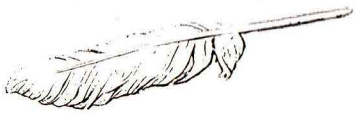


Информатички рат – фикција или стварност

УДК: 356.255.2:316.774:623.618

Др *Бошко Родић,* пуковник, и *Војислав Родић*

Аутор је, полазећи од тога да је информација један од најважнијих ресурса у рату, предложио начин за систематизацију и прецизније одређивање појмова везаних за деловање на људски мозак ради сламања воље за одбраном. Неокортикални рат је дефинисан као најшири облик рата срачунат на деловање на кортекс.

Посебна пажња је посвећена информационом рату, који обухвата, према аутору, прекид у преносу информација, њихово модификовање, пресретање и пласирање.

Аутор објашњава и суштину информатичког рата, указује на значај савладавања техника за његово вођење и наводи таксиономију напада на рачунарске системе, који, у ствари, детерминишу информатички рат.

Увод

Последњих година у нашој литератури се често појављују некритички, као синоними, термини *неокортикални (неокортички)*, *информациони* (раније *психолошки*), *инфо, кибер, дигитални, мрежни,* нежни,[1] па и *електронски,*[2] а посебно *информатички рат,* који углавном имају исто значење: деловање на људски мозак, посебно на кору великог мозга, ради сламања непријатељеве воље за одбраном (или нападом). Проблем се додатно компликује због утицаја англосаксонске терминологије, односно преплитања значења термина *рат* и *ратовање*[3] (war рат, и warfare – рат, али и вођење рата, *ратовање*).

[1] С. Петровић, *Компјутерски криминал,* „Безбедност" и „Полицајац", Београд, 2000.

[2] А. Разингар, *Електронска противдејства,* Војноиздавачки завод, Београд, 1971. и Група аутора, *Електронски рат – стање и перспективе – I фаза – принципи електронског рата* (студија), Електротехнички факултет Универзитета у Београду, Београд, 2000.

[3] М. Бенсон, *Енглеско-српскохрватски речник,* „Просвета", Београд, 1980.

Под термином *рат* подразумева се „комплексан, интензиван и масован сукоб... Основни садржај је оружана борба, али се Р. не своди само на њу, већ укључује и друге облике борбе (политичку, економску, психолошку, моралну) што га чини тоталним сукобом“,[4] а према истом извору је: „*Психолошки рат* – скуп организованих поступака које једна или више држава (обично потенцијални агресори) предузимају према становништву и ОС друге државе, како би се утицало на свест, мишљење, схватање, осећања и понашања људи у миру и рату“.

Према Шафранском, „*ратовање* је скуп свих борбених и неборбених активности које се предузимају да би се потчинила супротстављена воља противника или опонента. Ратовање, у овом смислу, није синоним за рат. Ратовање не захтева објаву рата нити захтева постојање услова који се у најширем смислу сматрају као 'стање рата'. Циљ ратовања није увек да се противник убије, већ да се потчини. Противник је потчињен када се понаша на начин који је коинцидентан начину на који – агресор или нападнута страна – жели да се он понаша“.[5] (Сагласно са *Војним лексиконом*[6] у раду се користи термин рат, а не ратовање, без обзира на његове аспекте).

Неокортикални рат

Назив и значење неокортикалног рата, према Шафранском,[7] потичу од речи *кортекс* (у општем значењу мозак) и *неокортекс* (мозак или церебрални систем код сапијенса). *У неокортикалном рату мозак је и субјекат и објекат деловања.* Неокортекс или капа мозга, или мозак неосисара, чини 80 одсто укупне мождане масе. Према *Војном лексикону*[8], у кори великог мозга, кортексу, налази се седиште свести, која је место приспећа или полазно место свесних нервних подстицаја, тј. осећајности и моторике. Неокортикални рат[9] – потчињавање противника без насиља – није само рат будућности – то је начин рата с највећим захтевима и најмаштовитијим и најефикаснијим моделима ангажовања. Наиме, неокортикални рат (ратовање) није детерминисан средствима[10] која могу да утичу на људски мозак (свест или подсвест): дроге (опијати – хемијска средства), електромагнетни таласи, звук и, коначно, информације перцепиране на било који начин. Према томе, неокортикални рат је најшири облик рата (ратовања) срачунат на деловање на кортекс.

---

[4] Група аутора, *Војни лексикон*, Војноиздавачки завод, Београд, 1981.
[5] Р. Шафрански, *Теорија информационог ратовања – припрема за 2020. годину*, „Military Review“, November, 1994.
[6] Група аутора, *Војни лексикон*, исто.
[7] R. Szafranski, *Neocortical warfare? The acme of skil*, „Military Review“, November, 1994.
[8] Група аутора, *Војни лексикон*, исто.
[9] R. Szafranski, *исто.*
[10] *Исто.*

У западним изворима изједначени су *информациони* и *неокортикални*[11] рат. Према Б. Шешићу, уколико је за „постојање информација нужан фактор свести односно знања које постоји само код свесних бића“,[12] деловање на подсвесно (дрогом, електромагнетним импулсом...) не може да се прихвати као информациони рат јер међу субјектима нема размене информација, односно један од релата (повезаних информацијом) требало би да буде свестан.[13] Међутим, теза о информационом рату може, ипак, да се прошири на релацију човек – „машина“, и то у два случаја: 1) када човек даје информацију машини – то је само одређени утицај (импат) на машину или узрок одређене функције,[14] и 2) машина даје одређене индикације, које човек схвата као знаке одређеног значења (звук ваздушних кочница код немачких бомбардера – „штука“, у Другом светском рату, бескрајно кружење бомбардера НАТО-а, нарочито ноћу, пре дејства пројектилима у рату 1999). У наведеним релацијама један од релата је свестан, па се може прихватити да је неокортикални рат исто што и информациони рат.

