

КОРЕЛАЦИЈА ИНФОРМАЦИОНЕ И НАЦИОНАЛНЕ БЕЗБЕДНОСТИ

Доц. др Саша Мијалковић
Криминалистичко-полицијска академија, Београд
(sasa.mijalkovic@kpa.edu.rs)

Доц. др Вера Арежина-Ћерић
Академија за дипломатију и безбедност, Београд
(vera.a@verat.net)

Доц. др Горан Бошковић
Криминалистичко-полицијска академија, Београд
(goran.boskovic@kpa.edu.rs)

Абстракт: Савремена концепција националне безбедности захтева и концепцијску употребу дигитализованог знања у достизању, заштити и унапређењу виталних националних вредности и интереса. Без обзира да ли се у томе ослању на (могућу) употребу политичких, економских, војних или информационих елемената националне моћи, државе ће бити ефикасније уколико успоставе контролу над мрежним чворовима међународних комуникација и над ресурсима у виду вредних информација. С обзиром на информациону глобалну међузависност, државе ће тежити да буду примарне архитекте и посредници у информационим мрежним операцијама, чиме ће осигурати своју безбедност. Стога и национални информациони ресурси постају витална национална вредност, а безбедност и интегритет кибер-простора, тј. *информациона безбедност*, постаје један од виталних националних интереса.

Кључне речи: информациона безбедност, моћ државе, кибер-простор, национална безбедност.

УВОД

Безбедност је једна од основних људских потреба.¹ Генерално, безбедност постоји када постоји и несметано се испољава (достиге се, развија и унапређује, може да се ужива) оно што је (за нас) вредно и значајно, и када је такво стање очигледно извесно, предвидиво и контролисано, што подразумева и (нашу) способност да га заштитимо од нежељених утицаја. То је процес, а пре свега (жељени) производ тог процеса – стање. Бити безбедан значи бити заштићен од утицаја нежељених појава, и осећати се заштићеним (сигурним, без страха) у предвидивом и контролисаном амбијенту.

¹ Као непобитна гаранција опстанка, напретка и благостања, те слободног живота без страха или тешкоћа, безбедност је универзално добро и супстрат културе савременог човечанства. Burke, A.: *Apogies of Security, Alternatives: Global, Local, Political*, Vol. 27, No. 1, 2002, p. 1.

Очигледно је да се у фокусу безбедности налазе извесне вредности, као идеална својства одређених предмета, друштвених појава, процеса и садржаја свести које им људи (појединачно и колективно) придају, а које их чини пожељним јер им омогућавају задовољење потреба, побољшавају живот, односно уживају у њима.

Вредности појединца су несметано задовољење основних животних и биолошких потреба, обезбеђења услова и средстава за живот, неприкосновеност менталног и физичког интегритета, достојанства и личне имовине, те слободно испољавање воље, духа и самоафирмације. Неретко се исказују кроз концепт људских права. *Вредности колектива (група)* су бројне (језик, култура, идеологија, традиција, верска, расна, етничка припадност итд.). Због специфичности и бројности, збирно се називају *индетитетом*.

Националне (државне и друштвене) вредности су: опстанак државе и нације; квалитет живљења становништва и социјално благостање; уставни и правни поредак; јавни поредак, ред и мир; економски просперитет, енергетска стабилност; информациони ресурси; политичка стабилност и национално јединство; територијални интегритет; суверенитет; национални понос и достојанство; здрава животна средина;² национални идентитет и друге.

Међународне вредности су својствене међународном систему. То су међународни мир и безбедност; међународно пријатељство, помоћ и сарадња; међудржавна и међунационална толеранција и уважавање; међународно право, стандарди и принципи; међународна правда; међународни поредак и друге.

Најзад, као *глобалне (човечанске, планетарне) вредности*, поред наведених, могу да се издвоје још и: опстанак људске врсте; демографска стабилност, подмлађивање, квалитет живота и здравље светског становништва; здрава животна средина и нови-обновљиви извори енергије; безбедност космичког пространства; стабилна и прогресивна светска привреда; контролисаност ширења оружја за масовно уништавање; глобална безбедносна култура и етика и друге.

