РАЗВОЈ И ЗАШТИТА ИНФОРМАЦИОНИХ СИСТЕМА

РАЊИВОСТ ГЛОБАЛНИХ ТЕХНОЛОГИЈА

Стратегијским прегледом одбране Републике Србије, као најзначајнијим документом за планирање, организацију и остваривање процеса реформе система одбране Србије и Војске Србије до 2010. године, између осталих приоритета наведен је и развој телекомуникационо -информационог система, односно његова техничка модернизација. У тим процесима трансформације и модернизације требало би детаљно размотрити и стручно проценити правце развоја и заштите телекомуникационих и информационих система, сходно захтевима руковођења и командовања.

Развојем технологија електронских система осматрања и извиђања али и информационих технологија, расте и ризик од злоупотребе војних, економских и осталих поверљивих информација, нарочито због пораста тероризма данас у свету. Сходно томе веома је важно да се обрати велика пажња на развој криптосистема и заштите од електронског извиђања, те уради добра техничка процена заштите информација у будућности.

Уз тенденцију ка европским интеграцијама у сваком погледу, па и у војном, морамо се информисати о прогнозама развоја технологија у свим областима, поготово што је фокус њиховог војног занимања постављен у областима комуникација и информационих система. Тако Агенција Натоа за консултације, командовање и контролу (NATO Consultation, Command and Control Agency – NC3A) у својим дугорочним студијама развоја технике до 2025. године даје процене и прогнозе о потенцијалним технолошким трендовима у одређеним областима и нивоима оспособљености. У студији је обухваћено 14 основних технолошких области, а затим је дата синтеза односно уопштавање ових општих категорија у шест области интересантних за војне сврхе, међу којима су комуникациони и информациони системи.

РАЗВОЈ ИНТЕРНЕТА

Тако је NC3A у свом документу размотрила, односно прогнозирала трендове, чији детаљи садржаја обезбеђују планерима њихову ширу и дубљу анализу, те разумевање и разматрање способности, ефеката и утицаја на војне операције, те ризике које носи одређени напредак у тој технолошкој области. У својој глобалној прогнози развоја технологија није им била намера да предвиђају будућност и стриктно намећу решења, већ омогуће скуп опција развоја, односно избор за будућност, наглашавајући могућности одређених технолошких области без политичких и економских утицаја и аспирација.

Анализом нових технологија у домену телекомуникационих и информационих система сагледано је шест главних трендова у области Интернета који ће доста утицати на њих. Први међу њима је Интернет и његова web инфраструктура, која ће наставити да се шири, тако да се предвиђа да ће Интернет технологије многе организације користити као примарни сервис.

Следећи тренд се односи на сервисно оријентисане структуре које ће фокусирати своју делатност на испоруку информација до корисника и њихова снага мериће се њиховом способношћу да испоруче услугу која треба да буде приступачна, а у исто време водећи рачуна о безбедности и приватности корисника. Ширењем опсега мреже за коју се предвиђа да ће наставити да расте, очекује се и да сервиси који пружају Интер-

нет услуге обезбеде информације на правовремен начин.

Употреба и производња мобилних рачунарских система наставиће драстично да расте због употребе интегрисаних рачунара, а web технологија биће основни механизам за рад таквих уређаја. Током тог процеса вредност рачунарских средстава наставиће да пада, док ће истовремено трошкови људских ресурса расти, али ће се настојати да се у том процесу нађе решење које ће задовољити све стране.

На крају се предвиђа да ће садашње сервисе који обезбеђују Интернет услуге клијентима заменити државне и пословне мреже које ће радити у једном центричном рачунарском окружењу, што ће допринети да они имају једну активну улогу у развоју мреже и пружања услуга.

Можемо дакле закључити да ће снага рачунара, као и развој и побољшање преноса података и обим њихове размене за различите сврхе и услуге, наставити да расте. Сагледавањем коришћења тих технологија код војних организација треба да се задовоље захтеви безбедности и трошкова, тако да ће борба између могућег и прихватљивог у војсци увек постојати, што у неким тренуцима може оспорити развој у тим структурама.

САЈБЕР РАТОВАЊЕ

Следеће две кључне области из информационих технологија које треба глобално размотрити у смислу планирања развоја и заштите су командни и информациони системи и кибернетско сајбер ратовање (cyber warfare).

Главне теме у разматрању планирања командних и информационих система су оне које се тичу развоја инфраструктуре и софтвер технологија.

Инфраструктура информационих система зависиће од снаге и перформанси рачунара, начина чувања података и њиховог руковођења, а то ће бити и један од главних проблема у будућем периоду. Зависиће такође и од инфраструктуре мреже за коју се предвиђа повећање брзине и увођење нових Интернет сервис модела, затим комуникација и безбедности инфраструктуре. Предвиђа се унапређивање дигиталних интегрисаних кола, а тиме и побољшања перформанси рачунара, а потом и њихово опадање после 2018. године, јер тренутне пратеће технологије неће бити у могућности да подрже такав развој процесора и повећање њихове брзине чак изнад 5 GHz, што доноси одређене тешкоће у раду. Ипак, решавање тог проблема види се у паралелном раду више процесора што повећава снагу рачунара да би се задовољиле одређене апликације.