Информационо ратовање, према С. Петровићу[15] јесу: „Акције предузете да се оствари информациона супериорност нападањем противничких информација, процеса базираних на информацијама и информационих система, док се бране сопствене информације, процеси базирани на информацијама и информационим системима“. Такође, према једној студији,[16] информационо ратовање *(information warfare – IW)* чине активности које се предузимају ради утицаја на информације и информационе системе противника и ради заштите властитих информација и информационих система. У *IW* информације и информациони системи противника су циљеви на које се дејствује да би се утицало на процесе који зависе од информација *(information dependent process).*

---

[11] Ако се на Интернету тражи објашњење појма неокортички *(neocortical)* претраге се своде на – информациони *(information).*

[12] Б. Шешић, *Основи методологије друштвених наука*, „Народна књига“, Београд, 1988.

[13] Јасно је да ниједна машина неће „сама од себе“ упутити поруку у неокортикалном рату, нити ће се, на пример, дрога сама употребити на циљу. Према томе, ако циљ и није свестан „поруке“ (електромагнетски импулс, дрога итд.), свестан је онај који такву „поруку“ упућује.

[14] „Околности у којима саопштавам наредбу некој машини не разликују се битно од стања у коме наредбу саопштавам некој особи“ (Н. Винер, *Кибернетика и друштво – употреба људских бића*, „Нолит“, Београд, 1973).

[15] С. Петровић, *исто.*

[16] Група аутора, *Електронски рат – стање и перспективе – I фаза – принципи електронског рата* (студија), Електротехнички факултет Универзитета у Београду, Београд, 2000.

Према Националном универзитету за одбрану *(NDU – National Defence University* – највиша војно-политичка школа САД), „Информационо ратовање је приступ оружаном конфликту који се усмерава на руковођење (менаџмент)[17] и користи информације у свим облицима и на свим нивоима да би се остварила одлучујућа војна предност. . . мада је у крајњем случају војно по својој природи, води се и у политичкој, економској и друштвеној сфери... кроз примену најсавременије информационе технологије. . .“

Електронски рат, према А. Разингару,[18] јесте „. . . скуп техничких и оперативних мера, којима је циљ да, с једне стране, спрече противника да употреби електромагнетне таласе, смањи њихову ефикасност, ако су већ употребљени, или, чак, да се ти таласи користе против њега, а, с друге стране да се обезбеди властитим снагама слободно и ефикасно коришћење електромагнетских таласа упркос противничких дејстава (са битком за Британију родио се – електронски рат)“. Према једној студији,[19] електронски рат *(Electronic Warfare – EW)* скуп је војних дејстава чији је главни циљ контрола електромагнетног простора – домена. У релацији информациони рат – електронски рат, електронски рат се, према истој студији, сматра подскупом информационог рата.

Информационо ратовање је израз који су прихватили и Министарство одбране САД *(Department of Defense – DOD)* и Здружени генералштаб, а под њим се подразумевају акције којима се достиже информациона супериорност над противником. И према тој дефиницији се информационо ратовање (по)везује с информационим системима, рачунарским мрежама и слично. У прилог тим тезама је и следеће мишљење: „Онај ко води рат (информацијама) налази се у положају човека који има само две амбиције у животу. Једна је да измисли растварач који може да раствори сваку чврсту супстанцу, а друга да измисли универзални суд који може да прими сваку течност. Шта год овај изумитељ учинио, он ће бити осујећен“.[20] Коначно, према Конопатову и Јудину,[21] „незадрживи пораст научног и технолошког напретка, развој друштвене свијести и повећање улоге стваралачке способности човјека, довело је до тога да је у другој половини XX вијека на прво мјесто у развоју друштва дошао разум човјека, (и) управо су на човјекову свијест и усмјерили главни удар покретачи ’хладног рата’“.

Информација је према једној дефиницији:

---

[17] Шафрански сматра менаџмент најважнијим циљем у неокортикалном рату.

[18] А. Разингар, *исто.*

[19] Група аутора, *Електронски рат – стање и перспективе – I фаза – принципи електронског рата,* исто.

[20] Н. Винер, *исто.*

[21] С. Н. Конопатов, В. В. Јудин, *Устаљени појам рата је застарео,* „Информативни билтен превода“, бр. 1, ЦВНДИ, Београд, 2001.