Осим што представља јединствен концепт, национална безбедност је садржалац и чувар свих наведених вредности, односно „раскрсница свих концепата безбедности“. Конкретније, национална безбедност обухвата *заштиту и заштићеност националних вредности од свеколиког (војног и невојног, унутрашњег и спољног) угрожавања, као и партиципације државе и друштва у сферама међународне и глобалне безбедности*.

Очигледан је значај и утицај информационе технологије на све наведене сфере савременог живота, а тиме и на поменуте нивое (појединачне, друштвене, националне, међународне и глобалне) безбедности. Суочавајући појединце, друштва, нације, државе и међународну заједницу са изазовима адаптирања, иновирања и реаговања на прилике и могућности које им се указују, информациона технологија врши неумитну трансформацију (*информациона револуција*) из индустријског у информатичко друштво, најављујући нову дигиталну еру. „Све што се ради – аутоматизује се, све што вреди – дигитализује се“. Готово сва догађања укључиваће коришћење рачунара, а најразноврсније друштвене вредности, у опсегу од минорних до виталних, трансформисаће се у тзв. *кибер-добра*. Улога и значај информационих система у раду савремене државне управе (*e-government*), пословања, здравства, научно-образовног рада, система националне безбедности и одбране

² Упореди – Арџина Вера, „Еколошка безбедност – основа међунационалних безбедности“, Криминалистичке теме – часопис за криминалистику, криминологију и сигурносне студије, Сарајево, 2008.

су неспорни и пресудни. Истовремено, повећана је њихова рањивост од разних појава које теже њиховој деструкцији. Стога је неспорно да су национални информациони ресурси у функцији осталих друштвених вредности, али и да су сами постали вредност савременог друштва.³

Због свог значаја, национални информациони ресурси се у савременој теорији националне безбедности с правом сматрају једном од виталних националних вредности, а њихово одржање и развој једном од примарних националних интереса.⁴ Ово стога што је савремено друштво све више „дигитализовано и аутоматизовано“, па и достизање, заштита, одржање и развој осталих вредности друштва све више зависе од информационих ресурса и степена њиховог развоја и заштићености.

Стратешким вредностима морала би да се пружи и стратешка заштита. То би се најадекватније постигло конципирањем и реализовањем извесне *националне стратегије информационе безбедности*, која би била интегрална компонента *стратегије националне безбедности*, као и институционализацијом извесног подсистема националне безбедности који би, по принципима специјализације и професионализације, био надлежан за њено спровођење.

Национални информациони ресурси као витална национална вредност

Национални информациони ресурси обухватају тоталитет информационог знања (о савременим информационим технологијама и њиховој употреби, као и дигитализовано знање из других сфера друштвене делатности и свести), информационе материјално-техничке капацитете и инфраструктуру у поседу нације, као и њихово партиципирање у глобалним информационим процесима и односима. Конституенс су *националне информационе моћи*, засноване на степену технолошког развоја (*технолошка моћ*), односно на стратешкој предности у односу на друге државе коју субјекти безбедности достижу правовременим и објективним обавештајним информацијама и подацима (*информациона моћ у ужем смислу*).

Савремено, технолошко-информацијско доба је помакло средиште националних вредности и интереса који попримају нову форму, садржај и значај. Традиционално поимање концепције заштите и остваривања државних и националних вредности и интереса засноване на одређеним стратегијама, кроз извесну политику и посредством одређених средстава, радикално је измењено:

³ Петровић, С.: О неопходности националне стратегије заштите кибер-простора, *Наука – Безбедност – Полиција*, број 2, Криминалистичко-полицијска академија, Београд, 2006, стр. 3–28; види и – *Technologies of (In)Security – The Surveillance of Everyday Life* (eds. Aas, K. F.; Gundhus, H. O.; Lomell, H. M.), Routledge, London, 2008; Jordan, T.; Taylor, P.: *Hacktivism and Cyberwars – Rebels with a Cause?*, Routledge, London, 2008.

