УДК: 007:004.056 ;
343.533::004

ПРИЛОГ НАЦИОНАЛНОЈ СТРАТЕГИЈИ ЗАШТИТЕ КИБЕР-ПРОСТОРА

Слободан Р. Петровић[*]

Удружење судских вештака за информационе технологије, Београд

Ефекти и импликације информационе револуције указују, с једне стране, на њен огроман потенцијал исказан приликама и могућностима доступним савременом човеку, а, с друге стране, на сву озбиљност и сложеност њених импликација због којих информационо друштво постаје зависније од те технологије и осетљивије на разне врсте поремећаја, са потенцијалним последицама у распону од тривијалних до катастрофалних. Управо те чињенице намећу императивну потребу предузимања адекватних заштитних мера и акција, не само на микроплану и у локалу већ, пре свега, на националном нивоу, са тенденцијом да се оне, због глобалне природе проблема, уклопе у мере и акције међународне заједнице. У том контексту у раду се указује на неопходност доношења националне стратегије заштите кибер-простора и сугеришу и образлажу неки од елемената те стратегије.

Кључне речи: *кибер-простор, информациона технологија, информациона инфраструктура, претње, стратегија, заштит*.

Увод

Савремени развој технологија обогатио је речник бројним новонасталим терминима међу којима су и „национална информациона инфраструктура“ и „информациона супераутострада“. Међутим, мада су ти термини недавно постали део речника, друштва су увек имала своје инфраструктуре. Од поште која је преношена бродовима и Пони Експресом, преко телеграфа, телефона и бежично, човек је развијао начине и технологије који су му омогућавали комуникацију са другима који су били мање или више

[*] Проф. др Слободан Р. Петровић је председник Скупштине удружења, slobo.petrovic@nadlanu.com.

удаљени од њега. Оно шта је тако драматично другачије код данашњих информационих инфраструктура јесте *моћ* и *досег*. Дигитална технологија, оптички пренос података и информација и континуирано бујање могућности микрочипова у обради података изродили су ширење комуникационе мреже широм света. Тај технолошки напредак нуди безбројне могућности у буквално свим пољима људске делатности. Инвестирање значајних средстава у развој и имплементацију не само информационих, већ и других мрежних инфраструктура – физичких мрежа, као што су мреже за енергију и транспортни системи, и виртуелних мрежа, као што је интернет, допринели су да савремена друштвена заједница и модеран начин живота све више постају зависни од изграђене мрежне инфраструктуре, а самим тим и рањивији, односно осетљивији на разне врсте поремећаја.[1]

С тим у вези позната је чињеница да терористи, атакујући на један или више делова физичке инфраструктуре, могу разорити целе системе и изазвати значајне проблеме за нацију. Међутим, много мање је познато да терористички напади на виртуелну мрежну инфраструктуру могу изазвати исте, ако не и озбиљније националне проблеме. Због тога је неопходно побољшати заштиту појединачних делова и интерконектованих система који чине критичну инфраструктуру. Заштита критичне инфраструктуре и кључних добара неће их само учинити безбеднијим од терористичких атака, већ ће, такође, редуцирати и њихову осетљивост на природне катастрофе, организовани криминал, хакере и разнородне шпијунске активности противника.

Релативно кратак и не превише детаљан приказ ефеката и импликација информационе револуције, изложен у ауторовом претходном раду,[2] довољно јасно указује, с једне стране, на њен огроман потенцијал исказан приликама и могућностима доступним савременом човеку, а, с друге стране, на сву озбиљност и сложеност њених импликација које више него јасно најављују да информационо друштво у све већој мери постаје зависније од те технологије и осетљивије на разне врсте поремећаја, са потенцијалним последицама у лепези од тривијалних до катастрофалних. Управо из те чињенице произилази императивна потреба предузимања адекватних заштитних мера и акција, не само на микроплану и у локалу, већ, пре свега, на нацио-

[1] Anderson K, *Computers and the Information Revolution*, Updated 2002 Probe Ministries, http://www.leaderu.com/orgs/probe/docs/computer.html; Петровић Р. С., *О информационој револуцији у контексту злоупотребе информационе технологије*, Саветовање Злоупотреба информационих технологија (ZITEH), Зборник радова (CD-ROM), Тара, 31. мај – 03. јун 2004; *The National Strategy to Secure Cyberspace*, The White House Washington, february 2003, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf ; Copeland E. T, *The Information Revolution and National Security*, August 2000, http://www.strategicstudiesinstitute.army.mil/pdffiles/pub225.pdf

[2] Петровић Р. Слободан, *О неопходности националне стратегије заштите кибер-простора*, Наука, безбедност, полиција (NTB), Београд, vol. XI, no. 2, 2006, стр. 3–28. http://www.kpa.edu.rs/data/akademija/nbp/nbp_2006_2.pdf

налном нивоу, са тенденцијом да се оне, због глобалне природе проблема, уклопе у мере и акције међународне заједнице.

Критична инфраструктура обухвата велики број сектора. Зато, заштитом добара, система и функција виталних за националну безбедност, државну управу, економију и национални морал, треба уклонити могућност да се наносе трајне и/или велике штете нацији. Дакле, „здраво" функционисање кибер-простора је суштинско за економију и за националну безбедност, посебно што бројни догађаји осветљавају постојање високе осетљивости кибер-простора и чињеницу да злонамерни актери континуирано покушавају да ту осетљивост максимално експлоатишу.

Слика стања

Да бисмо могли да оценимо и што прецизније лоцирамо наше место и улогу у кибер-простору, послужићемо се статистичким показатељима који се односе на коришћење интернета,[3] а који су, у данашње време, кључни индикатори достигнутог технолошког развоја.

Табела 1 – *Стање у земљама у окружењу*

Земља	Популација (процена за 2008)	Корисници интернета	Захваћено популације у %	Увећање корисника у % (2000–2008)
Словенија	2.007.711	1.300.000	64,8	333,3
Бугарска	7.262.675	4.000.000	55,1	830,2
Румунија	22.246.862	12.000.000	53,9	1.400,0
Хрватска	4.491.543	1.995.400	44,4	897,7
Мађарска	9.930.915	4.200,000	42,3	487,4
Црна Гора	678.177	280.000	41,3	…..
Македонија	2.061.315	685.000	33,2	2.183,3
БиХ	4.590.310	1.055.000	23,0	14.971,4
Србија	10.159.046	1.500.000	**14,8**	275,0
Албанија	3.619.778	471.200	13,0	18.748,0

Судећи по табели, у којој су подаци рангирани у затамњеној колони, очигледно је да се у односу на републике бивше заједничке државе и државе у непосредном окружењу не можемо похвалити. Једино смо по броју становника на другом месту – иза Румуније. Иначе, по проценту популације која користи интернет (14,8%) на самом смо дну. Иза нас је само Албанија (13,0%), али је она за период 2000–2008. имала стопу пораста од фантастичних 18.748,0%, а наша је износила само 275,0%.

[3] Internet World Stats, http://www.internetworldstats.com/stats4.htm

Табела 2 – *Стање у земљама кандидатима за пријем у ЕУ*

Земља кандидат за пријем у ЕУ	Популација (процена за 2008)	Корисници интернета	Захваћено популације у %	Увећање корисника у % (2000–2008)
Хрватска	4.491.543	1.995.400	44,4	897,7
Турска	71.892.807	26.500.000	36,9	1.225,0
Македонија	2.061.315	685.000	33,2	2.183,3
УКУПНО	**78.445.665**	**29.180.400**	**37,2**	**1.208,5**

У односу на стање у земљама кандидатима за пријем у Европску унију такође смо са 14,8% инфериорни и у појединачном поређењу и у односу на њихов просек (37,2%).

Табела 3 – Стање у земљама Европске уније

Земље Европске уније	Популација (процена за 2008)	Корисници интернета	Захваћено популације у %	Увећање корисника у % (2000–2008)
Холандија	16.645.313	15.000.000	90,1	284,6
Шведска	9.045.389	7.000.000	77,4	72,9
Португалија	10.676.910	7.782.760	72,9	211,3
Луксембург	486.006	345.000	71,0	245,0
Финска	5.244.749	3.600.000	68,6	86,8
Данска	5.484.723	3.762.500	68,6	92,9
Велика Британија	60.943.912	41.817.847	68,6	171,5
Словенија	2.007.711	1.300.000	64,8	333,3
Немачка	82.369.548	52.533.914	63,8	118,9
Шпанија	40.491.051	25.623.329	63,3	375,6
Естонија	1.307.605	780.000	59,7	112,8
Италија	58.145.321	34.708.144	59,7	162,9
Француска	62.177.676	36.153.327	58,1	325,3
Аустрија	8.205.533	4.650.000	56,7	121,4
Бугарска	7.262.675	4.000.000	55,1	830,2
Румунија	22.246.862	12.000.000	53,9	1.400,0
Белгија	10.403.951	5.490.000	52,8	174,5
Чешка Република	10.220.911	5.100.000	49,9	410,0
Ирска	4.156.119	2.060.000	49,6	162,8
Кипар	792.604	380.000	47,9	216,7
Литва	2.245.423	1.070.800	47,7	613,9
Словачка	5.455.407	2.350.000	43,1	261,5
Мађарска	9.930.915	4.200.000	42,3	487,4
Пољска	38.500.696	16.000.000	41,6	471,4
Малта	403.532	158.200	39,2	295,0
Литванија	3.565.205	1.333.200	37,4	492,5
Грчка	10.772.816	3.800.000	35,3	280,0
Европска унија	489.188.563	292.999.021	57,0	326,3

У поређењу са земљама Европске уније код којих је, са бројем становника 489.188.563 (процена за 2008) и бројем корисника интернета 292.999.021 (подаци ажурирани 30. јуна 2008), просечан проценат корисника интернета 57,0%, ситуација је још неповољнија, јер је наш проценат корисника интернета (14,8%) скоро четвороструко нижи од просека у Европској унији.

