутар FBI-ја

[795] Дракулић М., Дракулић Р.: *Cyber криминал*, 2005, http://www.bos.org.yu/cepit/drustvo/sk/cyberkriminal

формирани су посебни тимови за анализу,[796] који имају троструку улогу – да проналазе и анализирају податке неопходне за подршку инспекторима FBI-ја, да буду техничка и саветодавна подршка и да помогну развоју софтверских и других производа за обезбеђивање сигурности рачунарских система и мрежа.

Операционализација сарадње између различитих актера на европском нивоу постигнута је формирањем Форума ЕУ, који обухвата разне агенције, провајдере Интернет-услуга, операторе телекомуникација, организације за људска права, представнике корисника, тела за заштиту података и све друге заинтересоване који желе да се установи сарадња у борби против кибер криминала. Форум има за циљ:

- развој двадестчетворосатне везе између државних органа и индустрије;
- дефинисање стандардних захтева за које провајдери треба да обезбеде информације о коришћењу Интернета;
- изградњу и примену етичког кодекса, са дефинисањем „добрих пословних обичаја“ свих актера, а посебно у међусобним односима између државних органа и индустрије;
- поспешивање размене информација о трендовима криминала високих технологија између различитих партнера, посебно у оквиру индустрије;
- успостављање посебних концерна за развој нових технологија;
- развој механизама менаџмента којима се пружа заштита, олакшава идентификација и савладавају претње везане за информациону инфраструктуру;
- успостављање чвршћих облика експертске сарадње између различитих међународних организација, тела и асоцијација (нпр. Савета Европе и Г8);
- развој принципâ сарадње (*Memorandum of Understanding*, *Codes of Practice in line with the legal framework*).[797]

Са аспекта националних држава али и међународне заједнице, посебна пажња посвећује се супротстављању оним актерима у кибер простору који у постизању својих циљева користе терор. Спровођење цензуре над Интернетом свакако би поспешило борбу против тероризма. Цензурисање садржаја у глобалној мрежи, са друге стране, нарушило би њен демократски карактер. Контрола

[796] Такозвани Computer Analysis and Response Teams (CART) – према: Дракулић М., Дракулић Р., *op. cit*.
[797] *Ibid*.

Интернета и ограничавање приступа одразили би се на све његове кориснике. У својој садашњој „отвореној“ форми Интернет је отелотворење демократских идеала слобода мисли и изражавања и представља извор идеја без премца у историји човечанства. Уколико бисмо због терориста морали да ограничимо и властиту слободу, омогућили бисмо победу терористима и задали ударац демократији, сматра Вајман.[798]

Неопходно је, дакле, пронаћи компромис између борбе против тероризма и очувања грађанских слобода. Многе од до сада предузетих мера (на пример, затварање сумњивих и доказано терористичких *web*-сајтова), које су иницирале поједине владе, нису се показале успешним. Испоставило се да је уклањање терористе из глобалне комуникационе мреже врло тежак задатак, с обзиром на то да су услуге закупа *web*-простора (*web hosting*-а)[799] често бесплатне или могу бити купљене без давања било каквог личног податка осим броја кредитне картице. Дакле, и када се терористички сајтови затворе, они се убрзо појављују поново, јер им то омогућавају други провајдери, несвесни садржаја који се публикује путем њиховог сервера.

Делимично решење овог проблема могло би се постићи сарадњом локалних Интернет-провајдера (ISP), који би морали да континуирано контролишу садржај сајтова помоћу специјализованих „sniffer“-програма. Ови програми су у стању да трагају за кључним, задатим речима, те да укажу на евентуалне терористичке садржаје. Неки експерти сматрају да би, уместо „лова“ на такве сајтове, безбедносне службе требало дубље да се позабаве анализом и тумачењем садржаја терористичких сајтова. Херменеутички приступ би допринео увећавању фонда знања о терористичкој идеологији и унапредио разумевање симболичке и шифроване комуникације. Многи аналитичари сматрају да је обавештајни систем САД већ дуже време посвећен овој врсти мониторинга.[800]

---

[798] Weimann G.: “Terror Groups Exploit Internet for Communications, Recruiting, Training*”, JINSA Policy Forum*, http://www.jinsa.org

[799] Web hosting је сервис који омогућава закуп Интернет-сајта. Закупац може на страницама сајта приказивати мултимедијалне садржаје по сопственом избору. Web hosting-сервис је обично намењен фирмама које од провајдера закупљују простор на серверу. Парадоксално, многи терористички сајтови отворени су посредством америчких фирми са седиштем у САД.

[800] Weimann G.: *Terror Groups Exploit Internet for Communications, Recruiting, Training*, *op. cit*.

Задатак истраживања, мониторинга и анализе терористичке комуникације у Мрежи није нимало једноставан. Први значајнији резултати у том смислу постигнути су употребом америчког система „Carnivore“ (или DCS1000). Овај систем је развијен под покровитељством FBI-ја 1996. године да би помогао федералним властима у криминалистичким истрагама. Систем је коришћен, уз ауторизацију тужилаштва, ради „пресретања“ порука електронске поште послатих са адресе осумњиченог. Подаци прикупљени на овај начин остају на располагању безбедносној служби ради анализе. Да би могао функционисати, систем мора бити инсталиран у сарадњи са локалним провајдером, који корисника над којим се врши истрага снабдева услугом повезивања на Интернет. Остали системи које користе америчке безбедносне службе јесу „Magic Lantern“, „Fluent“ и „Oasis“.

„Magic Lantern“ инсталира софтвер (малициозни програм типа *keylogger*) на рачунар осумњиченог. *Keylogger* је у стању да препозна тачне дигиталне карактере и пренесе их централи FBI-ја. На овај начин се могу прикупити лозинке које је осумњичени користио ради шифровања информација меморисаних у рачунару. Малициозни кôд може бити послат путем електронске поште или „засејан“ у рачунар информатичким нападом.[801]

„Fluent“ омогућава анализу докумената написаних у различитим програмским језицима, док се „Oasis“ користи за транспоновање аудио- и видео-сигнала у текстуалну форму и у стању је да разликује речи и дијалекте различитих језика (арапског, кинеског и енглеског). О корисности овог система довољно говори податак да „Oasis“ анализира тридесетоминутни запис за само десет минута, у односу на деведесет минута, колико је потребно експерту-аналитичару.

Ограниченост ових система представљена је количином података, која често премашује њихове техничке способности. Разноврсне технике комуникације које користе терористи чине овај задатак још компликованијим за аналитичаре, јер онемогућавају моментано разабирање битних од небитних података. Познато је, на пример, да су неке назнаке могућег терористичког напада против Америке уочене пре 11. септембра 2001, али су биле толико уопштене да није било могуће дефинисати начин и време извршења.

---

[801] Sullivan B.: *FBI software cracks encryption wall*, 2001, http://www.msnbc.com

Дакле, тренутно расположиве технологије, иако представљају користан инструмент у истрази и борби против тероризма, још нису у стању да прикупе довољно података за правовремену реакцију. С друге стране, употреба ових технологија отвара и етичке дилеме – како оне могу бити ефикасно коришћене у једном демократском и отвореном друштву а да не повреде његове основне принципе. По свему судећи, сваки корисник глобалне мреже биће у скоријој будућности изложен контроли у погледу „путовања“ информационим магистралама, навика или комуникације и, следствено томе, изложен ризику да постане „анатемисан“ због посете сумњивом сајту или употребе одређених симбола и израза. Међу једноставније и прикладније превентивне мере спадају повећање степена сарадње између различитих агенција за цивилну и војну безбедност у размени и интерпретацији информација, као и уклањање осетљивих информација са Интернета, оних које би могле да буду од користи терористима и другим злонамерним актерима у односу на њихове потенцијалне циљеве.

ЗАКЉУЧНА РАЗМАТРАЊА

Друштвени конфликти су историјска и актуелна константа људског друштва те се могу сматрати једном од најупечатљивијих карактеристика историје људског рода. Друштвени сукоби су сложени и структуирани јер произлазе из разлика у положају, интересима и вредносним оријентацијама социјалних група које су у конфликтној интеракцији. Они се разликују и по својој природи, функцији, интензитету, носиоцима, средствима која се користе, последицама, начинима разрешавања, окончавања итд.

Ратни сукоби јесу најстарији и најекстремнији облик друштвених конфликата. На крају XX и почетку XXI века ратни сукоби су попримили одређене, специфичне карактеристике по питању припреме за рат, начина његовог вођења (средстава и технике), учесника и ефеката. У настојању да истакну одређена својства савремених ратова, теоретичари их сврставају у „епохе“ или „генерације“, односно покушавају да им надену одређене квалификације са аспекта интензитета, односа снага, поштовања правила или утицаја на емоције као детерминишућих атрибута. Према томе, можемо закључити да у научној литератури не постоји јединствен приступ феномену рата. Неслагања су изражена не само у дефиницији ратног сукоба већ и у приступима класификацији ратова. Феномен савременог рата, дакле, још увек није у потпуности дефинисан, класификован и садржајно одређен.

Са друге стране, по питању узрока ратова сагласност постоји. Узроци свих досадашњих ратова, па и савремених, превасходно се налазе у економским мотивима и политичким интересима. Као и сви конфликти, и ратни сукоби настају из супротстављености и противречности интереса и вредности. Дакле, кроз историју се само мењала форма рата али нису се мењали покретачки мотиви за њихово вођење.

Доминантну улогу у савременом друштву, као и у војним активностима, заузела је информационо-комуникациона технологија. Развој информатичких наука у другој половини прошлог века и примена информационо-комуникационих технологија у свим сферама друштвеног живота у последњој деценији прошлог века произвели су ефекат информатизације друштва.

Научна открића и технолошке иновације су, у другој половини XX века, у знатној мери допринели развоју софистициране ратне технике а тиме, посредно, и

измени својстава савремених ратова. Развој технологија за пренос информација (звука, слике и мултимедијалних садржаја) је у великој мери отворио и могућности за управљање перцепцијом током ратних сукоба. Мас-медији постају значајан чинилац (средство) у рату од шездесетих година прошлог века. Револуција медија и информационих технологија суштински је променила не само начин интеракције у друштву, већ и начин на који државе (и паравојне, антидржавне формације) воде ратове. Непрекидном фузијом револуционарних достигнућа на пољу рачунара, сателитских комуникација и медија радикално су унапређене могућности ратовања и поред тога што информационо-комуникациона револуција није суштински изменила геостратешке и политичко-економске циљеве самог рата.