⁴ Види – Мијалковић, С.: *Национална безбедност*, Криминалистичко-полицијска академија, Београд, 2009, стр. 159–161. *Интерес* је, уопштено, далекосежна усмереност воље, пажње и делатности појединца или колектива ка одређеном циљу, чије је постизање за њих важно. У достизању интереса исказује се задовољавање одређених потреба материјалне или духовне природе. Тадић, Љ.: *Политиколошки лексикон*, Завод за уџбенике и наставна средства, Београд, 1996, стр. 78–79; као безбедносно–политичка категорија, *интерес* је политички изражена или освешћена потреба, при чему садржај интересних опредељења битно зависи од постојећих система вредности носиоца потребе, који и дефинише интерес. Павловић, В.: *Интерес, Енциклопедија политичке културе* (група аутора), Савремена администрација, Београд, 1993, стр. 428–429.

– вредност информације повећана је у савременој глобалној економији, због чега је прерасла у нову вредност и постала стратешко национално добро;

– интелектуални капитал и интелектуални рад добијају превагу над материјалним капиталом и физичким радом, а националне економије су, више него икада, зависне од информационих система;

– глобалне информационе мреже олакшавају међународну економску сарадњу која је, нарочито у делокругу мултинационалних компанија, све независнија од националних влада, чиме традиционални суверенитет држава-нација губи значај;

– информацијско доба подиже важност политичких над безбедносним интересима, а технолошки неототалитаризам озбиљно угрожава старе тоталитарне режиме – технологија савременог доба представља оруђе превентивне дипломатије које помаже у промоцији људских права и демократије;

– економска безбедност и просперитет држава зависе од мултинационалних компанија које посредством информационе технологије искоришћавају националне државе једне против других у потрази за већим профитом при чему их, због интернационалне сфере деловања, није могуће позвати на националну одговорност, нити је могуће суверено контролисати светско тржиште;

– кибер-простор постао је ново поље ратовања и тероризма, а суверене нације које немају сателите више не могу да следе сопствене интересе путем ратова (оружја информацијског доба поништавају војни принцип масе; кибер-ратовање не захтева бојно поље нити посебно обучене војне јединице; тешко је приметити почетну офанзиву која долази „ниоткуда“ и бранити се од ње, при чему се непријатељ физички не уништава, већ парализује и контролише);

– дигитализовано знање је богатство које може само да се увећава, не и да се троши;

– владе које преузимају вођство у обликовању информацијских мрежа и лоцирају чворове међународних мрежа унутар својих граница стичу огромне погодности и предности на међународној економској, политичкој, телекомуникационој и „другим сценама“, а тиме и у сфери националне безбедности итд.⁵

Данас је остваривање националних вредности и интереса заправо концепција употребе знања која подразумева циљеве кооперативне и динамичне конкуренције на међународној сцени, контролу мрежних чворова међународних комуникација и организацијску прилагодљивост, и захтева ресурсе у виду вредних информација побољшаних искуством. Стога се и безбедност и интегритет кибер-простора морају сматрати важним, па и једним од виталних националних интереса. То условљава измене у досадашњем поимању стратегија националне безбедности које би морале да уваже информациону димензију живота друштва, држава и међународне заједнице.⁶

Савремена успешна концепција безбедности захтева уравнотежење циљева, начина и средстава концепцијске употребе дигитализованог знања. Без обзира на то да ли употребљавамо политичке, економске, војне или информацијске елементе националне моћи, државним и националним стратешким циљевима најбоље се служи кроз сарадњу у обликовању робусних информационих мрежа које промичу динамичку конкуренцију и

⁵ Националне вредности и национални интереси у информацијском добу, <http://zakladahanzekovic.ijf.hr/2003/slucaj.pdf>; види и – Keohane, R. O.; Nye, J. S. Jr.: Power, Interdependence and the Information age, *Perspectives on World Politics* (eds. Little, R.; Smith, M.), Routledge, London–New York, 2006, pp. 187–194; Karatzogianni, A.: *The Politics of Cyberconflict*, Routledge, London, 2008; Williams, M.: *Virtually Criminal*, Routledge, London, 2008.