Слично је и у односу на светску популацију (број становника 6.676.120.288, број корисника интернета 1.463.632.361, или 21,9%, што је такође изнад нашег процента (14,8%).

Табела 4 – Стање у земљама са највишим процентом корисника

#	10 водећих земаља	Популација (процена за 2008.)	Корисници интернета	Захваћено популације у %
1.	Гренланд	56.326	52.000	92,3
2.	Холандија	16.645.313	15.000.000	90,1
3.	Норвешка	4.644.457	4.074.100	87,7
4.	Аниква и Барбуда	69.842	60.000	85,9
5.	Исланд	304.367	258.000	84,8
6.	Канада	33.212.696	28.000.000	**84,3**
7.	Нови Зеланд	4.173.460	**3.360.000**	80,5
8.	Аустралија	20.600.856	**16.355.427**	79,4
9.	Шведска	9.045.389	7.000.000	77,4
10.	Фокландска острва	2.483	1.900	**76,5**

Поређење са 10 водећих земаља света, код којих се проценат корисника интернета у односу на популацију креће између 92,3% (Гренланд, који је на првом месту) и 76,5% (Фокландска острва, која су на десетом месту), за сада не би имало смисла.

Табела 5 – Стање у европским земљама са најнижим процентом корисника

#	Последњих пет у Европи	Популација (процена за 2008)	Интернет корисници	Захваћено популације у %	Увећање корисника у % (2000–2008)
1.	Украјина	45.994.287	10.000.000	21,7	4.900,0
2.	Ватикан	549	93	16,9	0,0
3.	Молдавија	4.324.450	700.000	16,2	2.700,0
4.	Србија	10.159.046	1.500.000	14,8	275,0
5.	Албанија	3.619.778	471.200	13,0	18.748,0

Међу пет земаља које су на дну европске листе по проценту популације која користи интернет налази се и Србија. Иза ње је само Албанија. Нажалост, Србија је, изузимајући Ватикан, имала најмањи проценат увећања ко-

рисника за период 2000–2008. (свега 275%), док је Албанија, која је последња на листи, имала увећање 18.748%, а Молдавија и Украјина, које су испред Србије, имале су 2.700%, односно 4.900% респективно. Изложени подаци указују да ће, у случају да се наведени тренд настави, Србија дуже време остати на претпоследњем месту. Иза ње ће вероватно бити само Ватикан, који је вероватно достигао свој максимум.

Ако се узме у обзир да су информациона технологија и њен најснажнији инструмент – интернет – главни покретачи друштвеног развоја данашњице, онда су наведени подаци толико алармантни и иритирајући да би ретко кога у Србији могли да оставе равнодушним. Таква, не баш сјајна позиција, која је првенствено последица свих оних немилих и нежељених појава и догађаја који су нас пратили у недавној прошлости, али и низа наших унутрашњих слабости и проблема, не даје нам за право да будемо пасивни, напротив. Утолико пре, јер су обиман развој наше националне информационе инфраструктуре и растућа примена информационе технологије сасвим извесни и незаустављиви процеси. С тим у вези, не смемо превидети чињеницу да ће шира примена информационе технологије и нас учинити осетљивијим и рањивијим, што нам, уколико ништа у том смислу не предузмемо, итекако може загорчати будућност. Зато се већ сада морамо припремити да на адекватан и целовит начин редуцирамо осетљивост националног кибер-простора на све потенцијалне претње које могу озбиљније угрозити критичну инфраструктуру и кључне ресурсе, а које ће се временом само умножавати и појачавати.

При томе треба знати да је заштита националног кибер-простора *екстремно тежак стратешки изазов, који захтева пуно стручности и знања, материјалних и финансијских ресурса, кооперацију и координацију великог броја чинилаца и фокусирање на напоре целе заједнице* да се обезбеди да такви поремећаји кибер-простора буду ретки, минималног трајања, парцијални и да изазивају најмању могућу штету по националне интересе и интересе грађана. Приступни принцип је крајње једноставан: *уложити више данас да би нас сутра много мање коштало!*

Заштита кибер-простора

Није потребно посебно наглашавати да се национални интереси не могу бранити само лепим жељама и добрим намерама, већ адекватном акцијом. Зато, одговорни за безбедност и заштиту земље и нације морају знати и разумети важност и тежину чињенице да смо укључивањем у интернет креирали наш виртуелни кибер-простор, који је по значају адекватан ваздушном простору и нашим речним и копненим границама. У њему се већ извршавају функције чији се број и разнородност непрекидно увећавају и од

којих су многе виталне са становишта националних интереса. У исти простор се у дигиталној форми увелико складиште и по информационим аутострадама преносе наша информациона, интелектуална, духовна, материјална и финансијска добра, чији се обим и укупна вредност такође само увећавају. Стога, узимајући у обзир чињеницу да смо земља са веома скромним потенцијалом и ресурсима, било би крајње неразумно и неодговорно да оно што имамо олако препустимо на милост и немилост онима који нису малобројни, а спремни су и способни да то искористе и злоупотребе и на најдиректнији начин угрозе наше националне интересе.

С тим у вези, треба имати у виду да је национална безбедност термин који се првенствено везује за владу, чиме се указује на њену кључну одговорност за стање у тој области. Зато је од суштинског значаја да државно руководство прихвати изазове нове технологије и да на адекватан начин (осмишљено и целовито) одговори на њих. Императивни задатак владе и њених органа задужених за безбедност и заштиту земље и нације био би усвајање основних принципа и на њима засноване политике заштите националног кибер-простора, а остварени резултати ће у највећој мери зависити управо од њихове спремности и способности да иницирају и истрају у реализацији тог значајног, обимног и сложеног задатка.

Отежавајућа околност да влада прецизно дефинише опсег опасности за националну информациону инфраструктуру јесте у чињеници да, као и у већини других земаља, изостаје одговарајућа активност обавештајне заједнице у прикупљању релевантних података и њиховој аналитичкој процени. Постоје бројна објашњења зашто обавештајне и криминалистичке службе нису у стању да колективизирају захтеване податке за процену националних претњи: прво, проблем се не сматра национално значајним, најчешће због непознавања и неразумевања, па с тим у вези и не постоји обавезно извештавање; друго, због бројних специфичности информационе технологије из легалне и организационе перспективе обавештајно колектирање је тешко у виртуелном свету у којем владају електронски импулси и дигитални бројеви. У физичком свету обавештајне и контраобавештајне одговорности базиране су, највећим делом, на извору – пореклу претњи. Стога, генерална подела посла у том домену, широко распрострањена у свету, јесте да је обавештајна заједница (нпр. *CIA* у САД или БИА код нас) одговорна за процену спољних претњи, док су криминалистичке службе (као што је *FBI* у САД) одговорне за процену домаћих (унутрашњих) претњи. При томе, постоје правила која лимитирају могућност једне службе да се меша у домен рада друге службе. Тако је, на пример, *CIA* лимитирана у прикупљању домаћих информација. Слично, *FBI* није активан у прикупљању страних информација.[4]

[4] *Security in cyberspace*, Staff statement, U.S. Senate, Permanent subcommittee on investigations, june 5, 1996, http://www.fas.org/irp/congress/1996_hr/s960605t.htm

Међутим, виртуелни свет је, ипак, свет без граница и стога се не уклапа лако у организацију физичког света, па и та подела домена рада између појединих служби у том (виртуелном) свету не би била одржива. Технологије које примењују хакери дозвољавају им да узимају бројне путање када нападају циљ. На пример, за један напад који потиче из стране земље није необично узети заобилазну руту кроз различите нације и различите рачунарске мреже, и јавне и приватне. Дакле, када је напад откривен може се показати да он потиче из домаћег рачунара иако стварно потиче изван границе земље, што то би у разрешавању таквих случајева, према садашњем стању ствари, водило до сукоба надлежности.

Коначно, и можда најзначајније, то једноставно још није висок приоритет обавештајне заједнице. Све док државно руководство активно и експлицитно не означи информационе претње национално значајним, сигурно је да неће постојати спремност да се врши релоцирање ионако ограничених ресурса ка новим активностима.