Развој софтвер технологија утицаће на области као што су web технологије које представљају једну од најбрже растућих подручја за развој трговине и услуга, такође на руковођење информацијама и њихово коришћење и обликовање односа људи и машина.

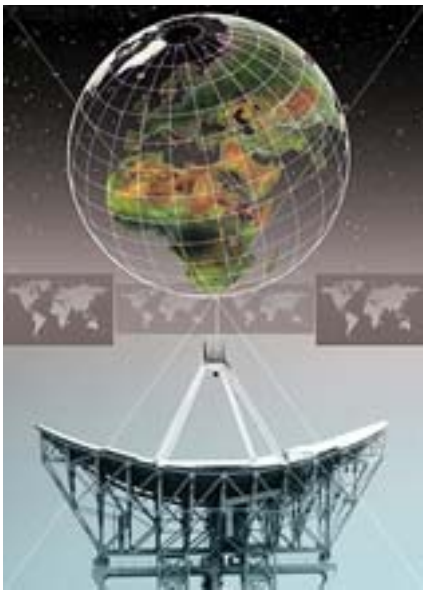
Појавом нових технологија, посебно у области информатике и комуникација у комбинацији са текућим процесом глобализације, отварају се нове могућности у свим областима. Наравно, то носи и одређене тешкоће и проблеме у погледу приватности, етике и опасности поготово за војне телекомуникационе и информационе системе, јер опасне групације могу да их злоупотребе и угрозе.

БЕЗБЕДНОСТ КОМУНИКАЦИЈА

Квантна криптографија је основ за заштиту комуникационих мрежа од велике важности и поверљивости, закључио је Европски пројект SECOQC (Secure Communication based on Quantum Cryptography). Безбедност комуникација на бази квантне криптографије је пројекат који финансира Европска унија са 11,4 милиона евра. Иницирао га је аустријски истраживачки центар и чини га 12 земаља које су укључене у тај пројект.

ЗЛОНАМЕРНИ НАПАДИ

Постоје многа, свима доступна средства која омогућавају да било која компјутерски писмена особа нападне, искористи, упадне, извиди и претражи одређене компјутерске мреже. У већини случајева напади долазе од злонамерних хакера, индустријске шпијунаже, терориста и других нација. Њихови напади су углавном усмерени на националне инфраструктуре, банковне системе, комерцијалне и административне системе. Али, противник може циљати и на војне информативне мреже да би ометао мобилизацију и развој борбеног поретка, борбене операције и логистичко снабдевање.



Механизми заштите, као што су антивирус софтвери и network firewalls (програм који се брине о улазу и излазу програма кроз тзв. портове), чине базу за безбедност инфраструктуре, заједно са приступним заштитним мерама као што је криптографско потврђивање приступа. Међутим, јасно је да такве мере не могу дати тоталну заштиту информација и мреже, поготово када се у будућности рашири употреба бежичне технологије која носи са собом и веће могућности за сајбер нападе (cyber-attacks), а ослањање на поменуте механизме заштите постаје недовољно.

Сајбер рат укључује употребу информационих система или информационих технологија да се онеспособе, искористе или униште противникови информациони системи. Може бити усмерен на војну, економску или телекомуникациону инфраструктуру, и може бити покренут из било ког дела света. Све широм употребом углавном комерцијалног софтвера чији детаљи и приступачност су широко познати, расте рањивост одређених организација, поготово у области одбране. Поменимо да многи оружани системи данас користе такав комерцијални софтвер.

У разматрањима се дошло до закључка да постоје знаци да комплексност компјутерских мрежа расте брже него способност да се она разуме и заштити. Такође, од поузданости и расположивости информационих система зависиће одбрана и безбедност војних структура и неке државе уопште.

КВАНТНА КРИПТОГРАФИЈА

На крају можемо закључити да су многе државе и њихова научна војна тела препознала проблем заштите телекомуникационих и информационих система и мреже и предложила мере за обезбеђење заштите, поготово што и њихов целокупан развој, производња и безбедност зависи од поменутих технологија.

Сагледана је и важност информација у свим доменима и њихова заштита у будућности која се види у развоју квантних компјутера и квантне криптографије. Предвиђа се да ће квантни компјутери бити доступни великим организацијама и владама до 2015. године, а осталима највероватније до 2025. Први експерименти у овој области обављени су већ 2004. у Европи, а такође и у САД где су Национална агенција за безбедност и једна банка у саставу федералних резерви већ купиле од одређених компанија квантне криптографе. Сматра се да тајни кључ састављен од светлосних честица – фотона нико неће моћи да провали и у томе се види будућност заштите информација, што ће из темеља променити криптографију у целини.

Циљ пројекта је увођење квантне криптографије и постављање камена темељца за глобалну заштиту комуникационих мрежа истраживањем квантне технологије и њена уградња у криптографију, мрежне технологије и остале области везане за информационе технологије. Производња кључева кренула би 2008. године. Тада се предвиђа завршетак пројекта који је почео 2004. и који отвара нову еру развоја заштите информација кроз безбедност компјутерских мрежа у целини. ■

Дијана МАРИНКОВИЋ