Можемо констатовати да су коришћење најмодерније технике и употреба савремених информационо-комуникационих технологија, током ратних сукоба, довели до следећих међусобно условљених карактеристика савремених ратова: смањења могућности за постизање стратегијског изненађења; повећања улоге специјалних дејстава; учешћа паравојних формација и цивила у ратним сукобима; повећања улоге мас-медија и могућности за „препарирање“ јавног мњења; и промене улоге и значаја категорија простора и времена.

Прекретницу у сфери војних активности али и поимања националне, регионалне и глобалне безбедности представљао је настанак кибер простора. Нови „простор“ пружио је енормне могућности за спровођење специјалних пропагандних дејстава али и извођење напада посредством рачунарских мрежа на противничке информационе системе. За овај нови вид конфронтације у виртуелном простору се у англосаксонском говорном подручју користи појам *кибер ратовање*. Напади у виртуелном простору, наоко неприметни, могу у реалном, физичком, свету резултовати људским жртвама и материјалним разарањима. Због тога је кибер ратовање данас у жижи интересовања теоретичара и стручњака из области војних, информатичких, правних и безбедносних наука.

Израз кибер ратовање води порекло из војних доктринарних и стратегијских докумената САД. У научној и стручној литератури се изрази *информационо ратовање* и *кибер ратовање* често синонимно употребљавају. Други појам је, међутим, ужи по обиму јер снажно наглашава рачунарске и мрежне аспекте информационог ратовања. Због тога се, сматрамо, под прихватљивом дефиницијом кибер ратовања може подразумевати свака дефиниција информационог ратовања

која садржи рачунарску мрежу као просторну одредницу дефиниендума, тј. у којој се активност информационог ратовања одвија посредством рачунарске мреже.

Са семантичког аспекта значајна је и разлика коју поједини аутори праве између појма кибер ратовање и „појмова са сродним значењем“ међу које сврставају: кибер криминал, хактивизам, кибер шпијунажу и кибер тероризам. Друга група аутора, пак, не прави разлику између кибер ратовања и појмова са сродним значењем већ појам кибер ратовање употребљава као збирни назив за свеукупност поменутих активности и тенденција. У битно обележје кибер ратовања они сврставају и тенденцију његовог померања изван војних граница на индивидуалну, друштвену и комерцијалну раван. Док је појмовно одређење информационог ратовања истицало његову војну димензију, данас већи део литературе о кибер ратовању истиче аспект његовог проширења ван војних области. Термин кибер ратовање се, дакле, најчешће употребљава да опише широк распон активности на индивидуалном, друштвено-социјеталном, корпоративно-економском и војном нивоу.

У намери да феномену кибер ратовања приступимо холистички, у његовој анализи смо пошли од претпоставке да је овај појам најшири по обиму те да обухвата и оне активности које поједини теоретичари подводе под појмове са сродним значењем. Другим речима, под овим појмом подразумевали смо и оне активности које се подводе под војни аспект као и оне активности које се приписују недржавним актерима (паравојним и нерегуларним формацијама и индивидуалним корисницима глобалне рачунарске мреже).

На основу прегледа релевантне литературе и резултата спроведене конфликтолошке анализе која је подразумевала засебно, рашчлањено, проучавање елемената структуре појединих кибер конфликата израженог интензитета, дошли смо до сазнања о субјектима (актерима) кибер ратовања, објектима кибер ратовања и средствима и техникама које се користе приликом конфронтација у кибер простору. Средства и технике кибер ратовања смо класификовали у две основне категорије: кибер нападе и пропаганду. Кибер нападе смо, даље, рашчланили на две поткатегорије: средства за аутоматизовано прикупљање информација и извођење напада, и специјалне технике обмањивања на индивидуалном нивоу. Идентификовали смо и класификовали објекте кибер ратовања у три категорије: информације, критичну информациону инфраструктуру и системе за аутоматизацију и управљање индустријским процесима. Наведене класификације су нам омогућиле

да сачинимо и класификацију субјеката претњи у кибер простору на основу покретачког, мотивационог фактора, и техника и инструмената за извршење кибер напада.

Засебно спроведена анализа сличности и разлика између кинетичког и кибер ратовања навела нас је на закључак да људски фактор у значајној мери одређује почетак, ток и исход сваког конфликта, како у физичком тако и у кибер свету. Осим овог фактора, конфликти у физичком и виртуелном свету, чини се, имају мало тога заједничког. Спроведена анализа наводи на закључак да се кибер ратовање, по већини својих карактеристика и принципа, разликује од конвенционалног, кинетичког ратовања. Једна од основних разлика између кибер ратовања и кинетичког ратовања јесте у природи њихових окружења. Кинетичко ратовање се одиграва у физичком свету, руководи се законима физике које познајемо и разумемо. Кибер ратовање се одиграва у вештачком свету који је тешко предвидив и подложан брзим променама. Уочили смо да се на кибер ратовање могу применити неки од принципа кинетичког ратовања али да већина других, традиционалних принципа, има мали значај у кибер простору или га уопште нема. Због ових разлога принципи кибер ратовања су, извесно, различити од оних који важе за кинетичко ратовање.

У складу са холистичким приступом и предметом истраживања који је дефинисан као идентификација и класификација савремених облика сукобљавања у кибер простору, покушали смо да сачинимо једну потпунију класификацију видова кибер ратовања. Једну од тешкоћа приликом сваког покушаја класификације представља чињеница да је број кибер претњи које могу угрозити појединца, друштво или државу практично неограничен, због чега их је и немогуће све предвидети. Другим речима, свакој класификацији се може замерити одређени степен непотпуности. Такође, треба имати у виду да међу појединим претњама постоји одређена међузависност, која условљава да појава једне претње иницира и појаву друге, као и да повећање интензитета једне аутоматски утиче и на повећање интензитета друге претње. Зато идентификација претњи захтева наглашену опрезност, из простог разлога што се претња која није била идентификована често може показати као катастрофална. Из тог разлога се поставља и питање избора адекватног методолошког приступа, посебно зато што у вези са овим проблемом ни на нивоу теорије још не постоји јединствено мишљење, нити изграђено јединствено решење. Са друге стране, неизбежно је разврставање претњи из широког спектра

кибер конфликата у групе које, у извесном смислу, представљају логичке целине. Овакав приступ омогућава анализу сваке претње понаособ, што је неопходан корак за формулисање адекватне политике заштите. На основу увида у досадашња истраживања, и обављених дескрипција и систематизација, понудили смо, верујемо, једну од потпунијих класификација аспеката кибер ратовања. Издвојили смо четири аспекта кибер ратовања: војни, корпоративно-економски, индивидуални и друштвено-социјетални аспект. Наведена класификација је направљена на основу претходно добијених сазнања о субјектима кибер ратовања, њиховој мотивисаности за извођење кибер напада, мета напада и циљева који се нападом желе постићи. Осим анализе поменутих критеријума класификације, исцрпно смо описали и начине изазивања претње и поткрепили их чињеничним аргументима. Услед бројности актера кибер ратовања, али и ускраћености за приступ релевантним изворима сазнања (на пример, по питању субверзивне активности обавештајних служби у кибер простору), класификацијом смо обухватили оне субјекте кибер ратовања за које смо имали релевантне податке и у оној мери која, надамо се, задовољава епистемолошке критеријуме ове врсте истраживања.

Узимајући у обзир недостатак консензуса по питању формално-правног власништва над кибер простором, постојање националних и регионалних развојних диспаритета као и глобално изражену борбу за доминацију у кибер простору, можемо предвидети тенденцију раста активности кибер ратовања у будућности. Тим пре, што се број корисника глобалне мреже непрекидно увећава док цена рачунара, рачунарске опреме и софтвера опада. То чини алате кибер ратовања широко доступнима, свим потенцијалним актерима кибер конфликата.

Супротстављање кибер ратовању јесте тежак задатак, из више разлога – на првоме месту, због тога што је релативно једноставно сачувати анонимност у кибер простору и зато што је физичко место у којем се налази агресор готово увек различито од локације на којој се налази жртва. Територијална удаљеност узрокује проблеме не само у откривању и хватању извршилаца већ и у смислу неусаглашености националних правних легислатива. Хармонизација националних законика и међународна кооперација на свим нивоима представљају могуће решење које, да би било ефикасно, мора укључити што већи број земаља. Са применљивим правним мерама за заштиту кибер простора повезана је и тема одбране цивилних слобода. Спровођење ригорозних мера контроле корисника Мреже, ради откривања

евентуалних злоупотреба, могло би да знатно ограничи слободу изражавања и приватност грађана. На тај начин би се изгубила једна од основних врлина кибер простора – доступност информација и нових стимуланса, који се могу родити и ширити само у слободном изражавању.

Са аспекта националне, регионалне и глобалне безбедности, међутим, разумљива је теза по којој се безбедан кибер простор сматра императивом информационог доба. Не треба, међутим, сметнути с ума да се природа кибер простора противи стању апсолутне безбедности. Брзина којом се претње увећавају захтева усвајање поузданих, брзих и ефикасних безбедносних мера које треба да буду дискриминишуће према творцима претње. Ефикасан одговор претњама није могуће пружити само правним мерама. Задовољавајући степен заштите кибер простора није могуће постићи ни усвајањем и спровођењем техничких мера, већ, изнад свега, синергијским спровођењем серије противмера од стране међународних организација, државних институција, експертских удружења и индивидуалних корисника информационих система.

Заштитне активности, према томе, морају подразумевати константан напор свих оних који су одговорни за функционисање информационе инфраструктуре. На индивидуалном нивоу, однос корисника према информационим системима може да обезвреди и најсавременије и најскупље лимитирајуће безбедносне системе. Сваки корисник, дакле, има важну улогу у унапређивању безбедности кибер простора. Било који рачунар, уколико није адекватно заштићен, може постати објект и/или средство напада против других система. Према томе, промовисање безбедносне културе и развој компјутерске етике чине један од приоритета информационог доба.

Из претходно реченог може се закључити да је спроведено истраживање отворило читав низ правних, социолошких, психолошких, војних, политиколошких, етичких и семантичких питања на која ће бити потребно дати одговор у будућности. Са безбедносног аспекта, пак, мишљења смо да је наше истраживање идентификовало два кључна проблема везана за феномен сукобљавања у кибер простору: 1) терминолошки и семантички пробеми и 2) правна неодређеност, тј. правни статус ове врсте сукоба.

Са семантичког аспекта, увођење (преузимање) туђица из корпуса информационих и војних наука у српски језик додатно отежава анализу, тумачење, класификацију и разјашњење нових безбедносних феномена. У том смислу, један од

посебно значајних проблема јесте и оправданост употребе појма кибер рат, тј. подвођење овог спектра активности под категорију ратних сукоба. Чињеница је да међу теоретичарима нема сагласности по овом питању. Ми смо у засебном одељку рада покушали да дамо један предлог решења за овај проблем, свесни чињенице да је и он подложан критици. Намера нам је била скромна – да подстакнемо академску јавност на промишљање. Верујемо да је бар терминолошке проблеме могуће решити уколико постоји спремност и добра воља да се направи консензус по питању нормирања основних појмова и техничких термина. Значење и денотација неког појма, па и појма кибер ратовање су, на крају, само ствар конвенције.