Међутим, и без те подршке, која би свакако била врло значајна и која ће и убудуће бити веома потребна због изражене динамике, сложености и озбиљности проблема, влада мора да има истанчан осећај и довољно слуха да препозна потенцијалну жестину тог проблема и да означи његове врло озбиљне импликације на националну безбедност.

Оно што, свакако, не би смело да се деси јесте да у изради и спровођењу наше стратегије заштите кибер-простора буквално копирамо решења развијених земаља, посебно САД. Разлог је једноставан. Амбијенти нам се драстично разликују у свим елементима, укључујући достигнут технолошки ниво, степен остварене аутоматизације, ниво интегрисаности, бројност и стручност информатичких кадрова, бројност и обученост корисника и др. С тим у вези, посебно треба имати у виду да, с обзиром на чињеницу да влада САД у односу на приватни сектор администрира само са минорним делом националне критичне инфраструктуре и користи веома мали део кибер-простора,[5] основу њихове стратегије за заштиту кибер-простора представља чврсто партнерство јавног и приватног сектора. За разлику од ситуације код нас, њихов приватни сектор је веома развијен економски, технички, финансијски и стручно, располаже значајним делом кибер-простора у којем су смештене бројне критичне информационе инфраструктуре намењене њиховим потребама и у којем је свест о потреби заштите на завидном нивоу. Као најбоље опремљен и структуриран тај сектор је заинтересован и способан да у кооперативном партнерству са друштвеним сектором преузме свој део одговорности за заштиту кибер-простора.

Код нас је приватни сектор још увек неразвијен, без значајне сопствене информационе инфраструктуре, а свест и потреба за озбиљнијом заштитом још нису стекли право грађанства. С друге стране, ни друштвени сектор,

[5] *The National Strategy to Secure Cyberspace*, op. cit.

због поменутих недаћа које су нас пратиле, није превише одмакао у развоју. Међутим, значајно је указати да су присутни велика жеља и спремност да се изгубљено надокнади. Један од примера који недвосмислено потврђује наведену констатацију јесте и недавно усвојена *Национална стратегија изградње информационог друштва Републике Србије*.

Дакле, иако се на нашим просторима информациона технологија још увек не користи у великој мери и на интегрисан начин, ипак се значајни помаци не могу негирати. При томе највећу обавезу, бар у почетној фази, у предузимању адекватних мера и акција има влада са својим органима, како би обезбедила амбијент који би својом поузданошћу, безбедношћу и функционалношћу подстицајно деловао и на друштвени и на приватни сектор да се обухватније и снажније укључе у изградњу и развој информационих инфраструктура и у још ширу примену информационе технологије, тренутно главног покретача свеукупног друштвеног прогреса и у локалним и у глобалним размерама.

Данас када, због релативно слабо развијене националне информационе инфраструктуре, наша осетљивост није висока, па велике непосредне опасности тренутно и нема, требало би искористити указану шансу и припремити се за времена која долазе.

До сада обављене активности – Кривични законик усвојен 2005. године проширен је новим кривичним делима која се односе на рачунарски криминал, заштиту ауторских права и др. („Службени гласник РС“, број 85/05), Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала („Службени гласник РС“, број 61/05) и Закон о информационом систему Републике Србије (ИС ДОС) („Службени гласник РС“, број 12/96) могу да послуже као полазна основа за даљу добро осмишљену и свеобухватну акцију заштите кибер-простора.

У свом деловању у овој области, користећи домаћа знања и туђа позитивна искуства и решења, влада би требало да се руководи унапред усвојеним организационим и другим принципима, од којих би свакако требало поменути следеће:[6]

– *носилац активности – влада:* Улога владе у почетној фази заштите кибер-простора била би у *иницирању, усмеравању, подстицању и контроли* достизања прокламованих базичних циљева, док би се у каснијој фази, након што би биле изграђене респектабилне снаге заштите и у друштвеном и у приватном сектору, активност владе постепено преусмеравала ка другим задацима и циљевима. Ту се, пре свега, мисли на *промовисање* боље заштите,

[6] *National Infrastructure Protection Plan*, US Department of Homeland Security, 2006, www.dhs.gov/nipp; *National strategy for homeland security*, Office of Homeland Security, july 2002, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf; *Security in cyberspace*, op. cit; *The National Strategy to Secure Cyberspace*, op. cit.

подстицање на сарадњу и партнерство активних субјеката, *дељење информација* о кибер-претњама и осетљивостима, тако да сви заинтересовани ентитети могу усаглашавати своје стратегије управљања ризиком и планове реализације, *промовисање* креације и сарадње ради уздизања свести о потреби заштите, обучавања кадрова, идентификовања и отклањања слабости – осетљивости, размене информација и израде планова обнове – опоравка;

– *заштита приватности и цивилних слобода.* С обзиром на то да злоупотреба кибер-простора омогућава и олакшава нарушавање приватности и цивилних слобода грађана, дужност владе је да онемогућава такву повреду и злоупотребу. Кибер-заштита и персонална приватност не би требало да буду супротстављени циљеви. Програми заштите кибер-простора морају ојачавати, а не слабити, заштиту приватности и цивилне слободе. Дакле, пажња мора бити посвећена поштовању интереса приватности и другим цивилним слободама. Грађани *глобалног села* морају веровати да ће се са информацијама које нису јавне руковати тачно, поверљиво и поуздано, а бољег гаранта од владе сигурно нема. У том смислу влада би требало да предводи примером имплементирајући снажне политике и праксе приватности у својим органима;

– *регулациона и тржишна присила.* У разрешавању многих, па и овог проблема, могућа су три приступа: мобилизаторски подстицајним мерама, регулативним мерама и тржишном присилом. Државна регулатива не би требало да постане примарни начин заштите кибер-простора. Широко регулативно наређивање на који начин и како сви корисници информационе технологије морају конфигурисати своје информационе системе наметнуло би приступ најнижег заједничког имениоца кибер-заштите, што би могло представљати ограничавајући фактор успешнијим напорима разрешавања проблема. Чак и горе од тога, такав приступ могао би резултирати мањом заштитом него што је потребно, јер би је укључивање нове технологије брзо маргинализовало. Имајући то у виду могло би се констатовати да би било најбоље да сâмо тржиште обезбеди главни подстицај побољшању кибер-заштите и у том правцу би требало усмерити и владине акције;

– *надлежности и одговорности.* У политици која би се спроводила мора бити присутан став о потреби да се јасно назначе надлежности и одговорности свих учесника у реализацији заштите, као и водећи извршиоци за поједине кључне активности. Овде се мисли, пре свега, на надлежности и одговорности државних органа (криминалистичке и тајне службе, правосуђе, ...);

флексибилност. Кибер-претње се мењају рапидно. Сходно томе, усвојена политика би подразумевала неопходност да се наглашава потреба флексибилности у могућностима да се одговори на кибер-напад и управља редукцијом осетљивости. Рапидни развој алата за напад снабдева потенцијалне нападаче стратешком предношћу да брзо адаптирају своје офанзивне тактике циљу уочавањем слабости у умреженим информационим системи-

ма и могућностима нападнутог да одговори. С тим у вези, посебно треба имати у виду чињеницу да заштита кибер-простора не може бити непробојна на планиране и интелигентне нападе. Зато, информациони системи морају бити толико еластични да су у стању да функционишу док су под нападом и морају имати способност враћања у првобитно стање и постизање пуне оперативности након извршеног напада. Дакле, флексибилност треба да омогући онима који се штите да спрече напад, да се након напада брзо опораве и да могу поново да процене приоритете и прегрупишу ресурсе ако је кибер-претња изведена;

– *дугорочно планирање.* Заштита кибер-простора је процес који је у току и одвија се паралелно са појављивањем нове технологије и идентификовањем нових претњи и опасности, односно осетљивости. Због тога би требало обезбедити један иницијални оквир за достизање циљева заштите кибер-простора. Државни органи (влада, министарства и агенције) требало би да развију дугорочне планове заштите кибер-простора и да их прилагођавају за подршку њиховим потребама и улогама. И друге организације јавног и приватног сектора требало би, такође, да буду охрабрене да разматрају дугорочне планове заштите.

Стратегија заштите кибер-простора

Политика владе, заснована на наведеним и другим релевантним принципима, требало би да у разматраном контексту подразумева: *спречавање поремећаја операција информационих система за критичне инфраструктуре, како би се остварила заштита људи, економије, есенцијалних сервиса и националне безбедности земље, уз континуиран напор свих релевантних друштвених чинилаца.*

Успешна реализација упрошћено исказане, али свеобухватне и амбициозне политике на изнетом нивоу општости подразумева потребу да се сагласно усвојеним принципима и на њима дефинисаној политици обликује *национална стратегија заштите кибер-простора*, чији би кључни циљеви, поред осталих, требало да буду:

– спречавање кибер-напада против критичне инфраструктуре и кључних ресурса;

– редуковање националне осетљивости на кибер-нападе;

– минимизирање штете и времена обнове (опоравка) од кибер-напада који се десио.