„– опис једног својства које одређени ентитет посједује у одређеном моменту или временском периоду;

– информација је новост која повећава наше знање;

– информација подразумијева вјеројатност да се одређени систем налази у једном од могућих стања".[22]

Према М. Павлићу,[23] информација је протумачени податак. Она може да буде и обавештење, може да повећава знање, да смањује неизвесност, и слично. Према Шафранском[24], информација је „садржај или значење поруке". Информације се генеришу (и/или перцепирају) као визија (слика), звук, укус, мирис и све остало што прихватају људска чула. Иако, према М. Либицком,[25] информација није сама по себи медиј рата, ипак, *информациони је онај рат (оно ратовање) у којем је циљ свестан а средство за деловање на кортекс је информација без обзира на медиј пласирања информација* (новине, радио, телевизија, гласине итд.) Ради придобијања, односно сламања воље противника информације се могу мењати (модификовати), презентовати (лажно) и спречавати (ометати). Шематски, информациони рат, према В. Столингсу[26], може да се илуструје нападима на информације у преносу (шема 1).

Значај информације за рат може да се повећава. Крстарећа ракета не може да лети и погоди циљ ако нема податке (информације) о трајекторији и циљу, као ни пилот. Свака људска радња (у рату) која се предузима сагласна је, односно условљена неким информацијама. Монголи или Татари, иако бројно и материјално инфериорни, побеђивали су захваљујући, пре свега, брзом преносу информација.[27] Према томе, може се тврдити да је информација један од најважнијих ресурса[28] у рату.

Норберт Винер[29], у књизи *Кибернетика и друштво,* веома очигледно описује физиономију информационог рата. У светским пословима протекли период од неколико година[30] обележен је двема су-

[22] С. Ткалац, *Структура и организација података*, Свеучилиште у Загребу – Факултет организације и информатике, Вараждин, 1979.

[23] М. Павлић, *Систем анализа и моделирање података – пројектирање информацијских система*, „Научна књига", Београд, 1990.

[24] Р. Шафрански, *Теорија информационог ратовања – припрема за 2020. годину,* исто.

[25] M. Libicki, *What is information warfare, исто,* Институт за националне стратегијске студије САД, http: // www.infowar. com/, превод Б. Бајић, 1999.

[26] William Stallings, *Network and Internetwork Security Principles and Practice*, Prentice Hall, Englewood Cliffs, W, 1995.

[27] „Татарин" је некада у Србији био назив за скоротечу, гласника, улака и, на крају, за курира или поштоношу.

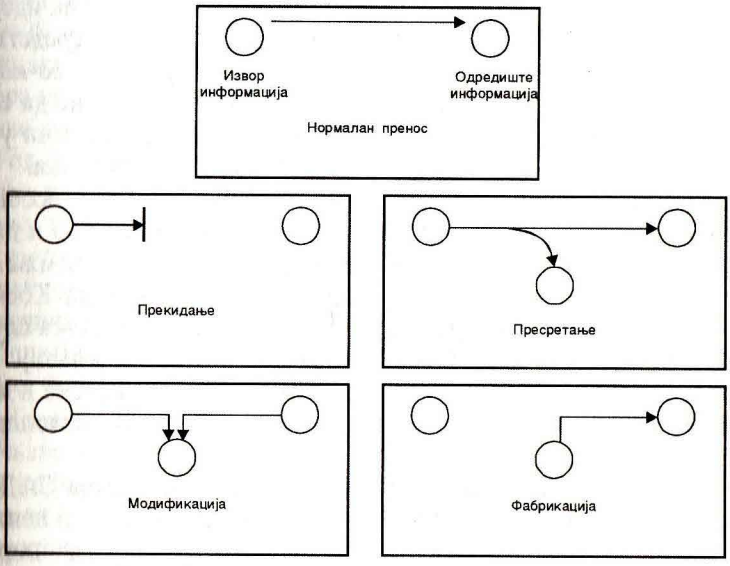
[28] Ресурс, фр. *resource* – помоћно средство; извор помоћи; извор (привреде) из којег се добављају сировине. . . (М. Вујаклија, *Лексикон страних речи*, „Просвета", Београд, 1980).

[29] Н. Винер, *исто.*

[30] Оригинални материјал потиче из 1954. године.

протним, чак противуречним тежњама. „С једне стране имамо мрежу комуникација, националних и интернационалних, која је потпунија него икада раније у историји, а с друге стране, под утицајем сенатора Макартија и његових следбеника, слепе и претеране класификације војних података и недавних напада на Стејт департман, ми залазимо у расположење тајности и подозривости коме у историји можемо наћи премац само у ренесансној Венецији". У вези с чувањем поверљивости, ометањем порука и блефирањем „... иде се за тим како би се сопственој страни омогућило да се снагама и средствима комуникација користи успешније од друге стране. У овој борбеној употреби информација исто је толико важно држати отворене сопствене канале колико и ометати другу страну у употреби канала којима располаже".[31]

Шема 1



Класификација информационих напада према Столингсу

„Ко се мача лаћа, он од мача гине", гласи пословица, а Норберт Винер је предвидео да „нема разлике између наоружавања самог себе и наоружавања својих непријатеља.[32] Стога свако застрашујуће откриће само појачава нашу потчињеност потреби за новим открићима". Нова оружја ће „... довести до тога да на овој планети ентропија расте све док разлике између врућег и хладног, доброг и рђавог, човека и материје не ишчезну у формирању белог усијања неке нове звезде".[33]

---

[31] Н. Винер, *исто.*

[32] Тај став је интересантан у вези с брзим овладавањем техникама информационог (информатичког) рата стране која их није створила.

