НЕКОНВЕНЦИОНАЛНО РАТОВАЊЕ

ДИГИТАЛНО БОЈНО ПОЉЕ

Војна употреба нових информационих технологија и Интернета је у великој експанзији. Питање које постављају војни и цивилни стручњаци многих развијених земаља, а све ради тражења одговора, изналажења решења и нових терминологија у плановима, доктринама и развоју система одбране, јесте да ли напад на рачунарске мреже, системе и стратегијски софтвер представља криминални, терористички или акт војне агресије.

У модерном друштву електронски руковођене информације дотичу се скоро сваког аспекта свакодневног живота, што повећава важност обезбеђења информација од недобронамерних појединаца, група, индустријске шпијунаже, непријатељских нација, организованог криминала и терористичких организација. Генерално, како информационе технологије постају напредније, брже, доступније, јефтиније и лакше за употребу, тако их је све теже контролисати. Високотехнолошки напади и криминал представљају веома сложену област, са научном, техничком, политичком, социјалном, пословном и економском димензијом.

Сагледавајући све то, војне структуре посебно треба да повећају ефикасност и брзину у борби против напада савременим технологијама, а државни је интерес да штити дигиталне информације од сајбер напада и злоупотребе посебно оних које се тичу националне безбедности. Безбедност података у рачунарима и на мрежи, односно безбедност рачунарских система и мрежа је способност да се они заштите, а односи се на интегритет меморисаних података, системе обраде и преноса података. Она, такође, укључује поузданост хардвера и софтвера, заштиту против крађе рачунарске опреме и одупирање компјутерских система инфилтрацији, односно упадима неовлашћених корисника као нпр. хакера.

Високе технологије су данас обележје војне снаге и доминације неке државе уопште, али то носи са собом и рањивост и могућност за нове врсте и начине претњи и напада. Зато се војни експерти у многим државама баве питањима безбедности, стратегије и новим облицима конфликата и напада у информационом добу, односно тактици и технологијама дигиталног ратовања.

Предности у информационим и комуникационим технологијама су убрзале развој сложених националних и међудржавних мрежа, које омогућавају хиљадама корисника да дистрибуирају, преносе, приме и размене све врсте података. Важност информационих и комуникационих система за целокупно друштво и глобалну економију се интензивира са повећањем вредности и квантитета података који се преносе и прикупљају овим системима. У исто време ови системи и подаци су све више рањиви на различите претње као што су неовлашћен приступ и коришћење, уништавање, проневера и промена података. Умножавањем рачунара, повећањем рачунарске снаге, интерне повезаности, децентрализације, раста рачунарских мрежа и броја корисника, односно повећањем броја људи са овлашћеним приступом критичној инфраструктури и пословним подацима, те притицањем информационих и комуникационих технологија, повећава се и вероватноћа напада, било преко техничких средстава, експлоатацијом грешака или корупцијом. Може се приметити да како Интернет, информациони и сви остали комуникациони системи све више постају део свакодневног живота, тако државне односно владине службе, државна безбедност, војска, полицијске службе и приватност појединаца постају опасно испреплетени. Наравно, како се појачава и шири коришћење ових система повећава се и могућност напада из било ког дела света.

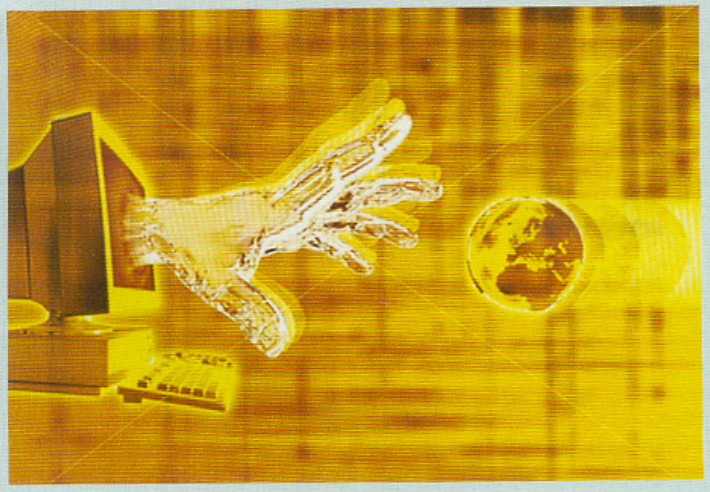
НАДГЛЕДАЊЕ ЛИЧНИХ ПОДАТАКА

Последњих година појавила се нова форма присмотре, надгледања и прикупљања података, а то су фајлови са личним подацима или дигитална особа – преглед података односно њихово надгледање путем рачунарских мрежа и комуникационих система. Доба рачунара донело је у извиђање нову еру у којој су информације о скоро свима доступне свакоме.