Дакле, потребна нам је једна снажна стратегија која би означила осетљивост наше информационе инфраструктуре и кључних ресурса и обезбедила оквир за њихову заштиту која је есенцијална за националну безбед-

ност, економску виталност и начин живљења. Јер, ако пропустимо да препознамо потенцијалне претње и не одговоримо са довољно ресурса имаћемо озбиљне консеквенце за националну безбедност како постајемо више умрежени и више зависни од наших информационих инфраструктура.

Технологије које креирају и подржавају кибер-простор развијају се рапидно из научно-истраживачких, односно академских иновација. Због разнородног хардвера и софтвера, који представљају „грађевинске" елементе од којих је саздан интернет, разноврсних процеса и функција који се одвијају и извршавају унутар информационе инфраструктуре, великог броја учесника (корисника и практичара), великог броја потенцијалних нападача (тренутно више од милијарду и четири стотине милиона),[7] бројних могућности, метода и техника угрожавања, бројних тачака и рута напада и мноштва разнородних циљева, влада не може сама довољно добро да штити кибер-простор. Зато би решење требало тражити у партнерству владе и њених органа, индустрије и научноистраживачких и академских институција, како би у кибер-простору заједнички деловали. У препознавању тих потреба за партнерством било би неопходно произвести стратегију коју би сви потенцијални учесници могли доживети на такав начин као да они у њеној реализацији имају директну и значајну улогу коју би могли да извршавају.

Стога би процес израде националне стратегије заштите кибер-простора требало да укључи све заинтересоване. То би се, користећи сопствену памет и позитивна искуства и решења других, свакако могло остварити кроз добро организовану и исто тако осмишљену јавну расправу којом би се објединили и активирали постојећа знања и памет. Прилози и коментари добијени на тај начин свакако би допринели да се обликује једна квалитетна стратегија сажимањем њеног фокуса и изоштравањем њених приоритета. Наравно, иако би на тај начин урађена стратегија рефлектовала многе од приложених предлога, сигурно је да сви предлози не би могли бити прихваћени, као и то да се неће сви сложити са сваком компонентом националне стратегије заштите кибер-простора. Многа питања не би могла бити разрађена у детаље, а друга још нису зрела за националну политику.

Међутим, оно што је битно јесте да би стратегија дефинисана на такав начин сигурно представљала резултат интегрисаног напора заштите у јединствен национални програм за достизање прокламованог циља. Самим тим имала би подршку већине, а то је већ једна врста гаранције да ће и њена имплементација имати широку подршку. С тим у вези посебно би требало нагласити да стратегија није непроменљива. Она ће се мењати и прилагођавати променама које настају у кибер-простору изазваним првенствено променама технологије, што ће свакако утицати и на промене претњи и осетљивости наших информационих инфраструктура, али и у зависности

[7] Internet World Stats, http://www.internetworldstats.com/stats.htm

од ширења наших знања и искустава у области кибер-заштите. Дакле, национални дијалог о заштити кибер-простора требало би да се реализује.

Сагласно томе, национална стратегија заштите кибер-простора пактично би била позив за националну свест и акцију и појединаца и институција широм земље, како би се на националном нивоу повећао обим и квалитет кибер-заштите и имплементирала квалитетна решења за идентификовање и отклањање – ублажавање кибер-осетљивости наших критичних инфраструктура.

Оквир стратегије могао би да буде листа приоритета који захтевају општу добровољну партиципацију. Сваки појединачни програм састојао би се од неколико компоненти, од којих би многи проистекли из препорука и сугестија јавне расправе на нацрт стратегије. У том смислу за реализацију наведених циљева национална стратегија заштите кибер-простора требало би да артикулише критичне приоритете, међу којима би свакако требало да буду и следећи:[8]

– програм просвећивања, обуке и едукације за заштиту националног кибер-простора;

– програм редуковања претњи и осетљивости;

– национална безбедност и међународна сарадња на заштити кибер-простора.

Програм просвећивања, обуке и едукације

Чињеница која се не може превидети или негирати јесте да многе кибер-осетљивости постоје управо због недостатка свести о потреби заштите код знатног дела чланова кибер-заједнице и недостатка безбедносне културе која би промовисала информациону заштиту увелико погоршава осетљивост информационе инфраструктуре. Такве на свести базиране осетљивости презентирају озбиљне ризике за критичне инфраструктуре, чак и ако оне нису стварно њен део. Ситуација код нас, означена нивоом свести о потреби заштите кибер-простора и нивоом безбедносне кибер-културе, указује да би један од првих и најважнијих стратешких задатака свакако био континуирана, свеобухватна и веома снажна активност на подизању на знатно виши ниво свести свих субјеката, а посебно оних који одлучују, о потреби заштите кибер-простора и развијању безбедносне културе, посебно код младих и запослених у државним органима. Тек „критична маса“ те свести може да гарантује да ће већина субјеката добровољно и одговорно, без икаквог убеђивања и присиле, прихватити своје обавезе и задатке у сложеном комплексу заштите кибер-простора. То је трајан, обиман и врло сложен, али и национално веома значајан задатак који се не може обавити

[8] The National Strategy to Secure Cyberspace, op. cit.

преко ноћи. Зато је врло ризично не реаговати на време. Јер, када се проблем појави – тада је касно.

Илустрације ради, укажимо на распрострањену праксу да се државни чиновници, посебно они вишег ранга, често сликају за новине и телевизију док раде на лаптопу или стоном рачунару, што свакако представља својеврсно признање значају и улози информационе технологије. Међутим, могло би се поставити провокативно питање: да ли је програм њихове обуке коришћења рачунара садржавао бар *основе* упознавања са потенцијалним проблемима и елементарним облицима неопходне заштите, с обзиром на то да су у питању државни ресурси који по природи ствари могу поседовати и информације (документа) различитог нивоа значајности и степена тајности или је то све препуштено њиховом здравом разуму и личној сналажљивости? Или, да ли су они који из државних органа све чешће и обимније користе интернет и електронску пошту упознати са могућностима компромитације њихових порука, потенцијалним последицама такве компромитације и да ли су елементарно обучени да се заштите? И, најзад, да ли акција, која је, узгред буди речено, за сваку похвалу и која ће се у блиској будућности вишеструко исплатити, чак и материјално, што је било предмет снажних, али неоправданих критика једног дела јавности, да се свим посланицима Народне скупштине обезбеде преносиви рачунари, у којима ће се сигурно наћи мноштво података различитог нивоа значајности и степена тајности, подразумева не само обуку посланика у коришћењу рачунара, већ и у заштити његовог садржаја?

На основу досадашњег искуства могло би се рећи да је питање заштите постављено као маргиналан проблем, што ће вероватно тако и остати све док се нешто озбиљније не деси, а питање је само када, где, у ком обиму и са каквим последицама. У таквим ситуацијама мора се знати да објашњења типа „нисмо знали“ не могу служити као оправдање, јер рачунар је давно престао да буде само играчка. У међувремену, прерастао је у један веома снажан и користан, али и врло опасан алат.

То што за сада немамо великих афера са компромитацијом поверљивих информација не значи да таквих компромитација није било или да их нема. Право питање би заправо гласило да ли нам је систем заштите, у ситуацији када бројна средства информисања, као и научни и стручни радови непрекидно информишу и упозоравају на осетан пораст разних врста шпијунаже (војне, економске, политичке, ...), довољно добар да такву компромитацију благовремено спречимо, откријемо и неутралишемо. С обзиром на то да је код нас евидентан недостатак јасног ауторитета за заштиту информационих система, одговор би био негативан. Посебно у кибер-простору у којем се дигитална информација са даљина које се мере хиљадама километара и брзинама које се приближавају брзини светлости може преузети, а да и даље остане на свом месту. Ни један противник нас о томе сигурно неће самоиницијативно и добровољно обавештавати. Део негативних последица са којима се суочавамо, или

ћемо се суочавати у економији, политици, итд., објашњаваћемо и правдати вишом силом, несрећним околностима, временским неприликама, нестабилним тржиштем, недобронамерним окружењем и сл., не прихватајући да су нам, можда, у неким случајевима намере и планови унапред били компромитовани. О тим чињеницама одговорни би требало бар добро да размисле!

Национална стратегија заштите кибер-простора би, с тим у вези, требало да идентификује, поред осталог, и следеће активности, односно иницијативе за свест, обуку и едукацију:

– иницирање, поспешивање и промовисање снажног националног програма подизања свести о потреби кибер-заштите и развијања безбедносне културе, како би се комплетна популација нашег дела електронског глобалног села оспособила да штити свој сопствени део кибер-простора;

– развијање адекватних програма за обуку и едукацију, чијом реализацијом би се подржале потребе националне кибер-заштите.