И поред тога што се активности које називамо кибер ратовањем спроводе већ више од деценије, за њих се још увек није нашла адекватна правна дефиниција. Целокупно поље кибер права је још увек недовољно развијено. Покушаји примене постојећих модела из међународног ратног права на ову област показали су се непримереним. Осим тога, није постигнута општа сагласност о међународним споразумима који би разјаснили правни статус држава и недржавних актера у кибер конфликтима.

На практичној равни, пак, кибер напади јесу једна од највећих претњи националној безбедности у XXI веку. Због тога технолошки развијене земље поимају осигурање властитог сегмента кибер простора као апсолутни императив. У идеалном свету државе би заједнички радиле на томе да елиминишу кибер нападе. Нажалост, то није случај. Глобална сарадња можда може постати реалност једног дана, али до тога неће доћи све док се не деси нешто што ће извршити притисак на државе које пружају уточиште актерима кибер напада да промене своје понашање.

Један од начина да се достигне стање повећане безбедности кибер простора јесте примена мера активне одбране против кибер напада који долазе из „недодирљивих" држава. Уколико би се постигла сагласност о примени мера активне одбране на међународном нивоу, не само да би државе-жртве могле боље да се заштите од кибер напада, већ би се и стало на пут агресији јер би се државе-уточишта приморале на поштовање преузетих међународних обавеза. На крају крајева, ниједна држава не жели да друга држава употребљава силу унутар њених граница, чак ни електронских. Пошто државе тренутно не користе мере активне одбране, свака одлука да се оне почну примењивати, представљала би одступање од

досадашње праксе. Као и сваки предлог који није у складу са актуелном праксом, и овај предлог ће морати да прође кроз процес јавне дискусије и правне критике.

На крају, можемо закључити да кибер рат јесте релативно нов и специфичан облик друштвеног конфликта који се води у специфичном окружењу, специфичним средствима, са специфичним обележјима и принципима. Он може бити рат без жртава али то не мора бити случај. Он се може водити самостално или као подршка конвенционалном, кинетичком, сукобу. Он више није ни облик тајног оружја које се држи скривено од противника и јавности. Он је јаван, а његове последице најчешће трпе цивилно становништво и привредне корпорације који покрећу државу. Кибер рат није алтернатива конвенционалном рату већ потпуно нов облик друштвених конфликата.

Покушали смо да докажемо да активност кибер ратовања не мора бити ограничена војним дискурсом. Принципи кибер ратовања присутни су у различитим друштвеним контекстима, мада распон мотивација и пракси може веома да варира. Кибер ратници користе добро промишљене тактике и стратегије како би тачно одредили мете својих напада и постигли своје циљеве на начин који наликује војним методама. Деструктивне акције различитих индивидуалних и групних субјеката у кибер простору могу имати сличне пориве, показати слична схватања (свесна или несвесна) стратешких предности које омогућавају методе напада засноване на информационим технологијама, и бити одмазда против оних чији животи у великој мери зависе од употребе комплексних информационих и комуникационих система.

Кибер ратовање не само да преиспитује одређене конвенционалне претпоставке о природи конфликата и потенцијалним упориштима компаративних предности, већ у исто време и илуструје неке од скривених могућности и парадоксалних потенцијала (социјална фузија и фисија) глобално умрежених технологија. Оно, такође, покреће мноштво питања везаних за етичност офанзивног кибер ратовања и адекватност постојећих мултилатералних прописа и конвенција у које би се ови нови модалитети могли уклопити.

Раздвојени од својих војних корена, вокабулар и принципи кибер ратовања могу имати велику аналитичку применљивост. Различити аспекти кибер конфликата, који су у раду приказани, могу се подвести под опште теоријске принципе и установљене карактеристике феномена који смо дефинисали појмом кибер ратовање. Умрежене технологије и појава комплексних рачунарских заједница стварају услове

који омогућавају мултидимензионално кибер ратовање, иако већи број научних и стручних анализа и дискусија, које се баве последицама које на друштво има свеприсутна употреба рачунара, не може пружити одговарајуће доказе за ове потенцијално дистопијске последице. Истраживање ефеката које употреба информационо-комуникационих технологија има на друштво било би додатно поспешено прихватањем консензуса по питању вокабулара, као и систематским проучавањем дугорочних импликација трендова идентификованих овим истраживањем.

ЛИТЕРАТУРА

1. "Active Engagement, Modern Defence", *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation*, Adopted by Heads of State and Government, Lisbon, 2010.
2. Adams J.: *The next world war: Computers are the weapons and the front line is everywhere*, Simon & Schuster, New York, 1998.
3. Adkins N. B.: *The Spectrum of Cyber Conflict From Hacking to Information Warfare:What is Law Enforcement's Role?*, Air Command and Staff College, Air University, Alabama, 2001.
4. Agee P.: *Dnevnik agenta*, Globus, Zagreb, 1975.
5. Alberts D., Papp D.: *The Information Age: An Anthology of Its Impacts and Consequences*, Volume III, National Defense University Press, Washington D.C., 2001.
6. Alford L. D.: "Cyber Warfare: Protecting Military Systems", *The Journal of the Defense Acquisition University Review*, Quarterly 7, No. 2., USAF, 2000.
7. "*Al Jazeera* Tops Net Search Requests", *Associated Press,* Aprile 11, 2003.
8. Anderson S., Cavanagh J.: "Corporate Empires"*, Multinational Monitor*, Vol. 17, No. 12, December 1996.
9. Arora K., et al.: "Impact Analysis of Recent DDoS Attacks", *International Journal on Computer Science and Engineering,* Vol. 3, No. 2, Feb 2011.
10. Arquilla J., Ronfeldt D.: *Networks and Netwars: The Future of Terror, Crime, and Militancy*, RAND, Santa Monica, California, 2001.
11. Арсић С.: „Нова теорија ратовања – против људског ума", *Одбрана*, 1. фебруар 2008.
12. Ashley B.: *Anatomy of Cyberterrorism: Is America Vulnerable?*, Research Paper, Air War College, Air University, Maxwell AFB, 2003.
13. Аврамов С.: *Постхеројски рат запада против Југославије*, I том, Ветерник, 1997.
14. Аврамов С., Креча М.: *Међународно јавно право*, Правни факултет Универзитета у Београду и Службени гласник, Београд, 2006.
15. Бараћ Д.: *Real-time оперативни системи за мале embedded системе*, Универзитет у Нишу, Електронски факултет, Ниш, 2010.
16. Барбуловић С., et al.: *Амнезија јавности – од пропаганде до тероризма*, Графо-комерц, Београд, 2004.
17. Беговић А., Прелевић М., Мркић С.: *Теорија о рату*, Војноиздавачки завод, Београд, 1978.
18. Bell D.: *The Coming of Post-Industrial Society: A Venture in Social Forecasting*, Basic Books, New York, 1973.
19. Bergen P. L.: *Holy War, Inc. Inside the secret world of Osama bin Laden*, The Free Press, New York, 2002.
20. *Безбедност и информационе технологије: нова средства и изазови*, Парламентарни надзор безбедносног сектора: начела, механизми и пракса,

Приручник за посланике број 5, Центар за цивилно-војне односе, Београд, 2003.
21. Bimbo S., Colaiacovo E.: *Sistemi SCADA - Supervisory control and data acquisition*, APOGEO srl, Milano, 2006.
22. Благојевић М.: „Социолошко проучавање друштвеног сукоба“*, На граници векова*, бр. 1-96, Универзитет у Београду, Београд, 1996.
23. Buxbaum P.: “U.S. Grapples with Cybersecurity”, *ISN Security Watch*, October 10, 2007.
24. Бошковић М., Путник Н.: *Улога друштвених мрежа у савременим социо-политичким и безбедносним појавама*, XIX Телекомуникациони Форум – Телфор, зборник радова, Београд, 2011.
25. Carr J.: *Inside Cyber Warfare*, O’Reilly Media, Sebastopol, 2010.
26. Cassese A.: *International Law*, Oxford University Press, New York, 2005.
27. Chirillo J.: *Hack Attacks Revealed – A Complete Reference with Custom Security Hacking Toolkit*, John Wiley & Sons, New York, 2001.
28. Clarke R., Knake R.: *Cyber War*, Harper Collins Publishers, New York, 2010.
29. Coser L.: *Functions of Social Conflict*, The Free Press, Cohtier-Macmillian Ltd. London, 1996.
30. Cronin B.: “Digibabble“, *International Journal of Information Management*, 18(1), 1998.
31. Cronin B., Crawford H.: “Information warfare: Its applications in military and civilian contexts”, *Information Society*, 15(4), 1999.
32. *Cross-dimensional aspects of security*, OSCE, SEC.GAL/150/04, 29 June 2004.
33. Cusumano M. A., Yoffie D. B.: *Competing on Internet time: Lessons from Netscape and its battle with Microsoft*, Free Press, New York, 1998.
34. Цветковић В.: *Социологија*, Факултет цивилне одбране, Београд, 2005.
35. *Cybercrime… Cyberterrorism… Cyberwarfare… Averting an Electronic Waterloo*, CSIS Task Force Report, Washington D.C., 1998.
36. Чомски Н.: *Контрола медија*, Рубикон, Нови Сад, 2008.
37. De Landa M.: *War in the age of intelligent machines*, Swerve Press, New York, 1991.
38. Denning D.: „Cyberwarriors, Activists and Terrorists Turn to Cyberspace“, *Harvard International Review*, Vol. XXIII, No. 2, Summer 2001.
39. Denning D.: *Information warfare and security*, Addison-Wesley, Reading, 1999.
40. Denning D.: “Reflections on Cyberweapons Controls”, *Computer Security Journal*, Vol. XVI, No. 4, 2000.
41. *Department of Defense Joint Publication 3-13*, Joint Doctrine for Information Operations, 9 October 1998.
42. Devost M.: “Hackers as a National Resource”, y: *Information Warfare – Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, Winn Schwartau (Ed.), Thunder’s Mouth Press, New York, 1996.
43. Dibbell J.: “A rape in cyberspace or how an evil clown, a Haitian trickster spirit, two wizards, and a cast of dozens turned a database into a society“, *The Village Voice*, 21 December 1993.