⁶ Националне вредности и национални интереси у информацијском добу.

побољшавају заједничко деловање. С обзиром на информациону глобалну међузависност, државе ће тежити да буду примарне архитекте и посредници у мрежним операцијама.

Информацијске мреже ће бити пожељна мета напада многих носилаца угрожавања безбедности, што ће представљати истовремени напад на појединца, државу, међународну заједницу, односно друге (првенствено привредне) субјекте који се протежу на овим нивоима. Уравнотежење националних циљева, начина и средстава за њихово достизање, као и концепцијска употреба знања, први су корак ка правим стратешким одлукама у сфери националне безбедности у новом информационом добу.⁷

Национални информациони ресурси као вид моћи државе и фактор међународне безбедности

Националну безбедност умногоме детерминишу моћ и потенцијал државе. Моћ је њена способност да изнуди извесно понашање друге државе или субјеката према којима је моћ усмерена. Потенцијал су капацитети државе на којима почива њена моћ.⁸

Моћ државе у савременом свету није више пресудно одређена само величином територије, бројем становника, војном моћи, богатством у тзв. грубим сировинама и изворима енергије. Значајни извори моћи су и степен техничко-технолошког развоја, образовна и старосна структура становништва, али и утицај на доношење одлука у међународним организацијама. Даље, нови видови испољавања моћи државе су и привлачност културних добара, идеологије, начина размишљања и живота итд. Речју, моћ се црпи из *привлачности укупног цивилизацијског обрасца*. Тако „тврду моћ“ (*hard power*), која је оличена у војној моћи, све више потискују економско-финансијска, техничко-технолошка, комуникацијско-информативна, политичка и својеврсна демократско-друштвена моћ („мека моћ“ – *soft power*). Међутим, нова невојна димензија безбедности свакако још дуго неће у потпуности искључити војна средства у промишљању безбедности.⁹ Истовремено, војна димензија безбедности у многоме зависи од економско-финансијске, техничко-технолошке и комуникацијско-информативне моћи друштва, која све више почива на електронско-информационој технологији.

Моћ земље је продукт више видова моћи, а пре свега¹⁰:

– *војне моћи*, односно поседовања мобилних и обучених људских и респективних материјалних војних капацитета који су способни да у сукобу са противничком снагом извојују победу и покре га, наметајући му вољу своје владе;

– *економско-енергетске моћи*, тј. поседовања сировинских, стручних кадровских, производних, енергетских, финансијских и сличних капацитета који државу чине богатом, а њеним грађанима гарантују задовољавајући животни стандард. Такве државе су и војно, технолошки и културно моћне, и утицајне у међународним односима;

⁷ Исто.

⁸ Види – Nye, J. S. Jr.: Limits of American Power, *Political Science*, Vol. 117, No. 4., The Academy of Political Science, New York, 2002/2003, p. 548; Art, R. J.: The Fungibility of Force, *The Use of Force – Military Power and International Politics*, (eds. Art, R. J.; Waltz, K. N.), Rowman&Littlefield Publishers Inc., Oxford, 2004, pp. 3–22.

⁹ Симић, Д. Р.: *Наука о безбедности – савремени приступи безбедности*, Службени лист СРЈ и Факултет политичких наука, Београд, 2002, стр. 37–38.

¹⁰ Упореди са – Бжежински, З.: *Велика шаховска табла*, ЦИД, Подгорица, 2001, стр. 28–29.