Безбедносна свест и култура. Свест, како је оригинално дефинисана у НИСТ 500–172, „креира осетљивост [запослених] на претње и рањивост рачунарских система и спознају да треба штитити податке, информације и начине њихове обраде". Фундаментална вредност програма за безбедносну свест јесте да они (програми) сетују платформу за обуку доношењем промена које мењају културу организације. Културна промена је схватање и разумевање да је информациона заштита критична зато што безбедносне грешке имају потенцијално негативне консеквенце за свакога. *Дакле, информациона заштита је посао свих*.[9]

Први и најзначајнији корак у решавању проблема заштите кибер-простора, чији значај није могуће речима довољно нагласити, јесте доношење и усвајање програма изградње безбедносне свести о потребама, могућностима и значају информационе заштите и развијања безбедносне културе. Тај програм требало би да прекрије целу нацију, све појединце који на било који начин учествују или ће учествовати у информационим процесима.

Циљ програма изградње безбедносне свести и развијања безбедносне културе јесте да омогући сагледавање претњи и осетљивости информационог амбијента и потенцијалних негативних последица, да обезбеди опште разумевање проблема заштите информација и да побољша укупну свест о потреби и обавези заштите информационог простора.[10]

---

[9] *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, NIST Special Publication 800-16, http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf; Петровић Р. С., *Безбедносна свест, обука и едукација – критичне компоненте заштите кибер-простора*, *Злоупотребе информационих технологија* (*ZITEH*), Тара, 31. мај – 03. јун 2006; Wilson M., Hash J., *Building an Information Technology Security Awareness and Training Program*, NIST Special Publication 800-50, October 2003.

[10] Information Security: Raising Awareness, Version 1.0, 14 April, 2000, Treasury Board of Canada Secretariat, http://www.cio-dpi.gc.ca/ ; Information Technology Security Training Requirements, op. cit.; Петровић Р. С., *Безбедносна свест, обука и едукација – критичне компоненте заштите кибер-простора*, op. cit.;

Безбедносна свест и култура су есенцијални елементи циклуса управљања ризиком и заштитом и захтевају пажњу на свим нивоима. Безбедносна свест и култура управо подразумевају схватање и разумевање ризика. Не може се очекивати да ће се руководиоци, корисници и други који имају приступ информационим ресурсима сложити са политикама којих нису свесни или их не разумеју. Слично томе, ако нису свесни ризика повезаних са њиховим информационим ресурсима, они неће моћи да разумеју потребу за подршком политикама дизајнираним за редуковање ризика.

Значајан изазов управљања ризиком јесте чињеница да се безбедносни ризици у информационом амбијенту мењају веома брзо зато што нове осетљивости и нападачки алати континуирано бивају идентификовани. Као консеквенца те чињенице, статичан процес процене ризика није више довољан, па процес управљања ризиком у новим условима мора бити дизајниран тако да омогућава брзо реаговање. То практично значи да се у процес морају укључити елементи процене и одговора у реалном времену.

Обука и едукација. Елементарне основе информационо-безбедносне писмености (безбедносни термини, концепти, осетљивости, претње, последице) стичу се кроз подизање свести о потреби заштите, а надоградња се реализује кроз обуку, тако да би транзиција од свести ка обуци требало да се одвија осмишљено на планиран и очекиван начин. Реализација програма изградње безбедносне свести о потреби заштите информационог амбијента на знатно виши ниво од тренутног јесте основни предуслов за обуку из области заштите кибер-простора.[11]

Уколико се жели остварити квалитетан систем заштите значајну пажњу свакако треба посветити обуци корисника из домена политике, процедура и техника заштите, као и управљачких, оперативних и техничких контрола потребних и расположивих за заштиту информационих ресурса. Предуслов и прелазна активност за обуку из информационе заштите требало би да подразумева програм подизања безбедносне свести на највиши могући ниво.

Едукација је јасно идентификована као сепаратни ниво учења намењен професионалцима и специјалистима за заштиту. Обезбеђивање формалне едукације и специфичних критеријума едукационог нивоа за ту групу у надлежности је програма које би требало да реализују академске установе. Сматра се да су едукација, која се разликује од обуке, и искуство повезано са послом, есенцијални за професионалце и специјалисте информационе заштите да би били у стању да одиграју своје улоге на ефикасан начин.[12]

[11] Information Technology Security Training Requirements ... , op. cit.; Петровић Р. С., *Безбедносна свест, обука и едукација – критичне компоненте заштите кибер-простора*, op. cit.; Wilson M., Hash J., op. cit.; Information Security: Raising Awareness, op. cit.

[12] Information Technology Security Training Requirements ... , op. cit.; Петровић Р. С., *Безбедносна свест, обука и едукација – критичне компоненте заштите кибер-простора*, op. cit.; Wilson M., Hash J., op. cit..

Свакако, треба указати на охрабрујућу и поштовања вредну активност Министарства просвете да се у свим школама у Србији уведу рачунари. Следећи корак био би да се дефинишу адекватни програмски садржаји у којима би заштита требало да заузима значајно место. Биће то инвестиција која ће се нацији вишеструко исплатити.

Програм редуковања претњи и осетљивости

Државни органи на свим нивоима извршавају есенцијалне сервисе који се ослањају, или ће се врло брзо ослањати, на сваки од сектора критичне инфраструктуре, као што су, примера ради, пољопривреда, транспорт, водоснабдевање, здравствена заштита, ванредне ситуације, телекомуникације, енергија, банкарство и финансије, хемијски и опасни материјали, поштански саобраћај... Из тих разлога произилази недвосмислена потреба поузданости функционисања критичне инфраструктуре и ничим неометаног извршавања есенцијалних сервиса.

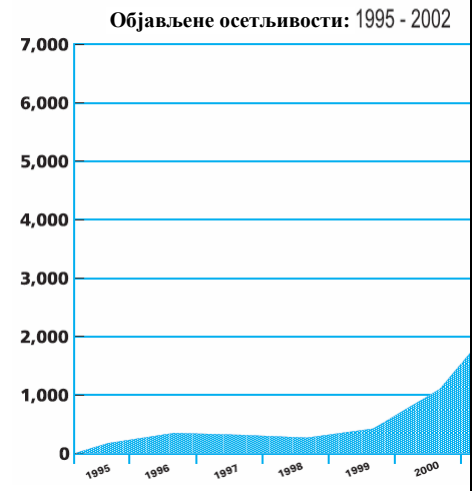
Ту потребу, без обзира на то колико је значајна, није лако задовољити. Основни разлог је у чињеници да критичну инфраструктуру карактерише висок степен осетљивости која знатно отежава задовољење наведене потребе. Та осетљивост резултира из слабости у технологији, нерегуларне имплементације, пропуста технолошких производа, оскудне безбедносне контроле и одсуства ефективног надзора. Досадашња искуства су потврдила да експлоатисањем осетљивости кибер-система, организовани злонамерни напади могу довести у озбиљну опасност безбедност националне критичне инфраструктуре. Осетљивости које могу наговестити опасности у кибер-простору, у најкраћем, јављају се у информационим добрима корисника информационе инфраструктуре, њиховим екстерним структурама за подршку, као што су механизми интернета и незаштићени сајтови на интернету.

С друге стране, претње које угрожавају информациону инфраструктуру, генерално посматрано, могу да потичу из четири различита извора, а то су: рачунарски криминал, кибер-тероризам, обавештајно деловање и информационо ратовање.[13] Носиоци тих претњи у кибер-простору могу узимати различите форме, укључујући појединце, групе, криминалне картеле, терористе, стране обавештајне службе и националне државе. Сви они ће у нападу покушавати да експлоатишу слабости креиране дизајном или имплемента-

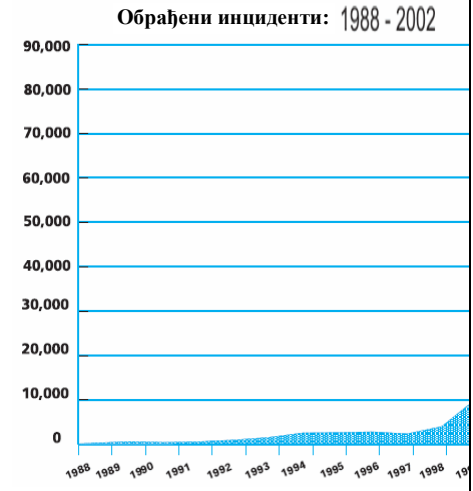
[13] C. Bryan Foltz, *Cyberterrorism, computer crime, and reality*, Information Management & Computer Security, 2004, Volume: 12, Issue: 2, Page: 154 – 166; Петровић Р. С., *КОМПЈУТЕРСКИ КРИМИНАЛ*, Војноиздавачки завод, Београд, 2004, III издање, стр. 393-442; Петровић Р. С., *Кибер-простор – пета димензија ратовања*, Војни информатор, бр. 4, јул-август 2001, стр. 29–50.