44. Димитријевић В., Стојановић Р., *Међународни односи*, Службени лист СРЈ, Београд, 1996.
45. Дингарац Д., Станчевић Т.: „Српски хакери Црна рука“, *Свет компјутера*, новембар 1998.
46. *Doctrine for Joint Psychological Operations - JP 3-53*, Department of the Army, Department of the Navy, Department of the Air Force, 2003.
47. *Доктрина сукоба ниског интензитета*, ЦОСИС, Београд, 1990.
48. Дракулић М.: *Компјутерски и cyber криминал – како се борити против њега?*, међународна конференција, Центар „Сава“, Београд, 21. 11. 2007.
49. Драшковић Д.: *Савремени ратови*, ИШ Стручна књига, Београд, 1999.
50. Duggan R.: *Insider Adversary Model Briefing*, DARPA IASET Insider Workshop, August 2000.
51. Dunn M., Wigert I.: *International CIIP Handbook 2004*, Center for Security Studies, ETH Zürich, 2004.
52. Џигурски О.: *Информатичко ратовање*, Зборник Факултета цивилне одбране, Београд, 2001.
53. Џигурски О.: *Информатика*, Факултет цивилне одбране, Београд, 2002.
54. Џигурски О.: *Информационе технологије у борби против тероризма*, Зборник Факултета цивилне одбране, Београд, 2005.
55. Џигурски О.: *Могућности заштите од стеганографије*, Зборник Факултета безбедности, Београд, 2008.
56. Џонсон Д.: *Компјутерска етика*, Службени гласник, Београд, 2006.
57. Endorf C., Schultz E., Mellander J.: *Intrusion Detection & Prevention*, McGraw-Hill, 2004.
58. Ерл М.: *Творци модерне стратегије*, Војно дело, Београд, 1952.
59. Erlanger S.: “*Small Serbian Town Is Striken By a Deadly Accident of War*“, *New York Times*, 7 April 1999.
60. Erlanger S.: “*Support for Homeland up as Sirens Wail and News is Censored*“, *New York Times*, 29 March 1999.
61. Erlanger S.: “*Televised Defiance Lost Amid Sirens, Blasts, and Fireballs*“, *New York Times*, 25 March 1999.
62. Fialka J.: *War by Other Means: Economic Espionage in America*, W.W. Norton, New York, 1997.
63. *Field Manual FM 100-6*: *Information operations,* Department of the Army, Washington, DC, 1996.
64. *From cybercrime to cyberwarfare*, “Défense nationale et sécurité collective”, No 6, The Committee for National Defence Studies, Paris, 2008.
65. Ganor B.: *The Counter Terrorism Puzzle*, Interdisciplinary Center of Herzlia and Transaction Publishers, Herzlia, 2005.
66. Gardner H.: *Averting Global War: Regional Challenges, Overextension and Options for American Strategy*, Palgrave, New York, 2007.
67. Gardner H.: “War and the media paradox“, *Cyber Conflict and Global Politics*, Routledge, Abingdon, 2009.

68. German M., Donahue D. A., Schnaars S. P.: "A chink in marketing's armor: Strategy above tactics", *Business Horizons*, March/April 1991.
69. Гибсон В.: *Неуромант*, IPS Media, Београд, 2008.
70. Гиденс Е.: *Социологија*, Економски факултет, Београд, 2003.
71. Glave J.: "Anti-Nuke Cracker Strikes Again", *Wired*, 3 July 1998.
72. Голенкова З. Т.: „Социјалне неједнакости и социјални конфликти", Зборник: *Социјални конфликти у земљама транзиције*, Институт друштвених наука Београд и Руска академија наука, Институт за социолошка истраживања, Београд, 1996.
73. Greenberg L., Goodman S., Soo Hoo K.: *Information Warfare and International Law*, National Defense University, Washington DC, 1998.
74. Група аутора: *Методологија ратне вештине*, ЦВШ, Београд, 1996.
75. Хантингтон С.: *Сукоб цивилизација*, ЦИД, Подгорица, 1998.
76. Harmon A.: "War Waged on Web: Killers Without Context", *New York Times*, 5 April 1999.
77. Harmon A.: "Serbs' Revenge: NATO Web Site Zapped", *New York Times*, 1 April 1999.
78. *Harper's Magazine*, October 2002.
79. Харт Л.: *Стратегија посредног прилажења*, Војно дело, Београд, 1952.
80. Hauslohner A.: "Is Egypt about to have a Facebook revolution", *The Time*, January 24th, 2011.
81. Херман Е., Мекчесни Р.: *Глобални медији – нови мисионари корпоративног капитализма*, Клио, Београд, 2004.
82. Hoffmann L.: "U.S. Opened Cyber-War During Kosovo Fight", *Washington Times*, October 24, 1999.
83. Hoffman B.: *Modern Terrorism Trends – Reevaluation After 9/11*, у: Ganor & Boaz (eds.), *Post Modern Terrorism*, Interdisciplinary Center of Herzlia, Herzlia, 2005.
84. Homer-Dixon T.: "The Rise of Complex Terrorism", *Foreign Policy*, January/February 2002.
85. Hubbard Z.: "Information Warfare in Kosovo", *Journal of Electronic Defense*, Vol. 22, No. 1, November 1999.
86. Huntington S.: "The Age of Muslim Wars", *Nesweek*, Special Davos Edition, December 2001.
87. Hutchinson W.: "Concepts in information warfare", *Logistics Information Management*, 15(5/6), 2002.
88. Ifrah L.: "Europe Confronted by Digital Crime", *European Issues*, No. 70, 2007.
89. Ifrah L.: "The Georgia-Russia conflict: Internet, the other battlefield", *Défense nationale et sécurité collective*, October 2008, Committee for National Defence Studies, Paris, 2008.
90. *Instrumentation Symbols and Identification*: *ANSI/ISA–5.1–1984 (R1992)*, ISA – The Instrumentation, Systems, and Automation Society, North Carolina, 1992.
91. Јакшић П.: *Савремени рат II*, Вук Караџић, Београд, 1969.

92. Janczewski L., Colarik A.: *Cyber Warfare and Cyber Terrorism*, Information Science Reference (an imprint of IGI Global), Hershey, 2008.
93. Jinks D.: "State Responsibility for the Acts of Private Armed Groups", *Chicago Journal of International Law*, Vol. 4, 2003.
94. Johnson K. L.: *Secret Agencies. U.S. Intelligence in a Hostile World*, Yale University Press, 1996.
95. *Joint Doctrine for Electronic Warfare - JP 3-51*, Department of the Army, Department of the Navy, Department of the Air Force, 2000.
96. *Joint Doctrine for Information Operations - JP 3-13*, Department of the Army, Department of the Navy, Department of the Air Force, 1998.
97. *Joint Doctrine for Military Deception* - JP 3-58, Department of the Army, Department of the Navy, Department of the Air Force, 1994.
98. José Rios M., Tenreiro de Magalhães S., Santos L., Jahankhani H.: "The Georgia's Cyberwar", Jahankhani H., Hessami G. A., Hsu F. (Eds.), *Global Security, Safety and Sustainability*, 5th International Conference, ICGS3 2009, London, September 1-2, Springer-Verlag, Berlin – Heidelberg, 2009.
99. Joyal M. P.: *Industrial Espionage Today and Information Wars of Tomorrow*, 19th National Information Systems Security Conference, Baltimore Convetion Centre, Baltimore, October 22-25, 1996.
100. Katz J.: "The digital citizen", *Wired* 5(12), 1997.
101. Kaufman M.: "Bush Sets Defense As Space Priority", *Washington post*, October 18, 2006.
102. Кегли Ч., Виткоф Ј.: *Светска политика, тренд и трансформација*, Желнид, Београд, 2006.
103. Kheng Lee Gregory Tan, *Confronting cyberterrorism with cyber deception*, Master's Thesis, Naval Postgraduate School, Monterey, California, 2003.
104. „Кина спремна за cyber-рат", *Com&GSM*, М3 d.o.o., бр. 236, Београд, 2007.
105. Клаузевиц К.: *О рату*, Војно дело, Београд, 1951.
106. Knapp K., Boulton W.: *Ten Information Warfare Trends*, in Janczewski L., Colarik A.: *Cyber Warfare and Cyber Terrorism*, Information Science Reference (an imprint of IGI Global), Hershey, 2008.
107. Ковачевић Б.: *Рат,* Светови, Нови Сад, 1995.
108. Ковачевић Ж.: *Компјутерска шпијунажа и заштита*, мастер рад, Факултет безбедности, Београд, 2010.
109. Krasner S.: "Sovereignty", *Foreign Policy*, January/Februrary 2001.
110. Кукрика М.: *Управљање сигурношћу информација*, INFOhome Press, Београд, 2002.
111. Курмон Б., Рибникар Д.: *Асиметрични ратови – сукоби јуче и данас, тероризам и нове претње*, НИЦ Војска, Београд, 2003.
112. Kushnick B.: *The Unauthorized Biography of the Baby Bells & Info-Scandal*, New Networks Institute, 1999.
113. *L' Armement*, No. 60, XII., Paris, 1997 - I. 1998.

114. Larsen A. W.: *Serbian Information Operations During Operation Allied Force*, Air Command and Staff College, Air University, Maxwell Air Force Base, Alabama, 2000.
115. *Le Monde,* April 4, 2003.
116. Libicki M. C.: *What is information warfare?*, National Defense University, Institute for National Strategic Studies, Washington DC, 1995.
117. Lind W.: *The Changing Face of War: Into the Fourth Generation*, Marine Corps Gazette, October 1989.
118. Marić I.: *Sustav za privlačenje i detekciju napadača*, Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, Zagreb, 2006.
119. Маринковић Д.: „Основе прикупљања података и управљања", *Микроелектроника*, Београд, бр. 1, мај 1998.
120. Marlin S., Garvey M.: "Disaster-Recovery Spending on the Rise", *Information Week*, August 9, 2004.
121. Матовић Ј.: *Војни послови Југославије и свет XX века,* Тетра ГМ, Београд, 2003.
122. McCrohan K. F.: "Competitive intelligence: Preparing for the information war", *Long Range Planning* 31(4), 1998.
123. McLuhan M.: *Razumijevanje medija,* Golden Marketing i Tehnička knjiga, Zagreb, 2008.
124. Meinel C. P.: "How hackers break in... and how they are caught", *Scientific American*, October 1998.
125. Микић С.: *Поглед на рат,* Генералштаб војске Србије и Црне Горе, Управа за школство и обуку, Војна академија, Београд, 2003.
126. Микић С.: *О рату*, Прометеј, Нови Сад, 2006.
127. Милашиновић Р., Милашиновић С.: *Увод у теорије конфликата,* Факултет цивилне одбране, Београд, 2004.
128. Милашиновић Р., Милашиновић С.: *Основи теорије конфликата*, Факултет безбедности, Београд, 2007.
129. Милашиновић Р.: „Могућности успостављања мира у свету и превенција конфликата", *Кризни менаџмент I – превенција кризе*, хрестоматија, Факултет безбедности, Београд, 2006.
130. Милашиновић Р.: *Терор Запада над светом - савремени механизми разарања и подчињавања суверених земаља и народа*, Институт за криминолошка истраживања, Београд, 1998.
131. Милашиновић Р., Путник Н.: „Герила као специфичан вид друштвеног конфликта", *Герила на Балкану: борци за слободу, бунтовници или бандити*, Tokyo: University Meiji, Institute for Disarmament and Peace Studies, Београд: Институт за савремену историју, Факултет безбедности, 2006.
132. Милашиновић С.: *Друштвени сукоби у земљама Централне и Југоисточне Европе*, Докторска дисертација, Факултет политичких наука у Београду, 2003.