[33] Према староегипатској легенди: „Када људи открију енергију која покреће звезде – тада ће нестати човечанства".

Према Ф. Џорџу[34], кибернетику као термин, зависно од интереса или гледишта, Норберт Винер, родоначелник тог појма, поједностављено тумачи као информатику *(information science)*, било као информациону технику *(information technology)*, било као теорију аутомата итд., што према Академији наука СССР-а коректно карактерише специфичност науке која се бави општим законима прихвата, чувања, дистрибуције и обраде информација – информатика, од француског information automatique – informatique – информатика[35] – аутоматизација информација. Ипак, Ф. Џорџ[36] појам кибернетике проширује и доводи у везу са математиком, логиком, аутоматима и коришћењем рачунских машина.

Технолошки[37] карактер информационог рата упућује на идеју да се говори и о *информатичком рату. То је рат у којем је средство за вођење рата информатичка технологија*[38]*: рачунар и његове компоненте, рачунарска мрежа,* и слично. Из те дефиниције може да се изведе појам *мрежни, хакерски, нежни, кибер рат* итд. Мада ни у том рату није, и не мора да буде, непосредни циљ воља противника.

Све владе имају и обучавају „кибер" војнике, који су способни да нападају и шпијунирају непријатеља преко компјутера, као и да покрећу удаљене нападе на виталне инфраструктуре неке земље. Немачки генерал Валтер Јерц, портпарол снага НАТО-а на Космету, новембра 2000, на симпозијуму који је организовала немачка служба БНД изјавио је да је интервенција НАТО-а против Југославије била први сукоб који је вођен и преко Интернета, и да су размена и манипулација подацима и информацијама били инструмент психолошког рата.

Пуковник Р. Шафрански[39], из Ратног ваздухопловства САД, повезујући неокортикални и информатички рат наглашава да ненаоружани елементи снага националне безбедности САД треба да шире демократске вредности и начин понашања унутар локалних култура; развијају мреже, тржиште и партнерство; уче основним вештинама и продиру у перцепције земаља циљева. Ненаоружани елементи треба да буду организовани као вишефункционални или унакрсно функционални, или као мреже. Важно да се има најмоћнији апарат за прикупљање обавештења (информација) и за ширење информација. Тај

[34] Ф. Џорџ, *Основы кибернетики,* Радио и связь, Москва, 1984.

[35] Тај термин на нашем простору увео је професор Стјепан Хан, а у СССР-у га је „озаконио", седамдесетих година, А. П. Ершов, дописни члан Академије наука Совјетског Савеза.

[36] Ф. Џорџ, *исто.*

[37] Технологија, у том случају, јесте примена информатичке технике.

[38] Примена рачунара – рачунарских мрежа.

[39] *Исто.*

апарат треба да чини добро интегрисана обавештајна и информациона агенција или мрежа агенција. Она треба да комбинује најбоље могућности и аналитичаре Централне обавештајне агенције *(CIA)*, Управе за националну безбедност *(NSA)* и Обавештајне агенције Министарства одбране САД *(DIA)* на нивоу испод више координационе групе. „Нова мрежа" (Си-Ен-Ен или можда Интернет), треба да ради у сарадњи са службама у иностранству, приватним сектором на терену и размештеним центрима за обуку и образовање. Мора се схватити да се може контролисати само оно што може да се види, чује или разуме, закључује пуковник Шафрански.

Пласирање информација (истинитих и из одређених разлога изабраних, полуистинитих или лажних) помоћу медија није никаква новост. Интернет у томе има неупоредиве предности. Процена броја корисника (око 100.000.000 1998. године, а очекивало се да ће тај број, веома брзо, до краја 20. века, бити више него удвостручен) којима се без икакве контроле (цензуре) могу пласирати информације по жељи аутора потврђује предности Интернета. Такође, Интернет има неупоредиве предности за обавештајни рад. Пре свега, у достави информација од обавештајаца, под условом да имају одговарајућу рачунарску опрему и телефонску линију. То су свакако предности, али само у повећању количине информација, у односу на остале традиционалне методе пласирања и прикупљања информација. Оно у чему је Интернет неупоредив јесте прикупљање информација директно са рачунара корисника прикључених на Интернет (приватна писма, научни радови, белетристика итд., целокупна култура једног народа или нације, сви могући подаци, сервирају се као на длану).

Доскора се могло само претпостављати да се Интернет злоупотребљава у војне сврхе. Међутим, с обзиром на злонамерно[40] угрожавање информационог система – рачунарске мреже, у последње време може да се говори и о информатичком рату. Рачунарска мрежа у информатичком (информационом) рату јавља се као мета, али и као средство. Неки аутори[41] користе израз информатички рат скоро искључиво за нападе на рачунарске мреже. За разлику од физичке борбе, то су напади на особине одређеног система, јер се нападају познати недостаци у безбедносној структури система. У том смислу, систем је саучесник у својој сопственој деградацији.