цијом софтвера, хардвера, мрежа и протокола да би постигли широк опсег политичких или економских ефеката. На слици 1 графички је приказан пораст објављених осетљивости за период 1995–2002.[14]

И најзад, како се ослањање легалних корисника на кибер-простор буде повећавало, тако ће се, такође, увећавати и број инцидената и опсег штете коју злонамерни актери могу остварити. Исто тако, даљи развој технологије и укључивање нових система имаће за последицу настанак и нових до тада непознатих осетљивости. Слика 2 графички приказује пораст обрађених инцидената за период 1988–2002.[15]



Слика 1



Слика 2

Због свега тога неопходно је да бар оне најризичније осетљивости буду редуковане и то на систематичан начин. То управо значи да стратегија не би требало да подразумева елиминацију свих осетљивости или спречавање свих претњи, већ да буде заснована на управљању ризиком у оквиру чега би се деловање усмерило на реализацију програма којим би се вршило:

– редуковање претњи и одвраћање злонамерних актера кроз ефикасан програм њихове идентификације и кажњавања;

– идентификовање и елиминисање оних постојећих осетљивости које би могле креирати највећу опасност за критичне системе, ако би биле експлоатисане.

[14] The National Strategy to Secure Cyberspace, op. cit.

[15] The National Strategy to Secure Cyberspace, op. cit.

Сходно томе, национална стратегија заштите кибер-простора требало би да идентификује главне активности и иницијативе за редуковање претњи и повезаних осетљивости, међу којима би своје место свакако требало да нађу и следеће:[16]

– оспособљавање државних органа за откривање напада и гоњење нападача у кибер-простору;

– непрекидна процена претњи и осетљивости националних кибер-система.

Већина кибер-напада представља криминал, тероризам, шпијунажу и/или информациону агресију.[17] Као резултат те чињенице кључну улогу у откривању извршилаца, спречавању њиховог деловања и њиховом брзом извођењу пред лице правде морали би да имају државни органи, а пре свих правосудни органи, криминалистичке службе и безбедносне агенције. При томе, неопходно би било остварити продуктивно партнерство између тих органа, које у највећој мери зависи од ефикасне сарадње и међусобне комуникације. Амерички приступ у том случају заслужује пажњу. Да би олакшали и ојачали ту сарадничку структуру они су означили „водећу агенцију" за сваки од главних сектора економије осетљивих на нападе на инфраструктуру. Тако је, поред осталих, *CIA* постала одговорна за процену спољних претњи америчким мрежама и информационим системима, док су министарство правде и *FBI* задужени да воде истрагу и судски гоне извршиоце кибер-криминала.

С обзиром на то да ће се и технологије и претње константно рапидно мењати задужени органи би морали често процењивати поузданост, рањивост и претње амбијентима националне инфраструктуре и користити одговарајуће мере и акције да их заштите. Зато је потребно делове тих служби оспособити и део њихових активности и обавеза преусмерити ка кибер-простору. То је много лакше констатовати него реализовати. Али, не смемо сметнути са ума да је реч о националном интересу, а он је изнад свих других интереса. Једно од свакако најприхватљивијих решења, према светском искуству, јесте да се у свим тим службама (правосудним, криминалистичким и безбедносним) формирају посебне јединице којима би превасходни задатак био заштита националног кибер-простора и спречавање његове злоупотребе. Јединице би чинили професионалци којима би морали да се обезбеде услови за непрекидно истраживање и стручно усавршавање, као и сви потребни ресурси неопходни за њихово непрекидно и несметано функционисање.

---

[16] Петровић Р. С., *КОМПЈУТЕРСКИ КРИМИНАЛ*, op. cit. стр. 443–450; The National Strategy to Secure Cyberspace, op. cit.

[17] Петровић Р. С., *Кибер-простор – пета димензија ратовања*, op. cit, стр. 29-50; Петровић Р. С., *Неки аспекти националне безбедности у информационом добу*, Наука, Техника, Безбедност, (НТБ), Рад по позиву, UDC: 681.324; 65.012.8, година XI, број 1, септембар 2001, стр. 7–27.

Чињеница је да су те службе тренутно у великој мери лимитиране својим раније дефинисаним мисијама, што свакако представља велику сметњу за њихово пуно укључивање у једну тако значајну националну акцију. Ако се томе дода још и извесност да ће то укључивање од неких, због свих специфичности које карактеришу информациону технологију, захтевати обимну промену традиционалних образаца рада и рефокусирање активности и ресурса (значајна преквалификација оних који прикупљају податке – колектори и оних који обрађују прикупљене податке – аналитичари) на ову значајну област, онда се може очекивати да то укључивање неће ићи ни брзо ни лако. Јер, познато је да су државни органи по својој бирократској природи врло инертни и не баш склони великим и брзим променама. Код многих је на снази златно правило: *Само да се не таласа*. Међутим, морамо бити свесни да информациона технологија драстично и драматично мења начине рада и живљења буквално свих (а то значи и пуно „таласања"), што намеће императивну обавезу онима који желе да опстану у новим условима да морају да им се прилагоде. Зато укључивање појединих органа у значајну националну акцију заштите кибер-простора, која је иначе трајног карактера, не би смело да се доводи у питање. Они који то буду чинили морају бити свесни сопствене одговорности, јер таквим ставом врло озбиљно доводе у питање једну значајну компоненту националне безбедности.

Илустрације ради, поменимо да су од Другог светског рата основна брига контра-обавештајне заједнице биле хладноратовске претње од шпијуна и издајника који су фотографисали класификована документа или крали поверљиве информације. Агенти су трагали за физичким уређајима за прислушкивање који су постављани по кућама и канцеларијама. Без сумње, физичка заштита била је значајна брига заједнице и имала је приоритет. У поређењу тадашње са садашњом ситуацијом у кибер-простору може се констатовати постојање одређене сличности, али и великих разлика. И сада, као и тада, краду се класификована документа и поверљиве информације. Разлика је само у обиму и брзини реализације, уз садашњи висок степен анонимности и уз могућност да се све то ради даљински са било ког места. Раније се знало од кога претње долазе и којим путем нападач може да приспе, па су се мере заштите често предузимале и на самој граници. Нажалост, информациона технологија је у кибер-простору у потпуности укинула физичке границе и многи напади, уколико се уоче, остају мистерија све док се до детаља не испитају, а тада је најчешће и сувише касно.

И криминалистичке службе из сличних разлога нису биле у могућности да обезбеде поуздану процену претњи и адекватно одговоре на напад.

Међутим, без обзира на све то, једно је сигурно: последњих година претње у кибер-простору су се увећале и изнад најпесимистичкијих очекивања, због чега је потреба да службе безбедности дају процену претњи заиста велика. Немогуће је спроводити садржајно управљање сложеним ризиком без поузданих података о потенцијалним претњама и нивоу и обиму могућег

угрожавања. Како субјекти који се штите да одреде ниво ресурса потребних за реализацију заштите кибер-простора без познавања димензија претњи и потенцијалних последица? Технологија упада у рачунарске мреже се рапидно мења. Уколико се не зна које методе и технике нападачи тренутно користе, како да се обезбеде и имплементирају контрамере? Коначно, зато што се многе од претњи повезују са компромитацијом осетљивих података и информација, тешко је, изостављањем значајних процена претњи, одредити каква је штета учињена. Јер, нација у амбијенту кибер-простора, поред осталог, може *губити информациону и економску предност а да се то и не зна*.[18] То је чињеница над којом морамо да се замислимо.

Управо због тога, а имајући у виду сложеност и значај процене претњи националним интересима у кибер-простору и заштити тог простора, влада би морала да у оквиру националне стратегије заштите кибер-простора дефинише улогу и одговорност државних ентитета, а посебно правосудних органа, криминалистичких и безбедносних служби. На тај начин њихово деловање у кибер-простору постало би легитимна мисија – мисија која израста и постаје увећано значајна.

Након усвајања стратегије министарства и агенције би имале задатак превођења препорука стратегије у акцију. На тај начин, са високим степеном вероватноће могло би се сматрати да ће нација бити у стању да спречи, одврати и значајно редукује кибер-нападе који би евентуално могли угрозити националне интересе.

Национална безбедност и међународна сарадња у заштити кибер-простора

Кибер-простор обједињава све државе света у једно јединствено електронско глобално село у којем не постоје физичке границе, гранична полиција, царина, ... У том обједињеном виртуелном простору злонамерним актерима је омогућено да делују на системе удаљене хиљадама километара и брзинама које су непојмљиве обичном човеку. Далекометност, брзина и врло висок степен анонимности кибер-напада чини распознавање у реалном времену злонамерних активности чији су носиоци криминалци, терористи, стране обавештајне службе или националне државе – агресори заиста врло тешким.[19] Те чињенице намећу обавезу да се дефинишу критичне мреже и да се изврше припреме које би омогућиле да се у сваком од тих случајева одговори на напад. Нација мора бити у стању да заштити и одбрани своје критичне системе и мреже – независно одакле и од кога напад потиче.

[18] Security in cyberspace, op. cit.

[19] Петровић Р. С., *О информационој револуцији у контексту злоупотребе информационих технологија*, Злоупотреба информационих технологија (*ZITEH*), Зборник радова (CD-ROM), јун 2004; The National Strategy to Secure Cyberspace, op. cit.; Copeland E. T, *The Information Revolution and National Security*, op. cit.