133. Milašinović S.: "Social conflicts and postsocialist east-european societies", *Science – Security-Police*, Journal of Academy of Criminalistic and Police Studies, Belgrade, Vol. VI, No. 2/2001.
134. Миловановић Г., *Концепт информационог друштва и друштвени ефекти интернета*, Центар за проучавање информационих технологија, Београдска отворена школа, Београд.
135. Милошевић М.: *Социјални и психолошки фактори криминалне мотивације терористa*, Универзитет у Београду – Факултет безбедности, Београд, 2009.
136. Мишић М.: „Нова фаза сајбер-ратовања", Дневни лист *Политика*, 06.10.2010.
137. Мишић М.: „Време је за сајбер детант", Дневни лист *Политика*, 16. јун 2011.
138. Мишовић С., Ковач М.: *Системи одбране*, Факултет безбедности, Београд, 2006.
139. Merriam-Webster Collegiate Dictionary of English, Tenth Edition, Springfield, Ma.: Merriam-Webster Inc. 1998.
140. Møller B.: "The Faces of war", у: *Реформа сектора безбедности*, зборник радова, прир. Мирослав Хаџић, Г 17 Институт и Центар за цивилно-војне односе, Београд, 2003.
141. Mulvenon J., Tanner S. M., Chase M., et al.: C*hinese Responses to U.S. Military Transformation and Implications for the Department of Defense*, RAND Corporation, 2006.
142. Negroponte N.: *Being Digital*, Alfred A. Knopf Inc., New York, 2005.
143. Nelson B., Choi R., Iacobucci M. *et al*.: *Cyberterror: Prospects and Implications*, Center for the Study of Terrorism and Irregular Warfare, Monterey, 1999.
144. Nugent J., Raisinghani M.: "Bits and Bytes vs. Bullets and Bombs: A New Form of Warfare", y: Janczewski, L., Colarik, A.: *Cyber Warfare and Cyber Terrorism*, Information Science Reference (an imprint of IGI Global), Hershey, 2008.
145. Nye J.: *Bound to lead: The Changing Nature of American Power*, Basic Books, New York, 1990.
146. Palmar I. C., Potter G. A.: *Computer security risk magement*, Jessica Kingsley Publishers, London, 1989.
147. Papp D. S., Alberts D., Tuyahov A.: "Historical Impacts of Information Technologies: An Overview", y: *The Information Age: An Anthology of Its Impact and Consequences*, vol. I, ed. David S. Alberts & Daniel S. Papp, CCRP Publication Series, 1997.
148. Parks R., Duggan D.: *Principles of Cyber-warfare*, Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001.
149. Perešin A.: „Paradigma *novoga* terorizma informacijskoga doba", *Politička misao*, Vol. XLIV, br. 2, Zagreb, 2007.
150. Peters R.: "How Saddam won this round", *Newsweek*, 30 November 1998.
151. Петковић Т.: *Пословна шпијунажа и економско ратовање*, Protexi Group System, Нови Сад, 2009.

152. Петровић С., *Полицијска информатика*, Криминалистичко-полицијска академија, Београд, 2007.
153. Петровић С.: „Кибертероризам“, *Војно дело*, број 2/2001, ВИЗ, Београд, 2001.
154. Петровић С.: *Компјутерски криминал*, МУП Србије, Београд, 2001.
155. Piccitto D.: *Terrorismo: dal fondamentalismo religioso ad Internet*, Facoltà di lettere e filosofia, Facoltà di Scienze Politiche, Università degli Studi di Perugia, 2005.
156. Плескоњић Д., Мачек Н., Ђорђевић Б., Царић М.: *Сигурност рачунарских система и мрежа*, Микро књига, Београд, 2007.
157. Pollitt M.: “Cyberterrorism Fact or Fancy?”, *Proceedings of the 20th National Information Systems Security Conference*, 1997.
158. Priest D.: “Bombing by Committee“, *Washington Post*, 20 September 1999.
159. Putignano D. S.: *La criminalità informatica: cyberterrorismo*, Facoltà di Giurisprudenza, Università degli Studi di Bari, 2002.
160. Путник Н.: *Сајбер простор и безбедносни изазови*, Факултет безбедности, Београд, 2009.
161. Ramirez A.: “Heroes vs. Intruders and Terrorists”, *New York Times*, 29 March 1999.
162. Ратковић Б.: *Војни лексикон*, 2-3, Београд, 1989.
163. Rehman R.: *Intrusion Detection Systems with Snort*, Prentice Hall PTR, 2003.
164. Remondino E.: *La televisione va alla guerra*, Sperling & Kupfer Editori, 2002.
165. *Replacement of Google with Alternative Search Systems in China Documentation and Screen Shots*, Berkman Center for Internet & Society, Harvard Law School, September 2002.
166. Ротмистров: *Историја ратне вештине*, том I, Београд, 1966.
167. „САД и Израел бацили сајбер бомбу на Иран“, Дневни лист *Политика*, 17. јануар 2011, стр. 1.
168. Saita A.: “Antiforensics: The Looming Arms Race”, *Information Security*, Vol. 6, No. 5, 2003.
169. Savarese R.: *Guerre intelligenti*, Franco Angeli, 1992.
170. Scalese A.: *La sicurezza del cyberspazio: analisi e considerazioni*, Facoltà di Scienze Politiche, Università degli Studi di Trieste, 2005.
171. Schmidt A., Jongman A.: *Political Terrorism*, North Holland Publishing Co., Amsterdam, 1988.
172. Schmitt M.: “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework”, *Columbia Journal of Transnational Law*, 37: 885, 1999. pp. 913-15.
173. Schneier B.: *Secrets and Lies. Digital security in a networked world*, Wiley computer publishing, New York, 2000.
174. Schwartau W.: *Information warfare: chaos on the electronic superhighway*, Thunder’s Mouth Press, New York, 1994.
175. Schwartau W.: *Information warfare. Cyberterrorism: Protecting your personal security in the electronic age*, Thunder’s Mouth Press, New York, 1996.

176. Sciolino E.: "Following Attacks, Spain's Governing Party Is Beaten", *The New York Times*, March 15, 2004.
177. Shackleford S.: "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law*, Vol 27, No 1, 2009.
178. Shaw M.: *International Law*, Cambridge University Press, Cambridge, 2004.
179. Симић Д.: *Наука о безбедности, савремени приступи безбедности*, Службени лист, Београд, 2002.
180. Симић Д.: *Позитиван мир – схватања Јохана Галтунга*, Академија Нова, Архив Кљакић, Београд, 1993.
181. Синг С.: *Књига о шифрама – умеће тајних комуникација од древног Египта до квантне криптографије*, ДН Центар, Београд, 2010.
182. Синковски С.: „Информациона безбедност – компонента националне безбедности", *Војно дело*, број 2/2005, ВИЗ, Београд, 2005.
183. Sklerov M.: "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent", *Military Law Review*, No. 201, July 2009.
184. Skoudis E.: *Counter Hack: A Step-By-Step Guide to Computer Attacks and Effective Defenses,* New Jersey, Prentice Hall, 2002.
185. Соколовски: *Војна стратегија*, ВИЗ, Београд, 1965.
186. *Социолошки лексикон*, Савремена администрација, Београд, 1982.
187. *Социолошки речник*, прир. Аљоша Мимица и Марија Богдановић, Завод за уџбенике, Београд, 2007.
188. Spitzner L.: *Honeypots: Tracking hackers*, Addison Wesley, 2002.
189. Стерн Џ.: *Екстремни терористи*, Alexandria press, Београд, 2004.
190. *Стратегија оружане борбе*, ЦЦНО, Београд, 1983.
191. Strano M, Neigre B.,Galdieri P.: *Cyberterrorismo,* Jackson libri, Milano, 2002.
192. Straton R. T.: *Organization of cyberspace forces*, Air Command And Staff College, Air University, Maxwell Air Force Base, Alabama, 2008.
193. Сун Цу: *Умеће ратовања*, Будућност, Нови Сад, 2004.
194. Свечин: *Стратегија*, Војно дело, Београд, 1956.
195. Szafranski R.: "Neo-corticalwarfare: The acme of skill?", *Military Review*, November 1994.
196. Тадић Љ.: *Наука о политици*, Издавачка радна организација „Рад", Београд, 1988.
197. Тадић Љ.: *Политиколошки лексикон*, Завод за уџбенике и наставна средства, Београд, 1966.
198. Tavani H. T.: *Ethics and Technology: Ethical Issues in an Age of Information and Communications Technology*, Hoboken, John Wiley & Sons Inc., 2003.
199. *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities*, William A. O., Kenneth W. D., Herbert S. L., editors, Committee on Offensive Information Warfare, National Research Council, 2009.
200. *The Guardian,* April 4, 2003.
201. *The New Yorker*, March 27, 2003.