– *културне моћи*, односно развијености културе, традиције, националне свести, националног идентитета и безбедносне културе, чиме друштво постаје модерна, сложна и хармонична целина способна да се одупре безбедносним проблемима и да свој допринос њиховом решавању;

– *политичке моћи*, која се јавља као резултанта наведених типова моћи државе, а огледа се у способности државе да доминира или да бар равноправно учествује у збивањима на међународној сцени, тј. у односима са другим државама и субјектима међународних односа и

– *моћи знања и технолошко-информационе моћи*, односно континуираног развоја науке, технике и технологије којим се унапређују образовни, производни, комуникацијски, истраживачки и животни процеси, али и војна и економска моћ земље.

Информациона моћ, коју поседују земље са развијенијом информационом технологијом, унапређује технолошку моћ, омогућава развој привреде и економије, модернизацију оружаних снага, унапређује животни стандард становништва, као и контролу чворова транснационалних комуникација и електронског саобраћаја, што увећава политичку моћ држава.¹¹

Ове врсте моћи неретко зависе и од демографског потенцијала државе, али и од геостратешког и геополитичког положаја земље; историје државе и права и друштвене традиције; географско-климатских фактора; политике, политичког система и политичке културе; дистрибуције моћи, интересних сфера и интересних група у друштву; идеологије, односно религије, културе и морала; међународних односа итд.

Моћ државе је традиционално средство очувања и заштите националне и међународне безбедности. *Међународна безбедност* је безбедност међународног поретка и заједнице, односно безбедност у односима држава и у међународним регионима. Може да се посматра на планетарном (*планетарна, светска безбедност*), континенталним (*континентална безбедност*) и на регионалним нивоима (*регионална безбедност*).¹² Односи међу државама крећу се од сарадње, преко надметања до сукоба, па се и међународна безбедност увек достизала кроз два модела: *конфликтни* (властита безбедност као добро за које се државе надмећу) и *кооперативни* (властита безбедност као заједнички циљ држава).¹³

Традиционално, примарни предмет међународних односа, међународног права, а тиме и међународне безбедности јесте етиологија и контрола силе као форме међународне комуникације. Овакав приступ оправдава „утисак да се у сваком веку, као да је у питању природан закон, појављује једна земља која поседује моћ и вољу, као и интелектуалну и моралну снагу, да у складу са сопственим системом вредности обликује читав међународни поредак, да утиче на међународне односе, уплиће се у унутрашње ствари других држава, намеће сопствене вредности, да се ангажује изван својих граница“.¹⁴ У данашњем – информационом свету, приметни су нови видови примене силе – тзв. *технотронични ратови*, које одликују дистанциона дејства „паметним“ (дигитализованим) оружјем, употреба високософистицираних

¹¹ Нye, J. S. Jr.: *Исто*, стр. 555.

¹² Упореди – Мијалковић С.: Безбеденост државе и концепти међународне безбедности, *Дефендологија – теоријско-стручни часопис за питања заштите, безбједности, одбране, образовања, обуке и оспособљавања*, број 25–26, Дефендологија центар за безбједносна, социолошка и криминолошка истраживања, Бања Лука, 2009, стр. 69–83.

¹³ Таталовић, С.: *Национална и међународна сигурност*, Политичка култура, Загреб, 2006, стр. 228.

¹⁴ Kissinger, H.: *Дипломатија I*, Верзал Прес, Београд, 1999, стр. 5.

„невидљивих“ летелица, злоупотреба сателитске и друге космичке технологије, вођење тзв. информационих ратова онеспособљавањем свих државних и друштвених система чији је рад подржан информационим системима, подршка тзв. кибер-тероризму итд.