Криминалистичка служба и безбедносне агенције морале би организовати снажну контраобавештајну заштиту да спрече кибер-базиране терористичке нападе, обавештајно прикупљање информација на основу којих би се могли угрожавати национални интереси или информациону агресију непријатељски настројених држава. Тај напор мора укључити дубље разумевање могућности и намера противника да користи кибер-простор као начин за шпијунажу и информациону агресију.

Америчке званичне процене још давне 1996. године указивале су да више од 120 земаља развија могућности офанзивног информационог ратовања.[20] Агенција за националну безбедност (*NSA*) оценила је тада да потенцијални противници широм света развијају масовни фонд знања и овладавају методама и техникама напада који укључују софистициране рачунарске вирусе и аутоматизоване нападачке рутине који омогућавају противнику да лансира неутврдљиве нападе са било ког места у свету према било коме у свету, бирајући путање из мноштва расположивих. Сигурно је да се до данас ситуација у том смислу само заоштрила. Имајући при томе у виду и чињеницу да ће рањивост информационих структура у том погледу само да се увећава и према текућој стопи контрамере неће никада ићи у корак са технологијом, јасно је колико је разматрани проблем значајан, озбиљан и врло актуелан.

Због свега тога укључивање служби безбедности морало би увећати националну могућност за брзо откривање извора опасних напада или акција како би се омогућио благовремен и ефикасан одговор. То ће захтевати снажну координацију и кооперацију између служби које ће бити укључене у кибер-базиране нападе, посебно што је за ту врсту напада често тешко одредити да ли је у питању страни или домаћи извор напада.

С обзиром на то да је заштита кибер-простора проблем глобалног карактера који не дотиче само нас, већ све земље света, наша је обавеза, пре свега због сопствених интереса, да се укључимо у напоре међународне заједнице у заштити глобалног кибер-простора, а самим тим и оног дела који припада нама. Ради тога морали би да усавршимо наше могућности и да делујемо у складу са захтевима међународне кооперације ради дељења информација, редуковања осетљивости и одвраћања злонамерних нападача.

Национални центар за заштиту

Базирано на мултидимензионалној природи кибер-претњи које су усмерене ка информационој инфраструктури, туђа искуства и наше процене указују на потребу успостављања једног ентитета који би могао спроводити и управљати оперативним реакцијама на кибер-нападе. Тај ентитет, са називом *Национални*

[20] Security in cyberspace, op. cit.

центар (орган, тело, комисија), укључивао би представнике криминалистичке, обавештајне и војне заједнице, као и спону са приватним сектором. Са конкретним *обавезама* и *овлашћењима* центар би на националном нивоу управљао заштитом кибер-простора и инцидентима који би могли имати утицаја на националне интересе и био би носилац свих кључних активности на плану заштите кибер-простора. Директно би био везан за владу са обавезом редовног периодичног извештавања владе о стању у тој области. На тај начин обезбедила би се *планирана, контролисана и синхронизована* реализација постављених циљева. Предуслови за успешан рад тог центра били би стручни кадрови, неопходни ресурси и 24-часовне оперативне могућности у реалном времену.

Национални центар за заштиту кибер-простора био би одговоран за многе иницијативе наведене у стратегији. То би, свакако, требало да укључи:

– развој садржајног националног плана за заштиту кључних ресурса и критичне инфраструктуре сагласан потребама и могућностима;

– предвиђање управљања кризама у одговору на нападе на критичне информационе инфраструктуре и кључне ресурсе;

– обезбеђивање тактичке и стратешке анализе процењених кибер-напада и осетљивости;

– побољшавање управљања националним инцидентима;

– обезбеђивање техничке помоћи приватном сектору и државним ентитетима с обзиром на потребу планова обнове-опоравка због отказа критичних информационих система;

– координирање са безбедносним агенцијама да би се обезбедиле специфичне упозоравајуће информације и савети о одговарајућим заштитним мерама и контрамерама држави, локалним и невладиним организацијама укључујући приватни, академски и јавни сектор;

– иницирање, извршавање и финансирање истраживања и развоја, што би требало да води до нових научних сазнања и технологија у подршци националној безбедности.

Сагласно тим задацима и одговорностима национални центар имао би и *координирајућу* и *контролну* функцију и представљао би средишњу тачку кибер-заштите из које би кључне мере и акције могле да досегну до свих државних, локалних и невладиних организација, укључујући приватни и јавни сектор и академску средину. Оно што у разматраном контексту нарочито треба нагласити јесте потреба да све процене и анализе које буде радио национални центар имају и своју некласификовану верзију, како би могла бити стављена на располагање невладиним ентитетима, што би им у знатној мери олакшало напоре у заштити кибер-простора.

И, најзад, због обавеза које имамо према међународној заједници, чији смо и сами део, тај национални центар имао би задатак да остварује непосредну међународну сарадњу у тој области и то по свим аспектима који су битни за успешно супротстављање угрожавању глобалног, па самим тим и националног кибер-простора.

Закључак

Мада је раст примене информационе технологије драматичан, већина експерата се слаже да је то само почетак њеног настављања и зависности о њој.[21] Може се показати да нема лимита на потенцијалну експанзију мрежа и корисника. Све то осетно увећава рањивост критичне инфраструктуре и институција које она подржава, па самим тим и цела друштвена заједница постаје знатно осетљивија на све врсте поремећаја.[22]

Међутим, ником није циљ да се због опасности одриче повољних могућности, већ да те могућности максимално, али осмишљено и контролисано, експлоатише ради сопствене добробити. Управо због тога технолошке иновације ће наметати императивну потребу адаптирања новим условима, правилима, могућностима и препрекама. При томе се мора бити свестан да промене нуде прилику, али да носе и врло велики ризик.

Тај ризик претпоставља да би кибер-напади доводили у опасност интелектуална, материјална и финансијска добра, пословне операције, инфраструктурне сервисе, поверење потрошача, јавни морал грађана и много тога другог. Поремећаји који би настали због изазваних проблема са националном информационом инфраструктуром за последицу би могли, поред осталог, имати потребу да се функционисање државних органа, али и других значајних ентитета, бар у неким сегментима, врати на стари – превазиђен систем рада. То би код грађана сигурно изазвало висок степен неразумевања, неспокојства, па и незадовољства, а то свака одговорна власт жели да избегне.

Зато, заштита критичне националне инфраструктуре и кључних ресурса, иако је изузетно сложен и тежак проблем за решавање, не само због обима инфраструктуре, претњи различите природе и мноштва извора претњи, већ и зато што јавност генерално мало разуме њихове импликације, мора имати врло висок национални приоритет.

При томе не би требало да понављамо грешку других. У многим развијеним земљама запада у протеклом времену приватни сектор, укључујући комерцијални и финансијски свет, није био вољан да објављује своје сопствене осетљивости због бојазни да инспиришу несигурност клијената. Као резултат појавили су се енормни губици који су избегли пажњи криминалистичке полиције и обавештајних заједница.[23] Слично је било и код државних институција, али је разлог био другачији. Они једноставно нису имали оба-

[21] Петровић Р. С., *КОМПЈУТЕРСКИ КРИМИНАЛ*, op. cit, стр. 443-444; Security in cyberspace, op. cit.

[22] Hundley O. R., Anderson H. R., Bikson K. T., Neu C. R.: *The Global Course of the Information Revolution*, RAND, 2003, http://www.rand.org/publications/MR/MR1680/; Copeland E. T, *The Information Revolution and National Security*, op. cit.

[23] Security in cyberspace, op. cit.

везу да пријављују упаде у информационе системе, а већина њих није ни имала искуства, стручности и алата да детектује упаде или покушаје упада.

Тренутно, свака нација има законе и друге механизме да обезбеди одговор на велике инциденте. Ти одговори углавном подразумевају истрагу, хапшење и кажњавање. Редукција претњи, међутим, укључује много више од кажњавања. Прикупљање, анализирање и дисеминација прикупљених практичних информација често може ублажити штету изазвану злонамерним активностима у кибер-простору и значајно помоћи подстицању заштите националне инфрастраструктуре. Да би те активности биле ефикасне на националном нивоу неопходно је вршити анализе, издавати упозорења и координирати напоре реаговања – одзива.

Како је једна од најзначајнијих празнина у информационој заштити недостатак извештавања о покушајима или успешним упадима у системе од националног интереса, мандатно извештавање о таквим догађајима подстицајно би деловало на ширење безбедносне културе и свести о потреби заштите кибер-простора. Због тога се препоручује да се влада обавеже да ће извештавати о упадима и покушајима упада у све њене системе и системе који су јој важни.

Такође, правосуђе и криминалистичка служба у оквиру својих активности на заштити кибер-простора морали би да информације прикупљене у истрагама конкретних случајева адекватно анализирају и деле са другим невладиним ентитетима како би промовисали побољшање управљања ризиком у критичним инфраструктурним секторима. Информације прикупљене у истрази могу представљати поуке из којих се много тога може научити.