202. "The Prevention and control of organised crime: A European Union strategy for the beginning of the new millennium"*, Official Journal*, C124, 2000.
203. "The Science of Strategy", Guangqian P., Youzhi Y., eds., *Military Science Press*, Beijing, 2001.
204. *The Sunday Herald*, September 15, 2002.
205. Thibodeau P.: "Offshore's Rise Is Relentless", *Computerworld*, Vol. 37, No. 26, 2003.
206. Thomas D.: *Hacker Culture*, University of Minnesota, Minneapolis, 2002.
207. Thomas T.: "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *Parameters*, Vol. 33, 2003.
208. Тофлер А.: *Трећи талас,* Просвета, Београд, 1983.
209. Тофлер А., Тофлер Х.: *Рат и антират*, Paideia, Београд, 1998.
210. Трифуновић Д., Стојаковић Г., Врачар М.: *Тероризам и вехабизам*, Филип Вишњић, Београд, 2011.
211. Турен А.: „Увод у проучавање друштвених покрета", *Обнова утопијских енергија*, Београд, 1987.
212. "US and Russia Differ on a Treaty for Cyberspace", *The New York Times*, June 27, 2009.
213. William J. L.: *A Conversation on Cybersecurity*, Brussels, September 15 2010.
214. Wray S.: *Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics*, A paper for The world Wide Web and Contemporary Cultural Theory Conference, Drake University, 1998.
215. Ван Кревелд М.: *Трансформација рата*, Јавно предузеће Службени Гласник и Факултет безбедности, Београд, 2010.
216. Verton D.: *Black Ice: the Invisible threat of Cyber-Terrorism*, The McGraw-Hill Companies, 2003.
217. Винер Н.: *Кибернетика и друштво*, Нолит, Београд, 1973.
218. Вирилио П.: *Информатичка бомба*, Светови, Нови Сад, 2000.
219. Вишњић Д.: *Појам оружане борбе*, ВИНЦ, Београд, 1988.
220. Вишњић Д.: *Тезе о рату*, ЦВШ ВЈ, Београд, 1988.
221. Вучинић З.: *Међународно ратно и хуманитарно право*, Службени гласник, Београд, 2006.
222. Вујановић Н.: „Савремене војне технологије и њихов утицај на б/д", *Нови Гласник*, Година 2, бр. 1, 1994.
223. Вукићевић В.: *Култура и народна одбрана*, ВИЗ, Београд, 1976.
224. Вулетић Д.: „Шта је информационо ратовање?", *Безбедност*, бр. 3, Београд, 2005.
225. Вулетић Д.: *Cyber криминал и могућност његовог откривања*, Докторска дисертација, Факултет организационих наука, Београд, 2008.
226. *Военная мысль*, Номер 3, Москва, 31. март 2007.
227. Волков В.: *Дезинформација – од тројанског коња до интернета*, Наш дом, Београд, 2005.

228. Wall R.: "USAF Expands Infowar Arsenal", *Aviation Week and Space Technology*, Vol. 151, Issue 20, New York, November 15, 1999.
229. Walter G. S.: *Cyberspace and the use of force*, Ageis, 1999.
230. Weiss L.: *The Myth of the Powerless State*, Cornell University Press, Ithaca, NY, 1998.
231. Westby J.: *Međunarodni vodič za borbu protiv kompjuterskog kriminala*, Produktivnost AD, Beograd, 2004.
232. Williams P.: "Transnational Criminal Organizations and International Security", Arquilla J., Ronfeldt D. F.: *Cyberware is coming!, in: Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, 1997.
233. Zolberg R. A., Suhrke A., Aguayo C.: *Escape From Violence: Conflict and the Refugee Crisis in the Developing World,* Oxford University Press, New York, 1989.
234. Жомини: *Преглед ратне вештине,* Војно дело, Београд, 1952.
235. *Directive Number 3600.1*, Department of Defense, Rev. one, October 2001.
236. *Information Operations Primer*, U.S. Army War College, Dept. of Military Strategy, Planning, and Operations & Center for Strategic Leadership, 2007.

Интернет извори

1. *24th Air Force activated, 2 units realign in joint ceremony*, August 19, 2009, http://www.af.mil.usairforce
2. *2003 CSI/FBI Computer Crime and Security Survey*, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf
3. *2006 CSI/FBI Computer Crime and Security Survey*, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf
4. AbrašMEDIA, http://abrasmedia.info/društvo/nauka-i-tehnologija/cyber-napad-može-značiti-i-objavu-rata
5. Adams J.: "Virtual defense", *Foreign Affairs*, May 2007, http://www.foreignaffairs.com/articles/57037/james-adams/virtual-defense
6. *An Analysis of Issues and Options*, http://csrc.nist.gov
7. *Annual Report to Congres on Foreign Economic Collection and Industrial Espionage,* July 1995, http://www.fas.org/sgp/
8. *Annual Report On The Military Power Of The People's Republic Of China*, IWS – The Information Warfare Site, http://www.iwar.org.uk/iwar/resources/news/china-io-2003.htm
9. Antončić V.: *Napadi s uskraćivanjem usluge (DoS napadi)*, http://os2.zemris.fer.hr/ns/2007_Antoncic/index.html#G.SQL-ubacivanje
10. *Architectural principles of the Internet*, Network Working Group RFC-1958, 1996. http://www.ietf.org/rfc/rfc1958.txt
11. Arquilla J., Ronfeldt D. F.: *Cyberware is coming!* In Athena's Camp: *Preparing for Conflict in the Information Age*, Santa Monica 1997, http://www.rand.org
12. Bank D.: "Spear Phishing tests educate people about online scams", *The Wall Street Journal online*, 17. 8. 2005, http://online.wsj.com
13. Barabasi A.: *Strength is weakness on the Internet*, http://physicsworld.com/cws/article/news/2806
14. *BBC NEWS*, May 02, 2007, http://news.bbc.co.uk/go/pr/fr//2/hi/europe/6614273.stm
15. Berg C.: "High-Assurance Design: Architecting Secure and Reliable Enterprise Applications", *Methods of Computer System Attacks*, http://www.awprofessional.com
16. *Biznis & Finansije*, http://www.docstoc.com/docs/4052048/Biznis-and-Finansije-2
17. Blau J.: "The battle against cyberterror", *Network World*, http://www.networkworld.com
18. Boot M.: *Statement Before The House Armed Services Subcommittee on Terrorism, Unconventional Threats, and Capabilities*, CFR, 29 June 2006, http://www.cfr.org/publication/11027/statement_before_the_house_armed_services_subcommittee_on_terrorism_unconventional_threats_and_capabilities.html
19. „Британија против ´сајбер рата´", BBC Serbian, http://www.bbc.co.uk/serbian/news/2010/10/101018_britishsecurity.shtml
20. *BT Counterpane*, http://www.counterpane.com

21. *BT Counterpane*, 13. 12. 2005, http://www.counterpane.com
22. Burns M.: *Information Warfare: What and How?*, http://www-2.cs.cmu.edu/~burnsm/Info Warfare.html
23. Caffe Europa, www.caffeeuropa.it
24. *California Anti-SLAPP Project*, http://www.casp.net/47usc230.html
25. CERT, http://www.cert.org
26. *Channelregister*, 29. 11. 2005, http://www.channelregister.co.uk
27. "China accused of cyberattacks on New Zealand", *ZDNet Australia*, September 13, 2007, http://news.zdnet.com/
28. *China's Copyright Regulations*, http://www.wipo.int/export/sites/www/about-ip/en/ipworldwide/pdf/cn.pdf
29. Clark Prosecutor, http://www.clarkprosecutor.org/html/death/US/mcveigh717.htm
30. Craig L.: *The Kosovo Liberation Army: Does Clinton Policy Support Group with Terror, Drug Ties?*, US Senate Republican Committee Report, 31 March 1999, www.fas.org/irp/world/para/docs/fr033199.htm
31. *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, Communication from the Commission to the Council, The European Parliament, The Economic and Social Committee and Committee of the regions, http://europa.eu.int
32. *Criminal Law of the People's Republic of China,* http://cybercrimelaw.net/laws/countries/China.html
33. "Critical infrastructure protection: a brief overview", http://chnm.gmu.edu
34. *Communications Decency Act*, http://www.cpic.org/free.speech/CDA/cda.html
35. *Computer Fraud and Abuse Act*, http://www.usdoj.gov/criminal/cybercrime/1030_new.htrnl
36. Computer Information Network and Internet Security, Protection and Management Regulations, http://newmedia.cityu.edu.hk/kiberlaw/gp3/pdf/law_security.pdf
37. *Computer Software Copyrigh Act*, http://www.ladas.com/Patents/Computer/Copyright.USA.html
38. "Computer viruses now 20 years old", *BBC on line*, November 10, 2003, http://news.bbc.co.uk
39. Congressional Research Service, Report for Congress, 2003, http://www.fas.org
40. *Control systems cyber security awareness*, http://www.cert-us.gov
41. *Convention on Cybercrime*, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
42. *Council of Europe*, http://conventions.coe.int
43. *Critical Foundations: Protecting America's Infrastructures*, President's Commission on Critical Infrastructure Protection, 1997, http://www.fas.org/sgp/library/pccip.pdf
44. CrucialPoint, http://crucialpointllc.com/services/federal-services/government-markets/cybercom-org-chart
45. *CyberCrime & Doing Time*, http://garwarner.blogspot.com
46. *Cyber Security Research And Development Act*, House Of Representatives, 2002, http://www7.nationalacademies.org/ocga/laws/PL107_305.asp

47. *Cyber Security and Enhancement Act,* www.usdoj.gov/criminal/cybercrime/homeland_ CSEA.htm
48. *Cyber Threats and Information Security: Meeting the 21st Century Challenge*, A report for the CSIS Homeland Defense Project, Washington D.C.: Center for Strategic and International Studies, 2001, http://www.csis.org/component/option,com_csis_experts/task,view/id,154
49. *Cybersecurity for Critical Infrastructure Protection – Technology Assessment*, United States General Accounting Office, GAO-04-321, http://www.gao.gov
50. "Cybersecurity for Critical Infrastructure Protection – Technology assessment", http://www.gao.gov
51. Dacey F. R.: *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO, 2004, http://www.gao.gov
52. Datz T.: *Industrial Control Systems: Out of Control?*, http://ses.symantec.com
53. DARPA Strategic Plan (2007), http://www.darpa.mil/body/news/2007/2007StrategicPlan.pdf
54. *Declaration of principles building the Information Society: a global challenge in the new millennium*, 2003 World Summit on the Information Society, document WSIS- 03/GENEVA/DOC/4-E, http://www.itu.int
55. Denning D.: *Is Cyber Terror Next?*, http://www.ssrc.org/sept11/essays/denning.htm
56. Denning D.: *Cyberterrorism – Testimony before the Special Oversight Panel on Terrorism*, Committee on Armed Services, US House of Representatives, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
57. *Department of Justice,* http://www.usdoj.gov
58. Der Derian J.: "Speed pollution", *Wired*, http://www.wired.com
59. *Digital Millenium Copyright Act*, http://www.copyright.gov/legislation/dmca.pdf
60. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain aspects of Information Society services, in particular electronic commerce, in the Internal Market, http://europa.eu.int
61. Дракулић М., Дракулић Р.: *Cyber криминал*, 2005, http://www.bos.org.yu/cepit/drustvo/sk/cyberkriminal
62. Дурсун Б.: *Основи међународног хуманитарног права*, http://www.scribd.com/doc/47408474/osnovi-medjunarodnog-humanitarnog-prava
63. Eedle P.: "Al Qaeda takes fight for 'Hearts And Minds' to the web", *Jane's Intelligence Review*, 2002, http://www.freerepublic.com
64. Electronic Communications Privacy Act, http://www.legal.web.aol.com/resources/legislation/ ecpa.html
65. Electronic Communications Privacy Act of 1986, http://www.cpsr.org/issues/privacy/ecpa86
66. *EIectronic Digital Signature Law*, http:// www.byakernet.com/ecommerce/russia-t.htm
67. Electronic Privacy Information Center, http://www.epic.org
68. *Electronic Signatures in Global and National Commerce Act*, http://www.ftc.gov/os/2001/06/es-ignreport.pdf