Циљ концепта међународне безбедности је спречавање таквих „сценарија“, што се данас постиже кроз тзв. безбедносно повезивање држава. Идеја овог концепта је знатно ширира од старе максиме: „ако не можеш да га победиш, онда му се придружи“. Његова вредност је у настојању држава да заједнички превазиђу традиционална ривалства у анархичним међународним односима и да, достизањем безбедности савеза којим припадају, осигурају и сопствену безбедност: одрицањем или (само)ограничавањем сопствених на рачун заједничких интереса, „улагања држава могу им се вишеструко вратити“. То је суштина механизма *заједничке безбедности*.¹⁵

У фокусу савремених концепата међународне безбедности су идеје реципроцитета, изградње заједничког идентитета, као и заједнички интереси држава и друштава. У савременом – глобализованом свету, ове идеје се најбрже и најефикасније шире и реализују посредством савремених информационих технологија: електронски медији, сателитске комуникације и интернет мрежа најефикасније су средство за стварање нове – *глобалне масовне културе*, за изградњу нових – *регионалних вредности и интереса* и за конституисање нових – *регионалних идентитета*.

Даље, свакодневна интерна и екстерна комуникација бројних међувладиних организација – војних и цивилних, универзалних и регионалних, заснована је на информационим технологијама.

Осим тога, на међународној сцени функционишу бројни недржавни актери – мултинационалне компаније, невладине организације, финансијске агенције, међународне банкарске и финансијске мреже и слични субјекти, који имају сопствене међународне информационе мреже, односно део су ширих таквих мрежа.

Значи, осим што је средство међународног комуницирања и функционисања државних и недржавних актера, савремене информационе технологије су и кохезиони – фактор њиховог зближавања кроз изградњу заједничког идентитета и протежирање заједничких интереса и вредности. Дисфункција овог глобалног система вредности и интереса заснованих на информационим технологијама у било којем њиховом чвору или на било којој њиховој деоници, одражава се на цео систем.

Можда се због тога савремени ратови и воде од стране информационо моћних држава, а против земаља које не спадају у ред „информацијских“ лидера, нису информациони чворови и деонице, али се налазе на важним геостратешким положајима, обилују енергетским и индустријским ресурсима и јефтином радном снагом. У том смислу, држава која је информационо моћна, уједно је и безбеднија. Што је више таквих држава у једном региону, већа је и (међународна) безбедност таквих региона.

¹⁵ Безбедност се ефикасније остварује у заједништву, него сопственом моћи ван њега. На овој идеји засновани су концепти колективне безбедности и одбране, али и безбедносне заједнице, режима, комплекса и сарадње у безбедности. Види – Baylis, J.: International and Global Security in the Post-Cold War Era, *The Globalization of World Politics* (eds. Baylis, J.; Smith, S.), Oxford Press, New York, 2001. pp. 253–276, у: *Реформа сектора безбедности* (ур. Хацић, М.), Институт Г 17 плус и Центар за цивилно-војне односе, Београд, 2003., стр. 80; Johansen, R. C.: Building World Security: The Need for Strengthened International Institutions, *World Security – Challenges for a New Century* (eds. Klare, M. T.; Chandrani, Y.), St. Martin's Press, New York, 1998, p. 387.

О концепту информационе безбедности

Идеја концепта информационе безбедности није нова. Наиме, шездесетих година прошлог века у САД је развијен концепт тзв. *комуникационе безбедности* (COMSEC – *communication security*). Са појавом рачунара седамдесетих година, развијен је и концепт *компјутерске безбедности* (COMPUSEC – *computer security*). Крајем осамдесетих година, COMSEC и COMPUSEC су обједињени у информациону безбедност (INFOSEC – *information security*), чиме се настојало интегрисању раније одвојених сфера безбедности особља, компјутерске безбедности, комуникационе безбедности и оперативне безбедности. Акценат *информационе безбедности* стављен је на спречавању неауторизованог приступа информационим системима, чиме су гарантовани поверљивост, интегритет и расположивост информација, као и спречавање лишавања услуга ауторизованих корисника, укључујући неопходне мере детекције, документовања и отклањања таквих претњи. Истовремено, *информациона гаранција* (IA – *information assurance*) подразумева аутентичност и непорицљивост информација која, за разлику од информационе безбедности, обухвата и оперативност и осетљивост на време, односно детекцију и реакцију на којима се заснива концепт информационог ратовања и одбрамбених информационих операција (DIO – *defensive information operations*).¹⁶