Проблема ће свакако бити и у придобијању државних службеника за нови систем рада који ће се одвијати у за њих сасвим новом амбијенту. Наиме, наши државни службеници навикли су на заштиту у физичком свету у којем се класификовани подаци одржавају на заштићеним локацијама са физичким баријерама (врата, зидови, стража, разне врсте детектора, интерна телевизија, ...), које служе као обезбеђење губљења података. Штавише, особе које имају приступ у зграду немају приступ до извесних (рестриктивних) простора, докумената, заштићених картотека. Само поверљиве особе имају приступ до ових зона и информација. Смештањем података на рачунаре умрежене у кибер-простору та врста заштите јесте потребна, али не и довољна. Чак, у неким сегментима, поједини облици физичко-техничке заштите постали су примитивни у новим условима. Умрежавање рачунарских система креирало је нове осетљивости давањем широког мрежног приступа рестриктивним подацима. И, како каже један обавештајни официр:[24] *„свако на мрежи, од чиновника до момка на другој страни зграде може прегледати критичне информације, а да нико о томе не зна ништа“*.

[24] Security in cyberspace, op. cit.

Због свега тога предстоји врло озбиљан и дуготрајан рад са државним службеницима у смислу развијања информационе безбедносне културе и подизања свести о потреби заштите информационог амбијента, као и обуке и едукације у реализацији адекватног система заштите.

Најзад, одговорност за заштиту у државним органима морала би бити персонализована. Питање је колико наших државних органа, који су у мањој или већој мери већ изградили информациони систем, има систематизована и попуњена радна места за заштиту информационих система или је тај задатак додатна обавеза неком од извршилаца других послова. Дакле, јасно је да се последично занемарује непобитна чињеница да је заштита и превише озбиљан, сложен и значајан проблем да би се могао успешно решавати парцијално, с времена на време и узгред.

На крају, може се констатовати да ће се наша земља све мање бранити на граничним прелазима, а све више у кибер-простору који се и код нас неумитно шири. Управо због тога држава **МОРА** да се припреми да предузимањем свих расположивих мера и акција успешно одговори на све изазове, осујећујући сваки покушај угрожавања националног кибер-простора без обзира на то одакле и од кога потиче.

Литература

1. Anderson K, *Computers and the Information Revolution*, Updated 2002 Probe Ministries, http://www.leaderu. com/orgs/probe/docs/computer. html

2. Bologna S., Luiijf E., Setola R., *R&D activities in Europe on critical information infrastructure protection*, Copyright © 2008 Inderscience Enterprises Ltd.. Int. J. System of Systems Engineering, Vol. 1, Nos. 1/2, 2008, 257–270.

3. C. Bryan Foltz, *Cyberterrorism, computer crime, and reality*, Information Management & Computer Security, 2004, Volume: 12, Issue: 2, Page: 154–166, http://www.emeraldinsight. com/10.1108/09685220410530799

4. Common Risks Impeding the Adequate Protection of Government Information, The Identity Theft Task Force, July 2007, http://csrc. nist. gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info. pdf

5. Copeland E. T, *The Information Revolution and National Security*, Strategic Studies Institute of the US Army War College, August 2000, http://www.strategicstudiesinstitute. army.mil/pdffiles/pub225.pdf

6. Critical Infrastructure Protection – Challenges in Addressing Cybersecurity, United States Government Accountability Office (GAO), 2005, http://www.globalsecurity.org/security/library/report/gao/d05827t. pdf

7. G8 Principles for Protecting Critical Information Infrastructures, Adopted by the G8 Justice & Interior Ministers, May 2003, http://www.usdoj. gov/criminal/cybercrime/g82004/G8_CIIP_Principles. pdf

8. Gheorghe V. A., Masera M., Weijnen P. C M., *Critical Infrastructures at Risk – Securing the European Electric Power System*, Published by Springer, The Netherlands, 2006, pp 153.

9. Gorge M., *Cyberterrorism: hype or reality?*, Computer Fraud & Security, February 2007, pp 9–12.

10. Hundley O. R., Anderson H. R., Bikson K. T., Neu C. R.: *The Global Course of the Information Revolution*, RAND, 2003, http://www.rand. org/publications/MR/MR1680/

11. Information Security: Raising Awareness, Version 1.0, 14 April, 2000, Treasury Board of Canada Secretariat, http://www.cio-dpi. gc. ca/

12. Information Technology Security Training Requirements: A Role- and Performance-Based Model, NIST Special Publication 800–16, http://csrc. nist. gov/publications/nistpubs/800–16/800–16.pdf.

13. Internet Advertising Maintains Growth in 2005, ClickZ News, April 20, 2006, http://www.clickz. com/news/print. php/3600536

14. Internet Growth Statistics - Global Village History, http://www.internetworldstats. com/emarketing. htm

15. Internet World Stats, http://www.internetworldstats. com/europa1.htm

16. Jones A., *Cyber Terrorism: Fact or fiction*, Computer Fraud & Security, June 2005, pp 4–7.

17. Macaulay T., *Critical Infrastructure : understanding its component parts, vulnerabilities, operating risks, and interdependencies*, CRC Press – Taylor & Francis Group, 2008, pp 337.

18. Marshall McLuhan Foresees The Global Village, http://www.livinginternet. com/i/ii_mcluhan. htm

19. Metz S, *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare*, Strategic Studies Institute of the US Army War College, March 2000, http://www.strategicstudiesinstitute. army.mil/pubs/display.cfm? PubID=226

20. National Infrastructure Protection Plan, US Department of Homeland Security, 2006, www.dhs. gov/nipp

21. National strategy for homeland security, Office of Homeland Security, july 2002, http://www.whitehouse. gov/homeland/book/nat_strat_hls. pdf

22. Nelson K. N., *„Applying the Principles of War in Information Operations“*, http://www-cgsc. army.mil/milrev/English/SepNov98/nelson. htm

23. Papa M., Shenoi S., *Critical Infrastructure Protection II*, International Federation for Information Processing, Springer Series in Computer Science, 2008, pp 275.

24. Personick D. S., Patterson A. C., *Critical Information Infrastructure Protection and the Law: An Overview of Key Issues*, Committee on Critical Information Infrastructure Protection and the Law, National Research Council, 2003, pp 104.

25. Peters T., *What Is It Worth to Understand Culture?* Times - July 2007, http://archives. subscribermail. com/msg/2ce280e4ebcd4f9c9c2f87e96237120b. htm

26. Петровић Р. С., *Безбедносна свест, обука и едукација – критичне компоненте заштите кибер-простора*, Саветовање *Злоупотребе информационих технологија* (*ZITEH*), Зборник радова (CD-ROM), ISBN 86–909511–0-5, COBISS SR-ID 135535372, Тара, 31. мај – 03. јуни 2006.

27. Петровић Р. С*., Кибер-простор – извориште нових претњи националној безбедности,* Међународни научно-стручни скуп Информациона безбедност 2009, Београд, фебруара 2009.

28. Петровић Р. С., *Кибер простор – пета димензија ратовања*, Војни информатор, бр. 4, јул-август 2001, стр. 29–50.

29. Петровић Р. С*., Кибертероризам*, Војно дело, год. LIII, бр. 2/2001, стр. 100–122.

30. Петровић Р. С., *КОМПЈУТЕРСКИ КРИМИНАЛ*, Војноиздавачки завод, Београд, 2004, 564 ст. III издање

31. Петровић Р. С*., Национална безбедност у раљама информационе технологије, Инфо м, Факултет организационих наука, Београд, год 8, св. 30, 2009.*

32. Петровић Р. С., *Неки аспекти националне безбедности у информационом добу*, Наука, Техника, Безбедност, (НТБ), Рад по позиву, UDC: 681.324; 65.012.8, Година XI, Број 1, Септембар 2001, стр. 7–27.

33. Петровић Р. С., *О информационој револуцији у контексту злоупотребе информационе технологије*, Саветовање Злоупотребе информационих технологија (*ZITEH*), Зборник радова (CD-ROM), Тара, 31. мај – 03. јуни 2004.

34. Петровић Р. С*., О неопходности националне стратегије заштите кибер-простора*, Наука Техника Безбедност (НТБ), Београд, вол. XI, но. 2, 2006, стр. 3–28.

35. Security in cyberspace, Staff statement, U. S. Senate, Permanent subcommittee on investigations, june 5, 1996, http://www.fas. org/irp/congress/1996_hr/s960605t. htm

36. Strackbein R, *Explore the Future*, 2001, http://www.strackbein. com/html/articles. html

37. Strackbein R, *Survive the Transition: Industrial Age to Information Age*, 2001, http://www.strackbein. com/html/articles. html

38. The National Strategy to Secure Cyberspace, The White House Washington, february 2003, http://www.whitehouse. gov/pcipb/cyberspace_strategy.pdf

39. White P. J, Deutch J, *Building capability from the technical revolution that has happened*, Strategic Studies Institute of the US Army War College, Report of the Belfer Center Conference on National Security Transformation. June 2004, http://www.carlisle. army.mil/ssi

40. Wilson M., Hash J., *Building an Information Technology Security Awareness and Training Program*, NIST Special Publication 800–50, October 2003.