Надгледање података у информационим мрежама и системима је систематична употреба личних података у истраживању или контролисању деловања или комуникација једне или више особа. Таква врста надгледања је знатно мање скупа него физичка и електронска присмотра, зато што се може аутоматизовати, а са развојем информационих технологија све је јефтиније. Постоје две врсте оваквог надгледања: присмотра једне особе – персонал дататвеиллонце, где се надгледа одређена особа која је претходно идентификована као интересантна, и масовно надгледање – масс дататвеиллонце, где се осматра група или већа популација људи, да би се детектовали појединци од интереса.

КАТЕГОРИЈЕ КРИМИНАЛНИХ ЕЛЕМЕНАТА

КАТЕГОРИЈА	УПОТРЕБА ИНФОРМАЦИОНИХ СИСТЕМА	ЗЛОУПОТРЕБА ИНФ. СИСТЕМА	АГРЕСИВНА УПОТРЕБА ИНФ. СИСТЕМА
Нижи ниво	Комуникације	Илегалан упад, крађа телекомуникационих средстава	Освета, вандализам
Преваре	Комуникације и књиговодство	Крађа, контрола криминалистичких служби	Изнуда
Организовани криминал	Комуникације и књиговодство	Крађа, контрола криминалистичких служби	Изнуда
Екстремистичке групе: политичке, верске и др.	Штампа, комуникације, пропаганда	Крађа	Саботажа, прекидање рада, информациони рат
Индустријска шпијунажа	Бизнис	Крађа	Саботажа
Међународна шпијунажа	Прикупљање и анализа података	Шпијунажа	Информациони рат
Тероризам	Комуникације	Крађа, циљне мете, прикупљање обавештајних података	Информациони рат, саботажа

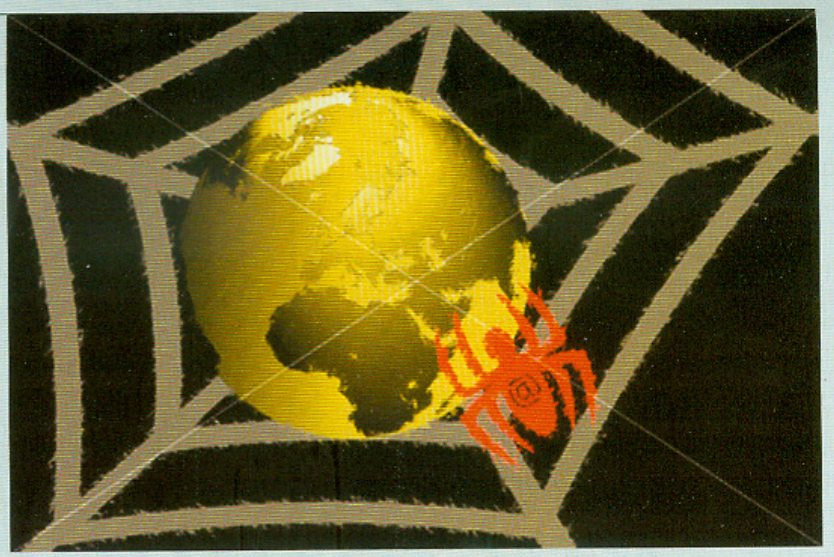


НАПАДИ НА ИНФОРМАЦИОНЕ СИСТЕМЕ

У многим светским државним и војним извештајима у планирању глобалне будућности и погледима како ће се свет развијати, идентификују се могућности и потенцијални негативни развој у глобалном друштву који може утицати на смер политичког и војног деловања. На бази консултација и са невладиним експертима дат је свеж поглед на кључне глобалне трендове за следећу декаду и њихов утицај на светска дешавања.

Тако на пример Национални обавештајни савет (National Intelligence Council, Washington) у свом пројекту планирања глобалне будућности до 2020. године наводи сајбер ратовање као специјалну тему и глобални тренд који ће утицати на планирање и изналажење метода борбе против таквих врста напада, а које се тичу нарочито државних односно војних структура.