Годину дана после завршетка „Пустињске олује" у америчкој публикацији *US news and world report* објављен је чланак у којем је наведено да су амерички шпијуни успели да убаце нов рачунарски чип у француски штампач који су Ирачани својевремено поручили од Француза за потребе ваздушне одбране Багдада. Чип је у електрон-

[40] Поред злонамерног угрожавања постоји и случајно угрожавање.

[41] M. Libicky, *What is information warfare,* Институт за националне стратегијске студије САД, http://www.infowar.com/, 1999. година.

ском струјном колу имао вирус намењен за онеспособљавање главног рачунарског центра при Врховној команди ирачке војске. Чип са опасним вирусом произвели су стручњаци из америчке националне агенције за безбедност у Форт Миду (Мериленд). Иако немају поуздане доказе, стручњаци те агенције верују да је вирус деловао тачно онако како је био програмиран. Уз то, додају да је Пентагон пре више година почео да финансира истраживачке радове везане за употребу рачунарских вируса за војне потребе. Истовремено, у Пентагону се јавила група стручњака за рачунаре која је критиковала идеју о коришћењу рачунарских вируса у војне сврхе и захтевала забрану даљих радова у његовим лабораторијама. Касније је објављено да та критика није утицала на наведену оријентацију Пентагона.

Чињеница је да су информације и информатичке технологије све важније за националну безбедност уопште, посебно у рату.[42] Сагласно томе, савремени конфликти ће се све више испољавати као борба преко информационих система. Сви облици борбе за управљање и доминацију над информацијама, у суштини, сматрају се једном борбом и технике информатичког рата посматрају се с аспекта једне дисциплине. Они који савладају технике информатичког рата биће у предности над својим противницима.

Информатички (у оригиналу: информационо ратовање) рат је последњих година реалност. Постоји неколико различитих облика информатичког рата[43]: 1) рат у сфери командовања и управљања (које је намењено за ударе против „главе и врата" противника); 2) обавештајни рат (који се састоји од пројектовања, заштите и спречавања система усмерених на сазнање довољно за доминацију над бојиштем); 3) електронски рат (радио-електронске и криптографске технике); 4) психолошки (неокортикални) рат (у којем се информација користи за промену људске свести); 5) „хакерски"[44] рат (у којем се нападају рачу-

[42] *Исто.*

[43] *Исто.*

[44] Хакер је рачунарски ентузијаста који детаљно познаје рачунарски систем и упада у њега ради игре и забаве. Међутим, хакери се више не сматрају доброћудним истраживачима, већ су то најчешће злуради наметљивци. У односу на нелегалност, нелегитимитет, насилништво и штете које изазивају може се тврдити да је мала разлика између хакера (који генерише вирусе) и терористе. „Изворни" хакери, да би се дистанцирали, „хулиганима електронског доба" којима хакирање омогућава испољавање сопствених фрустрација и агресивности дали су назив који боље одсликава њихове малициозне намере – кракери (cracker). На пример, у пролеће 1990, три хакера из Аустралије оптужена су у Мелбурну за оштећење података у рачунарима Владе Сједињених Држава. Према изјавама полиције (како је писао „Њујорк Тајмс"), наметљивци су – користећи шифрована имена „Феникс", „Електрон" и „Нон" – продрли у рачунаре институција као што су *Los Alamos National Laboratory, Digital Equipment Corporation, Lawrence Livermore National Laboratory, Bellcore* (телефонски истраживачки институт), Харвардски универзитет, Њујоршки универзитет и Универзитет Тексаса, а то су учинили из – Мелбурна.

нарски системи); 6) економско-информациони рат (блокирање или усмеравање информација да би се обезбедила економска доминација), и 7) „кибер" рат (скуп футуристичких сценарија). Из наведене класификације не може се уочити директна веза неокортикални – информациони – информатички (рат), што је и разумљиво јер у информатичком рату није (увек) непосредни циљ (мада јесте крајњи) људска воља. Због најчешћег начина (софистицираности) напада на мреже они се спроводе, углавном, као хакерски напади,[45] отуда – хакерски рат, који има више варијаната. Нападачи могу да буду унутар самог система, мада је распрострањено мишљење да се могу налазити било где. Разлози за напад могу да буду: потпуна парализа или честа искључења („пад мреже"), случајне и намерне промене у базама података, крађе информација, крађе разних услуга, надгледање рада система (и скупљање обавештајних података), убацивање лажног саобраћаја између рачунара у мрежи, приступ подацима ради уцене итд.[46] Популарна средства за напад су вируси, а хакерски рат се може даље поделити на дефанзивне и офанзивне операције. Према неким тврђењима, најбоља одбрана од хакерског напада јесте сам хакерски напад. Мноштво хакерских напада може имати исти ефекат као и терористички напади[47] (иритирање, узнемиреност, неспокојство итд.) и заиста могу утицати на животе много људи.

Рачунарске мреже могу да буду нападнуте у физичком, синтаксном и семантичком домену.[48] Забринутост за нападе на физичком нивоу је релативно мала (мада велики рачунари, на пример у *Wall Street*-у, могу да се нападну преко малих рачунара који управљају системом хлађења читавог система), а семантички напади су напади којима се утиче на значење нечега што је од некога рачунар примио.