69. Eriksson E. A.: “Information Warfare: Hype or Reality?”, *The Non-proliferation Review*, Spring-Summer 1999, http://cns.miis.edu
70. European Parliament, http://www.europarl.europa.eu
71. Filip A.: *Phishing*, http://www.inet.co.yu/textview.php?file=k-phishing.html
72. *FindLaw*, http://news.findlaw.com
73. Fischer E.: *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, CRS Report for Congress, http://csrc.nist.gov
74. Flach M.: *The Information Society - The Role of Networks and Information*, http://artilect.org/altman/moritz.pdf
75. *Foreign Relations Authorization Act*, http://www.state.gov
76. *Frankfurter Rundschau*, http://www.f-r.de/ressorts/nac...ik/thema_des_tages/?cnt=753624
77. *Fraud and Related Activity in Connection with Computers*, http://www.usdoj.gov\criminal\ cybercrime\1030NEW.lUm
78. GAO, http://www.gao.gov
79. *Georgia accuses Russia of waging cyberwar*, CBC News, August 12, 2008, http://www.cbc.ca/technology/story/2008/08/12/tech-georgia.html
80. *GFI white paper*, http://www.gfi.com/whitepapers/network-protection-against-trojans.pdf
81. *Globalspec*, http://communication-equipment.globalspec.com/LearnMore/Communications_Networking/Networking_Equipment/Distributed_Supervisory_Control_Systems_DCS_SCADA
82. Graham B.: *Bush Orders Guidelines for Cyber-Warfare – Rules for Attacking Enemy Computers Prepared as U.S. Weighs Iraq Options*, http://www.washingtonpost.com
83. Green H.: “We all knew better”, *BusinessWeek Online*, http://www.businessweek.com/magazine/toc/03_34/B38460333futuretech.htm
84. Griffiths T. R.: *The History of Internet*, Leiden University, Leiden, 2002, http://www.let.leidenuniv.nl/history/ivh/chap2.htm
85. “Guideline for Identifying an Information System as a National Security System”, National Institute of Standard and Technologies, http://csrc.nist.gov
86. *Guideline for Identifying an Information System as a National Security System*, National Institute of Standards and Technologies, http://csrc.nist.gov/publications/nistir/NISTIR7298_Glossary_Key_Infor_Security_Terms.pdf
87. Hawksley H.: “Big Brother is watching us all“, *BBC News*, September 15, 2007, http://news.bbc.co.uk/2/hi/programmes/from_our_own_ correspondent/6995061.stm
88. *History of viruses*, Pearson Education Inc., http://www.factmonster.com/pages/copyright.html
89. “How cyber crime went professional”, *The Independent*, August 13, 2008, http://www.independent.co.uk/news/business/analysis-and-features/how-cyber-crime-went-professional-892882.html

90. *How is Al Qaeda funded?*, Council on Foreign Relations, http://www.terrorismanswers.org
91. *How the Pentagon is Organizing its Cyber Warfare System*, May 2008, http://www.IntelligenceOnline.com
92. Hudson R.: *The sociology and psychology of terrorism: who becomes a terrorist and why?*, http://www.fas.org
93. *Information and Analysis: Kidnapping & Hostage Taking*, Northeast Intelligence Network – Terrorism News, http://www.homelandsecurityus.com
94. *Information Technology in the 21st Century Battlespace*, July 24, 2003, http://commdocs.house.gov/committees/security/has294260.000/has294260_0f.htm
95. *Information Assurance (IA) Glossary*, National CNSS Instruction n. 4009, Committee on National Security Systems, National Security Agency, 2003, http://www.nstissc.gov
96. *InfraGard,* http://www.infragard.net
97. Институт за стандардизацију Србије, http://www.iss.rs/news/news_33.html
98. International Association of Defense Counsel, http://www.iadclaw.org/books.cfm
99. *Internet Email Service Management Regulations,* www.cdt.org/international/censorship/20060220chinaspam.pdf
100. *lnternet lnformation Services Regulations,* www.usembassy-china.org.cn/sandt/netreg2000.html
101. *Internet Security Threat Report – Trends for January 05–June 05*, Symantec, http://www.symantec.com
102. *Internet Society*, http://www.isoc.org
103. Internet World Stats, http://www.internetworldstats.com/top20.htm
104. *Islamic Charity Indicted*, http://www.cbsnews.com
105. *ISO 27001*, ISMS requirements, http://www.iso27001/security.com/html/iso27002.html
106. *Историја XX века*, http://www.ceeol.com
107. ITU, http://www.itu.int
108. Joint Vision 2020, Director for Strategic Plans and Policy, J5: Strategy Division, US Government printing office, Washington DC, June 2000, www.dtic.mil/jv2020/jv2020.doc
109. Kaiser G.: *Dutch Botnet Bigger Than Expected*, 2005, http://informationweek.com
110. Karadjis M.: *Chossudosky's Frame-up of the KLA*, http://jinx.sistm.unsw.edu.au/~greenlft/1999/360/360p21/htm
111. Катиловић Д.: „Пецање наивних душа“, *Свет компјутера*, децембар 2004, http://www.sk.co.yu/2004/12/skin05.html
112. Kerstein P.: *How Can We Stop Phishing and Pharming Scams?*, http://www.csoonline.com
113. „Кинески хакери 'ушли' у Пентагон“, RTV B92, 4. 9. 2007, http://www.b92.net/indexs.phtml
114. „Кинези читали мејлове министра одбране САД“, дневни лист *Блиц*, 6. 9. 2007, http://www.blic.co.yu/

115. *Know your enemy: phishing – Behind the scenes of phishing attacks*, The Honeynet Project & Research Alliance, http://www.honeynet.org
116. *Know Your Enemy Whitepapers*, The Honeynet Alliance, http://www.honeynet.org/papers/kye.html
117. *Конвенција о кибер криминалу - Повеља потписа и ратификација*, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=18/06/04&CL=ENG
118. *Конвенција о кибер криминалу*, http://www.entel.rs/info/software/sajber%20kriminal-konvencija%20EZ.pdf
119. Krasavin S.: *What is Cyberterrorism?*, Computer Crime Research Center, http://www.crime-research.org
120. Law *and Internet: Legal aspects of SPAM in Russia*, http://www.russianlaw.net/english/ae06.htm
121. *Law of the Russian Federation on the Legal Protection of Computer Programs and Databases*, http://www.fips.ru/ruptoen2/law/pr_db.html
122. *Law on Information, Informatization and Protection of Information*, http://www.fas.org/irp/ world/russia/docs/lawjnfo.htm
123. Law *on Communications*, http://english.minsvyaz.ru/docs/FED.doc
124. Legal Aspects of Computer-related Crime in the Information Society – COMCRIME, http://europa.eu.int/ISPO/legal/en/crime/crime.html
125. Leyden J.: "UK card fraud hits £505m", *The Register*, 8. 3. 2005, http://www.theregister.co.uk
126. Leyden J.: *Cybercrime costs a bit more than physical crime*, http://www.channelregister.co.uk
127. Leyden J.: *The enemy within*, 21. 11. 2005, http://www.theregister.co.uk
128. *Making the Nation Safer: the Role of Science and Technology in Countering Terrorism*, The National Research Council, 2002, http://www.nap.edu
129. Manyon J.: *The Kosovo News and Propaganda War*, http://www.freemedia.at/KosovoB_Manyon.htm
130. Markoff J., Kramer A.: "U.S. and Russia Differ on a Treaty for Cyberspace", *The New York Times*, June 28, 2009, http://www.nytimes.com/2009/06/28/world/28cyber.html
131. Марковић А.: „Утисци са WSIS 2005", http://www.elitesecurity.org/t147318-Utisci-sa-WSIS-The-World-Summit-on-the-Information-Society-Tunis-to-November
132. Marsh R.: *Critical Foundations: Protecting America's Infrastructures*, The George C. Marshall Institute, http://cipp.gmu.edu/clib/43_TheMarshallInstitute-CriticalFoundationsProtecting.htm
133. *Maximizing Email Security ROI*, CipherTrust, http://www.ciphertrust.com/resourses/articles/articles/roi_2_virus
134. *Measures to eliminate international terrorism*, UN Document A/RES/49/60, http://www.un.org/documents/ga/res/49/a49r060.htm
135. Measures on Administrative Protection of lnternet Copyright, http://www.chinaitlaw.org/?pl=regulations&p2=051006180113

136. Mega S.: *La Cina vuol spiare il Pentagono*, www.analisidifesa.it
137. *National Security Presidential Directive 16 – To Develop Guidelines for Offensive Cyber-Warfare*, July 20, 2003, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/index.htm
138. NATO, http://www.nato.int/kosovo/pres/p990508b.htm
139. Nielsenwire, http://blog.nielsen.com/nielsenwire/category/media_entertainment/
140. *Okinawa charter on global information society*, http://lacnet.unicttaskforce.org
141. *Organised crime situation report 2004 – The threat of cybercrime*, Council of Europe, Strasburg, 6. 9. 2004, http://www.coe.int
142. *Patriot Act*, http://thomas.loc.gov/cgibin/bdquery/z7dl07:HR03162:TOM:/bss/dl07qu-cry.litnil
143. „Pentagon od Obame dobio smernice za cyber ratovanje“, *Personal magazin*, http://www.personalmag.rs/internet/pentagon-od-obame-dobio-smernice-za-cyber-ratovanje/
144. Peter, et al.: *The Kosovo News and Propaganda War*, International Press Institute, Vienna, 2000, http://www.freemedia.at/ KosovoB_Manyon.htm
145. *Plan of action*, 2003 World Summit on the Information Society, document WSIS-03/GENEVA/DOC/5-E, http://www.itu.int
146. *Prevention of Industrial Espionage*, University of Chicago, 2003, http://www.munuc.org
147. *Privacy Act*, www.usaid.gov/policy/ads/500/508.pdf
148. *Professional cyber arms dealers*, Defensetech, http://www.defensetech.org/archives/004142.html
149. *Project for the New American Century*, http://www.newamericancentury.org/
150. Pufeng W.: *The Challenge of Information Warfare*, http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm
151. *Qa'idat al-Jihad, Iraq, and Madrid – The First Tile in the Domino Effect?*, The International Policy Institute for Counter-Terrorism, http://www.ict.org.il/Articles/tabid/66/Articlsid/557/currentpage/15/Default.aspx
152. *Рачунарски речник Микро књиге*, http://www.mk.co.yu/pub/rmk/detalj1.php?EngOdrID=2304
153. *Regional Development Glossary*, http://www.emergence.nu/toolkit/glossary.php
154. *Regulations on Collective Management of Copyrights*, http://www.law-lib.com/law/ law vicw.asp?id=87904
155. *ReguIations on Safeguarding Computer Information System,* http://ftp.fas.org/irp/world/ china/clocs/computer_code.htm
156. Reimer J.: "U.S. Cyber Command Preparations Under Way, General Says", U.S. Department of Defense, March 16, 2010, http://www.defense.gov/news/newsarticle.aspx?id=58355
157. *Reporters Without Borders*, http://www.rsf.org
158. Richardson T.: "Brits fall prey to phishing", *The Register*, May 3, 2005, http://www.theregister.co.uk
159. Russia Profile, http://www.russiaprofile.org/