Кретање традиционалних криминалних активности према повезаним рачунарским мрежама је еволутивно по природи, а наша држава није изузета од појаве таквог облика криминала и напада на информационе системе и мреже. Сходно томе у Београду је недавно (март 2007), у организацији Савета Европе, одржана тродневна конференција о високотехнолошком криминалу на којој су учествовали представници 12 земаља југоисточне Европе. Том приликом, министар правде Зоран Стојковић нагласио је да Србија заједно са осталим земљама региона мора да повећа ефикасност и брзину у борби против високотехнолошког криминала, који финансира тероризам и организовани криминал, те да су у тој борби неопходни јача међународна сарадња и ефикасни национални прописи из ове области. Конвенцију Саве-



та Европе о високотехнолошком криминалу ратификовало је 19 држава. Србија је документа потписала још 2005. године али до данас нису ратификована, чека се потврда Народне скупштине.

На конференцији је сагледано да је најчешћи облик сајбер криминала у Србији крађа приступних Интернет налога и шифри, односно крађа Интернет времена и наручивање робе и плаћања услуга путем украдених бројева кредитних картица и пиратерија. Примећено је да су у порасту и озбиљнији облици сајбер криминала као што су злоупотреба службеног положаја и индустријска и компанијска шпијунажа, тзв. инсајдери. Закључено је да у Србији чак и корисник просечног знања може доћи до веома поверљивих докумената преко локалних компанијских мрежа јер нису прописно заштићене.

Интернет, који је почео као компјутерска мрежа између универзитета и лабораторија, прерастао је у огромни јавни форум доступан свакоме ко поседује рачунар. Међународне организације, државне и војне структуре, компаније, универзитети, истраживачки центри и појединци, сви имају приступ и могу да га користе. Постао је јавно средство забаве, велики извор информација, важно маркетиншко средство и велико виртуелно електронско тржиште са великим бројем економских трансакција сваке секунде, а такође обезбеђује ефикасну и јефтину комуникацију између људи широм света.

Страни војни стручњаци разматрали су појаву Интернета и дошло се до закључка да драматичан раст у величини и значају и осталих облика дигиталних комуникација представља велики изазов за извођење помоћу средстава везе односно извођење непријатељевих средстава везе. Као један од будућих трендова у области војног извођења средстава везе и прикупљања података, између осталих наведен је снажан тренд у настојањима да се нападну туђи рачу-

ИНФОРМАЦИОНИ РАТ У ВОЈНОМ КОНТЕКСТУ

Информатичка револуција и нове технологије промениле су и дефиницију рата и вођења војних операција. Технолошке промене су током историје континуирано утицале на промену војне доктрине, организације и стратегије. Модерно ратовање више него икад захтева већу акумулацију разних информација и података да би војне операције биле ефикасније, а приступ информацијама је одлучујући фактор надмоћности у модерним војним операцијама, као и поседовање наоружања.

Појава нових врста неконвенционалног ратовања као што је ратовање путем рачунарске мреже (computer network warfare) и комуникационих система, односно сајбер рат (cyber war) или информационо ратовање (information warfare), захтева и нову терминологију везану за војне операције путем компјутерских мрежа. Као нова дисциплина, и даље флуидна, терминологија из ових области може бити неконзистентна и у истој публикацији. Из тог разлога у многим студијама страних војних стручњака дају се предлози нових термина и нових принципа ратовања из области информационих и комуникационих технологија, а сходно новим врстама претњи.

Информациони рат (IW-information warfare) – Напад на виталне рачунарске системе односно критичну националну инфраструктуру која контролише пренос података, комуникације, финансијске трансакције и др. У војном контексту информациони рат представља одређене акције да се постигне информациона супериорност нападајући противникове податке, информатичке процесе, информационе и комуникационе системе и рачунарске мреже, те стратегијски софтвер, док на другу страну брани сопствене податке, информационе процесе, информационе системе и мреже.

Дефинисане су следеће форме информационог рата: командовање и управљање ратом (Command and control Warfare), обавештајни рат (Intelligence-Based Warfare IBW), електронски рат (Electronic Warfare – EW), психолошки рат (Psychological Warfare – PSYW), сајбер рат (Cyberwar), хакерски рат (Hacker warfare) и рат економским информација (Economic Information Warfare – EIW).

Сајбер рат (Cyberwar) или рат путем рачунарске мреже (computer network warfare – CNW) односи се на предузимање војних операција према принципима везаним за информационе технологије. То значи ометање или уништавање информационих и комуникационих система у критичним инфраструктурама.