Први упади у туђе системе сежу у далеке шездесете године, када се хакери нису ни звали тим именом. У то време термин „рачунар" најчешће се поистовећивао с подрумом неког факултета пуним цеви и каблова, с посебним климатским условима. Програмери који су радили на тим диносаурусима имали су веома ограничен приступ, па су често користили разне трикове да би што ефикасније завршили свој посао. Те рутине биле су познате под именом *hacks* – сецкање, одакле и потиче садашњи термин хакер.

[45] M. Libicky, *исто.*

[46] Области о којима се мање јавно пише, али које имају изузетну важност: контрола ваздушног саобраћаја, индустријски процеси, систем за управљање семафорима, систем за управљање електроенергетским системом, телефонски систем, системи нуклеарних централа којима се управља помоћу рачунара итд. лако се могу саботирати тако да се изазову тешке хаварије.

[47] После напада на Светски трговински центар у Њујорку, 11. септембра 2001, потенцирано је питање бреше у рачунарским мрежама великих (специјалних) система: електроенергетског система, водоводног система, система ваздухопловног и железничког саобраћаја, војске, осигуравајућих компанија, федералне полиције итд. Након напада институције као што су ФБИ, ЦИА, па и Пентагон, убрзано су се искључивали с Интернета.

[48] M. Libicky, *исто.*

Можда је најозбиљнији аспект хакерског рата стварање густог облака магије око хакерисања и, на тај начин, успоставе стања професионалне параноје.[49]

Да би проверила отпорност својих рачунарских мрежа[50] на напад хакера *DISA (Defence Information Systems Agency)* – Агенција за одбрану информационих система, формирала је 1994. године свој тим хакера и наредила им да преко Интернета нападну мреже Пентагона. Хакери су продрли и преузели контролу над 88 одсто од 8.900 рачунара које су напали и само је четири одсто продора евидентирано и пријављено. Резултати теста су комбиновани са подацима о 350 продора неидентификованих хакера и закључено је да је било више од 300.000 упада у рачунаре Министарства одбране САД у току 1994. године. Званични став *DISA* јесте да нису припремљени да се одбране од електронске верзије Перл Харбура и да њихова електронска структура није безбедна. Таксиономија напада на рачунарске системе, према Ховарду[51], која би требало да детерминише и информатички рат приказана је на шеми 2. Подразумева се да непосредни циљ у рату нису изазов или статус, као што би у рату требало да постоје само организовани нападачи, али нису искључени ни остали.

Примери информатичког рата из периода агресије на Савезну Републику Југославију

Период агресије НАТО-а обележен је, поред бомбардовања циљева, и снажним информационо-пропагандним дејствима.[52] Рачунар-

[49] У САД кружиле су гласине да су у нека популарна рачунарска интегрална кола (чипови) или оперативне системе намерно уграђени недостаци који ће онемогућити светске микрорачунарске системе баш када САД буду суочене са војним изазовима својих противника.

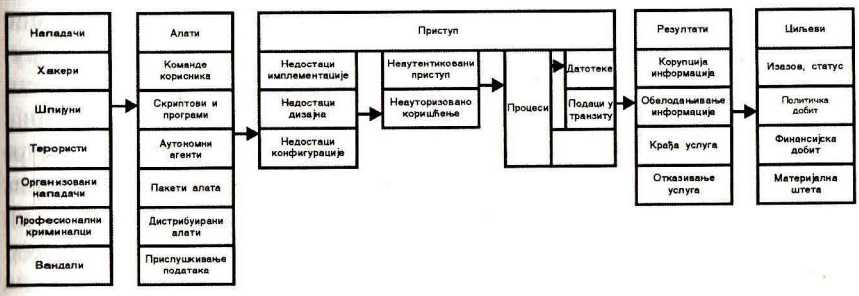
[50] P. E. Sakkas, *Espionage and Sabotage in the Computer World,* „Interantional Journal of Intelligence and Counterintelligence", 5, 1991.

[51] J. D. Howard, *An Analysis of Security Incidents on the Internet 1989–1995,* Thesis submitted in partial fulfilment of the requirements for the degree of doctor of philosophy, Carnegie Mellon University – Carnegie Institute of Technology, 1997.

[52] Извор – фирма И*НЕТ из Београда. Неколико података о активности те мале фирме довољно је илустративно и поучно у вези с вођењем информатичког рата. Фирма је приватно власништво (није била цензурисана), па су отуда постојали и нешто веће поверење и цитираност од стране корисника Интернета у свету. Вести су биле изузетно кратке, више пута проверене, на српском и на енглеском језику, са фотографијама као илустрацијама. Према И*НЕТ-у били су непосредни линкови *YAHOO NEWS*-а, *BBC*-а, *CNN*-а, итд. Фирму је више пута, па и током 2001. године, цитирао Stratfor, а дата су непосредно три интервјуа америчким радио-станицама у трајању од око 45 минута. Током ратних дана фирма је била у првих 5.000 по броју посетилаца на Интернету. Активни су били „мирор" сервери на Исланду, у Аустрији, Русији, Аустралији и Америци – практично је било немогуће блокирати

ски системи – рачунарске мреже, пре свега специјалних институција[53] у СР Југославији (приватне мреже ВЈ, МУП-а Србије, Савезног завода за статистику итд.), физички су одвојене од јавних и других приватних рачунарских мрежа, а степен аутоматизације је на релативно ниском нивоу. То је утицало на низак степен напада на рачунарске системе, изузимајући директни погодак вођеним пројектилом у рачунарски систем МУП-а Републике Србије.