160. *Russia Says "Nyet" to Anti-Spam Law*, http://www.lockergnome.com/nexus/net/2005/02/03/ru-ssia-says-nyet-to-anti-spam-laws
161. *Russian Federation Federal Law on Participation in International Information Exchange*, http://www.privacyexchange.org/legal/nat/omni/nol.html
162. Russian law makers to fight spam, http://www.gateway2russia.com/st/art_244487.php
163. *SCADA aplikacija za vođenje procesa pneumo-transporta zeolita*, http://www.automatika.rs/baza-znanja/teorija-upravljanja/scada-aplikacija-za-vodjenje-procesa-pneumotransporta-zeolita.html
164. Schneier B.: "Airplane Hackers", *Crypto-Gram Newsletter*, November 15, 2003, http://www.schneier.com
165. Schneier B.: *Internet Worms and Critical Infrastructure*, 2003, http://www.schneier.com
166. Schneier B.: *Liability changes everything*, http://www.schneier.com
167. Schneier B.: *The Hackers are Coming!*, http://www.schneier.com
168. Schniztler H.: *A Never Ending Story in Cell 13*, http://www.freemedia.at/ KosovoB_Schnitzler.htm
169. Schogol J.: "Official: No Options 'off the table' for U.S. Response to Cyber Attacks", *Stars and Stripes*, May 8, 2009, http://www.stripes.com/news/official-no-options-off-the-table-for-u-s-response-to-cyber-attacks-1.91319
170. Servida A.: *Towards a Dependable Information Society: from DEPPY to FP6*, European Commission, http://groups.inf.ed.ac.uk/safecomp/Download/safecomp2002/servida_safe-comp2002.PDF
171. Servida A.: *Towards a Dependable Information Infrastructure for the EU*, European Commission, http://www.safety-club.org.uk/resources/128/AServida.pdf
172. *Сигурност рачунарских мрежа*, http://www.conwex.info/draganp/SRM_Predavanje_16.pdf
173. SITE Institute, http://www.siteinstitute.org
174. Spam Laws, http://www.spamlaws.com/federal/can-spam.shtml
175. *Statement of major general Rhett Hernandez*, USA Incoming Commanding General, U.S. Army Forces Cyber Command, September 23, 2010, http://democrats.armedservices.house.gov/index.cfm/files/serve?File_id=067ffc96-e5c1-4cef-baa2-010d16e3be57
176. *Stratfor*, June 15, 1999, http://www.stratfor.com/media/ television/990615.asp
177. Sullivan B.: *FBI software cracks encryption wall*, 2001, http://www.msnbc.com
178. *Supervisory Control and Data Acquisition (SCADA) Systems*, National Communications System, 2004, http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf
179. Squitieri T.: *Cyberspace full of targets*, http://www.usatoday.com
180. *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, GAO, 2004, http://www.gao.gov/new.items/d04321.pdf
181. *Telegraph*, May 19, 2007, http://www.telegraph.co.uk

182. *The Criminal Code of the Russian Federation,* http://www.russian-criminal-code.com
183. *The fifteen major spenders in 2007*, SIPRI, http://archives.sipri.org/contents/milap/milex/mex_trends.html
184. *The National Strategy to Secure Cyberspace*, The White House, 2003, http://www.whitehouse.gov
185. *The Report of the President's Commission on Critical Infrastructure Protection*, http://www.securityfocus.com
186. "The State of the Internet", Akamai, http://www.akamai.com/stateoftheinternet
187. *Telecommunications Regulations,* www.cnii.com.cn/20020808/ca91368.htm
188. *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, 2000, http://www.oun.org
189. *The challenge of information warfare*, http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm
190. *The economist*, May 10, 2007, http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598
191. *The Federal Bureau of Investigation and Internet Crime Complaint Center*, http://scamfraudalert.wordpress.com/2010/03/13/fbi-2009-cybercrime-statistics
192. *The Insider Threat to U.S. Government Information Systems*, National Security Telecommunications and Information Systems Security Committee, http://www.cnss.gov
193. *The UN Resolution on CIIP*, UK National Infrastructure Security Co-Ordination Centre, http://www.niscc.gov.uk
194. The White House, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm
195. Thomas T.: *Like Adding Wings to the Tiger: Chinese Information War Theory and Practice*, http://www.iwar.org.uk/iwar/resources/china/iw/chinaiw.htm
196. *Threat Encyclopedia*, http://www.eset.com/threat-center/pedia/p.htm
197. Tikk E., et. al.: *Cyber Attacks Against Georgia: Legal Lessons Identified*, Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia, November 2008, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf
198. *UK Terrorism act 2000*, http://www.opsi.gov.uk
199. *United States Institute of Peace*, http://www.usip.org/pubs/specialreports/sr116.html
200. United States House of Representatives, http://www.house.gov
201. *U.S. Fleet Cyber Command Mission*, Navy Forces Online Public Sites, http://www.fcc.navy.mil/
202. *U.S. Policy on Counterterrorism PDD-39*, http://www.fas.org/irp/offdocs/pdd39.htm
203. US-CERT, http://www.cert-us.gov
204. *US cyberspace strategy,* www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
205. Васмут Ц. У.: *Педагогија мира*, www.dadalos.org/frieden_bih/grundkurs_4/konflikt.htm

206. Vatis M. A.: *Cyber attacks during the war on terrorism: a predictive analysis*, Institute for Security Technology Studies at Dartmouth College, September 22, 2001, http://www.ists.dartmouth.edu
207. Verton D.: *A Definition of Cyber-terrorism*, http://www.computerworld.com
208. Verton D.: *Virtual threat, real terror: Cyberterrorism in the 21st Century*, http://judiciary.senate.gov
209. *Virtual Criminology Report: the first pan-European study into organised crime and the Internet*, http://www.mcafee.com
210. *Virus stats*, CSA/TruSecure, http://www.ICSAlabs.com
211. *Водич кроз избор правних и законодавних инструмената за управљање миграцијама на територији Европске уније*, Међународна организација за миграције (IOM), 2005, http://iom.ramdisk.net/iom/images/uploads/Vodic%20kroz%20izbor%20pravnih%20i%20zakonodavnih%20instrumenata%20za%20upravljanje%20migracijama%20na%20teritoriji%20Evr_1185965257.pdf
212. Вулетић Д.: *Кибер ратовање као облик информационог ратовања*, http://www.singipedia.com
213. Webopedia, http://www.webopedia.com
214. Weimann G.: *How Modern Terrorism Uses the Internet*, United States Institute of Peace, Special Report, New York, http://www.usip.org/pubs/specialreports/sr116.pdf
215. Weimann G.: *Terror Groups Exploit Internet for Communications, Recruiting, Training*, JINSA Policy Forum, http://www.jinsa.org
216. *Where is Raed?*, http//dear_raed.blogspot.com
217. Williams P.: "Transnational Criminal Organizations and International Security", http://www.rand.org
218. Wilson C.: *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service – The Library of Congress, http://fpc.state.gov
219. Wilson C.: *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report for Congress, 2005, http://fpc.state.gov
220. Winkler S. I: *Case Study of Industrial Espionage Trough Social Engineering*, National Computer Security Association, Pennsylvania, http://www.simovits.com/archive/socialeng.pdf

Биографија аутора

Ненад Путник је рођен 14.03.1977. године у Београду, где је завршио основну школу и гимназију. Дипломирао је на Филозофском факултету у Београду, група за филозофију, 2002. године. Исте године, на истом факултету, уписао је последипломске студије, смер естетика. Магистарске студије на Факултету цивилне одбране уписао је школске 2003/04. године. Априла 2008. године одбранио је магистарску тезу под насловом „Безбедносне претње у сајбер простору са посебним освртом на проблем сајбер тероризма“, чиме је стекао академско звање магистра Наука одбране, безбедности и заштите – смер људска безбедност.

Током 2003. године Ненад Путник је био запослен у Земунској гимназији, на радном месту професора филозофије и логике. Радни однос на Факултету безбедности засновао је фебруара 2004. године, у звању асистента-приправника за ужу научну област Студије безбедности, на наставном предмету Теорије конфликата. Од јула 2008. године до данас ангажован је у звању асистента, на основним академским студијама, на истом предмету. Осим тога, ангажован је као предавач на специјалистичким струковним студијама из области Безбедносног менаџмента.

Ненад Путник је учествовао у већем броју научно-истраживачких пројеката као и у раду међународних стручних и научних скупова у земљи и иностранству. Објавио је више стручних чланака из области информационе безбедности, људске безбедности и теорија конфликата. Аутор је монографије *Сајбер простор и безбедносни изазови* у издању Факултета безбедности, 2009. године.

Прилог 1.

Изјава о ауторству

Потписани-а мр Ненад Путник

број уписа 115

Изјављујем

да је докторска дисертација под насловом

„Кибер ратовање – нови облик савремених друштвених конфликата"

- резултат сопственог истраживачког рада,
- да предложена дисертација у целини ни у деловима није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио интелектуалну својину других лица.

Потпис докторанда

У Београду, 19.4.2012.

Прилог 2.

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора мр Ненад Путник

Број уписа 115

Студијски програм _____

Наслов рада „Кибер ратовање – нови облик савремених друштвених конфликата"

Ментор проф. др Радомир Милашиновић

Потписани мр Ненад Путник

изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла за објављивање на порталу **Дигиталног репозиторијума Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис докторанда

У Београду, 19.4.2012.

Прилог 3.

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

„Кибер ратовање - нови облик савремених друштвених конфликата“

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство

2. Ауторство - некомерцијално

3. Ауторство – некомерцијално – без прераде

4. Ауторство – некомерцијално – делити под истим условима

5. Ауторство – без прераде

6. Ауторство – делити под истим условима

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

Потпис докторанда

У Београду, 19.4.2012.