Критична или стратегијска инфраструктура (војна, економска, телекомуникације) је део државне инфраструктуре која се сматра најкритичнијом за национални интерес, и стога захтева посебну заштиту од сајбер и осталих напада. Предложена је подела на пет оваквих сектора: информациони и комуникациони системи, банкарство и финансије, енергетика, укључујући системе електричне енергије, нафте и гаса, системе физичке дистрибуције и витолне службе за становништво. Све ово зовемо сајбер простор (cyberspace), а односи се на електронски простор који креирају међусобно повезани рачунари у мрежама као што је Интернет и где се обавља комуникација и контрола сложеним системима. У сајбер простору изводе се и сајбер напади или напади путем рачунарске мреже (цомпутер нетњорк аттацк), а представљају акције ометања, деградирања или уништења података у рачунарима и мрежама помоћу вируса или преоптерећењем система путем e-maila или за илегалне активности, које могу утицати на јавну безбедност, државну безбедност, примену закона, пословне интересе, интересе потрошача или приватност.

ларски системи, користећи Интернет и остала средства, а посебно добијање приступа заштићеним фајловима или комуникацијама пре него што се обраде криптографски. Интернет и глобално тржиште креирали су слободан проток информација, система и софтвера, цена снаге рачунара опада за половину сваких 18 месеци. Све то укупно гледано представља велики изазов за одбрану од разних облика сајбер напада на цивилне и на стратегијске војне информационе и комуникационе системе и мреже, стратегијски софтвер као што су телекомуникационе мреже, контрола саобраћаја, дистрибуција електричне енергије, а који је доступан кроз рачунарске мреже.

Информационе технологије у исто време ограничиле су право особе на приватност јер могу бити идентификовани преко свог ИД броја (идентификационог броја) или својих евиденционих докумената или пословања. Постоје многе владине базе података које садрже информације о скоро сваком грађанину у многим земљама као нпр. базе података о идентификационим подацима људи (имена, звање и остало), затим базе података о финансијама (кредитни подаци, финансијско стање), за идентификацију људи (телефонски именик, градски попис, регистар гласача и друго). Контролни механизми су у многим земљама неадекватни да изађу на крај са софистицираним технологијама прегледа дигиталних података, а неке државе се користе и као подлога за тестирање нових технологија прегледа података.

Такође помињу се термини као сајбер инфилтрација (cyber infiltration) што се дефинише као пенетрација у одбрамбени систем помоћу контролисаног софтвер програма којим се може извести манипулација, напад или упад. Сајбер манипулација (cyber manipulation) прати инфилтрацију, а означава контролу система преко софтвера који оставља систем нетакнут, али користи капацитете система правећи тиме штету као што је нпр. софтвер помоћу којег се може искључити електрична енергија. Сајбер упад (cyber raid) протеже инфилтрацију, представља манипулацију или добијање података унутар система, који оставља нетакнут, али резултат је трансфер, уништење, или измена података као нпр. крађа e-maila или узимање листе пасворда са mail сервера.

ЗАШТИТА РАЧУНАРСКИХ МРЕЖА

Карактер информација одабраних за надгледање и сајбер нападе креће се од телекомуникационих система до нових информационих технологија. Што се тиче државних односно владиних и војних органа и организација, предмет интересовања у компјутерским мрежама и базама података су осетљиве информације и државне тајне, телебанкинг, порески документи и остале финансијске информације, подаци који се користе у операцијама критичних инфраструктурних система односно стратегијског софтвера, општи уговори примљени електронском поштом и др.

Што се тиче финансијског пословања, предмет интересовања опасних групација у информационим и комуникационим системима могу бити уговори, фактуре (рачуни) и остала службена документација, поверљиве електронске трансакције и лиценце у тајним трансакцијама, подаци о пословима везаним за државну имовину, налози за наплату помоћу кредитних картица, наплате примљене on-line итд. Подаци преко Интернета могу бити сакупљени директно или индиректно, другим речима, могу се сакупити у тренутку контакта са кореспондентом (дописником) или без знања особе, често аутоматски. Природа прикупљених података варира према протоколима који се користе у мрежи тј. према типу сервиса. У пракси, различити протоколи се веома често користе у комбинацији, а према повећању профитабилности или количине размене. Зато у сврху заштите виталних рачунарских мрежа и система треба обезбедити шифровани командни приступ и регистровање упада у систем.

Може се закључити да се сајбер напади све више интензивирају, да је он већ у току, и да није виртуелна димензија, већ груба стварност која се одвија како између супротстављених држава и групација, тако и између „савезника" и коалиционих припадника. ■

Дијана МАРИНКОВИЋ