Шема 2



Комбинована таксиономија напада на рачунарске системе

Активности на Интернету су отпочеле много пре избијања оружаног сукоба као пропагандна припрема. Анализа тадашњих активности на Интернету показала је пораст различитих *WEB* сајтова, који су формално били у продукцији албанских субјеката (информациони сајтови, политичке организације, неформалне групе). Садржај тих сајтова се заснивао на непровереним и непроверљивим, али веома „уверљивим" примерима, који су служили као „доказ" за агресивну политику српских власти на Космету. Свакодневно су објављиване потресне приче о страдањима група и појединаца, са детаљним подацима о времену, месту и особама које су трпеле репресију. Нагласак је увек био на судбинама појединаца ради лакшег везивања посетиоца *WEB* сајта. За све те сајтове карактеристичан је био висок ниво продукције (обиље ажурно приказиваног материјала упућује на високе трошкове прављења таквих сајтова), али и шематизованост, која је

њен рад. У фирми је било непосредно ангажовано 15 људи, а поред њих је био активан и тзв. виртуелни тим од небројено много сарадника са Новог Зеланда, из Аустралије, Немачке, Њујорка... Непосредно је волонтерски сарађивало више сарадника у СРЈ који су достављали своје прилоге из разних области, све у вези с одбраном. У томе су били најактивнији и најбројнији радио-аматери. Процењено је да је у једном тренутку прилог дописника из Косова Поља читало око 250.000 корисника Интернета – прилоге је преузимао и „Коријере дела Сера" итд. Значајно је да у креирању вести није био ангажован ниједан новинар, већ искључиво инжењери – информатичари.

[53] Организациони системи посебно значајни за државу, високо захтевни у односу на поузданост функционисања и критични с безбедносног аспекта.

упућивала на координацију свих активности из једног центра. Одговора од СРЈ скоро да није било, осим службених саопштења преко државних сајтова и информација на сајтовима медијских кућа. Једини вредан подухват из тог периода јесте *e-mail* листа „*Nobombs*", преко којег су размењиване и координисане активности у земљи и дијаспори ради парирања активностима противничке стране (која је уживала потпуну подршку најважнијих западних медија).

После отпочињања оружаног дела агресије активности на Интернету развијале су се муњевитом брзином, много брже него активности на бојном пољу. У веома кратком временском периоду са наше стране се појавило мноштво *WEB* сајтова који су, нарочито после рушења већег дела телекомуникационе инфраструктуре у земљи и укидања сателитског линка за РТС, постали носећи канал информисања стране јавности о дешавањима у земљи. Ти сајтови су пружали ажурне информације (inet.co.yu, Beograd.com – 24 сата вести дневно) и критичку анализу пропагандних активности, и чињени су покушаји, на разне начине, да се дезинформације усмере на уношење забуне код агресора.

Креативност коју су показивали сви они који су били ангажовани на Интернету умногоме је надмашила противничку страну, која је имала неупоредиво веће ресурсе. Неформални тимови су се показали најмање подједнако успешни (ако не и успешнији) од агресорових организација. Међутим, ту изузетно ефикасну активност у току агресије нису озбиљније подржали држава и њени органи, па су скоро сви ти сајтови престали са радом убрзо по окончању оружаног дела агресије.

Најједноставнији начин да се парира пропагандним дејствима агресора било је објављивање истине на начин који је примерен особинама медија. Кратке, проверене информације, по могућству са фото, видео и звучним записима, без додатних коментара о догађајима и њиховим учесницима показале су се као најбољи контраефекат агресоровој пропаганди, која је, како је агресија одмицала а број циљева повећаван, све чешће била у ситуацији да одговара на непријатна питања и да се заплиће у сопствене дезинформације. Добар пример за то је напад на воз на мосту у Грделичкој клисури који се догодио 12. априла 1999. око 13 сати. Захваљујући репортеру локалне телевизије, комплетан извештај са фотографијама објављен је на сајту inet.co.yu око 16 сати истога дана. Представници НАТО-а за штампу прво су порицали тај догађај, а потом су покушавали да га минимализују и релативизују, да би се тек више месеци после рата открило и да су покушали да убрзавањем видео-снимка начињеног из авиона који је нападао воз објасне ту „колатералну штету". У том случају ажурном и тачном информацијом онемогућени су сви покушаји да се догађај накнадно тумачи и фалсификује.

Један од главних ефеката свеукупних активности на Интернету огледа се у успешном супротстављању активностима псеудоеволуције које је спроводио агресор[54] (псеудоеволуција као средство психолошког рата јесте планирано и намерно мењање слике о појединцу или групи људи, односно нацији, у свести одабране популације тако да се тај субјекат посматра као не-људско биће, страна особа или раса, односно као биће које не заслужује људску правду, љубазност и обзир). Наиме, у свим агресоровим медијима српска страна је приказивана искључиво, у „тоталу". Управо обрнуто од начина на који је приказивана албанска страна (увек са потресним причама о појединцима и њиховим породицама). Кроз *e-mail* преписку (тешко је проценити колико милиона *e-mail* порука је размењено тих месеци) корисницима Интернета из земаља агресора приближили су се корисници са српске стране и од индивидуално недефинисане (али свакако агресивне и злочиначке) противничке стране претварали су се у особе – појединце, који исто тако као и они седе за компјутером и користе Интернет, говоре енглески и живе са својим породицама на начин који је на цивилизацијски истом или веома сличном нивоу. Неосетно, али веома ефикасно, непријатељ се из безличне, „дехуманизоване" масе издвајао као појединац са свим људским карактеристикама. Веома је занимљив случај који је описао Рос Тејлор у „Гардијану" од 22. априла 1999. године. Наиме, корисник Интернета из Америке који је у тренутку објављивања тог чланка, тридесет дана по отпочињању агресије, још увек подржавао агресију, изјавио је: „Када је рат почео писао сам неким људима у Србији поруке пуне мржње. Тада се десило нешто занимљиво: почео сам да се бринем за те људе и њихове породице како се бомбардовање настављало. Упознао сам те људе и непријатељ је добио лице. Више не мрзим српски народ". Тако је на најбољи начин објашњен кључни ефекат *e-mail* комуникације „преко лини-

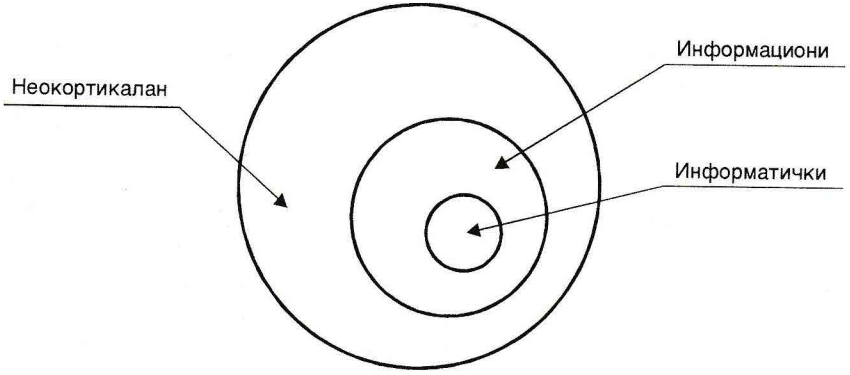
[54] Током ратних дана 1999. године вођен је у СРЈ и информатички рат, који се још увек води. Према сводочењу једног учесника информатичког рата у СРЈ, у тај рат је било укључено око 2.000 лица, организованих у (условно) три групе: прву групу су чинила лица која су ангажовале Влада Србије и Савезна влада, Савезно министарство за спољне послове, министарства информација, Савезно министарство за науку, развој и животну средину – Савезни завод за информатику, Радио-телевизија Србије и ТАНЈУГ; другу групу чинила су лица са универзитета и трећу групу – лица из разних удружења („Српски анђели"), па чак и из приватних фирми. Карактеристичан начин „борбе" био је следећи: на један од наведених сајтова стизала је порука из иностранства, обично од неког „србомрсца": „Ви Срби сте ... треба вас све побити". Одговарано му је: „Поштовани господине, хвала што сте се јавили, шаљемо вам фотографију срушеног Клиничког центра". Србомрзац: „Нека, заслужили сте". Сајт: „Ево вам и слика спрженог воза са путницима у Грделици..." Најчешће се таква кореспонденција завршавала тако што је србомрзац постајао сарадник, закључујући да су га „његови" лагали! Ако је србомрзац био упоран, сајт је био присиљен да употреби (у рату је све дозвољено) и методе као што је спам, и слично.

је фронта". Циљ агресора је управо било потпуно дехуманизовање противничке стране да би се домаће јавно мњење одвратило од протеста због масовних цивилних разарања. Већ сама могућност личног контакта била је највећа препрека таквим покушајима. У вези с тим, пуковник у пензији и експерт за информациони рат Кенет Алард, аналитичар агресора, закључио је следеће: „Покушаји НАТО-а да индоктринира противника дали су најлошији резултат који сам икад видео".

Закључак

Информатички рат *јесте фикција* за неупућене. Јесте фикција и у својој виртуелности – невидљивости. Међутим, *информатички рат је стваран.* Карактеришу га: снаге, средства, методе, циљеви и резултати. На шеми 3 приказан је однос неокортикалног (НР) информационог (ИФР) и информатичког рата (ИТР).

Шема 3



Однос неокортикалног, информационог и информатичког рата

Или: ИТР ⊂ ИФР ⊂ НР.

Према томе, у односу на циљ – кортекс, неокортикални рат се спроводи материјалним и нематеријалним средствима, па и информацијама; информациони рат се спроводи путем новина, електронских медија, гласинама и путем информатичке технологије, а кад се информациони рат реализује информатичком технологијом онда је то информатички рат. У вези с претераним залихама оружја „које брзо могу да укалупе војну политику у погрешном смислу", Винер сматра: „Много је веће преимућство имати слободу избора управо оног оружја које ће имати моћи да се најуспешније супротстави неком новом ванредном стању".[55]

[55] Н. Винер, *исто.*