Савремено поимање националне, али и других нивоа безбедности незамисливо је без сектора тзв. *информационе безбедности*. То није само један од сектора безбедности, већ је и пресек свих сфера безбедности у којима информационе технологије заузимају важно место. *Информациона безбедност је, дакле, интегрална компонента националне безбедности која подразумева стање заштићености животно важних вредности и интереса појединаца, друштва и државе у информационој сфери од спољашњих и унутрашњих опасности (ризика), односно стање заштићености информационе средине друштва које омогућава њено формирање, коришћење и развој у интересу грађана, организација и државе*. Стога је реално очекивати развој, па и преминацију овог сектора националне безбедности.¹⁷

Конкретније, *информациона безбедност је заштићеност националних информационих ресурса и потенцијала од физичког угрожавања, уз одсуство опасности које могу да угрозе информациону стабилност и самосталност*.

Информациона стабилност подразумева редовно, регуларно функционисање информационих система националних субјеката, уз постојање услова да се они развијају и остварују жељене и планиране циљеве, као и њихову перманентну заштићеност и заштићеност интереса корисника њихових услуга. Значи, *информациона стабилност* подразумева информациону ефикасност и информациону доступност.

Информациона ефикасност је сигурно и ефикасно функционисање информационих система државних и недржавних актера и њихово правовремено снабдевање неопходним информационим и електронским производима. *Информациона доступност* је могућност физичке доступности потребних електронских производа који су похрањени у сопственим електронским базама или у базама умрежених субјеката.

¹⁶ Петровић, Л.: Информациона сигурност у савременом свету, *Инфо М – Часопис за информационе технологије и мултимедијалне системе*, број 24, Факултет организационих наука, Београд, 2007, стр. 10–11.

¹⁷ Исто.

Информациона самосталност је независност државних и недржавних актера од иностраних информационих ресурса. Реч је о извесној *информационој независности*, односно *самодовољности* која, као витални национални и државни интерес многих друштава и земаља, подразумева постојање сопствених информационих ресурса којима се омогућавају минимум информационе стабилности, ефикасности и доступности.

Наравно, такве тежње би требало разликовати од тзв. *информационог национализма*, односно од потпуне информационе аутократије и самодовољности, што је у савременом свету готово немогуће. Колико год да су информационо доминантне, државе су део међународног информационог поретка. Информационо моћније државе су и „моћнији играчи“ на међународној сцени.¹⁸ Супротно, *информационо неразвијене и зависне* нације и државе немају капацитете и моћ за равноправно иступање у међународним односима, па су и подложније уступцима на разне притиске и уцене.

Најзад, *информациона зависност* је неопходност државних и недржавних актера да своје информационе потребе задовољавају „увозом“, јер то није могуће из националних информационих ресурса. Реч је о озбиљном проблему, због могућности наступања *информационе кризе*, тј. немогућности задовољавања основних информационим потреба, чак ни из иностранства.

О угрожавању националних информационих ресурса

Због значаја за функционисање државе и друштва, као и због номиналне и употребне вредности информација, података и електронских производа, информациони ресурси сваке земље су „пожељна и примамљива“ мета разних носилаца угрожавања безбедности. Начелно, сва угрожавања информационих ресурса могу да се поделе на она која настају унутар система (*унутрашња*), на она која долазе споља (*спољна*) и на она која су комбинованог порекла (*комбинована*).

Од безбедносних претњи унутрашњег порекла најзаступљеније су материјалне штете, оштећења и дисфункције које настају случајно, услед нерада и немара запослених, одговорних и руководећих лица. Свакако да су опаснија она угрожавања која су продукт свесног и намерног деловања људског фактора, од разних видова имовинског, преко економског, па до политичког криминала.

Спољна угрожавања информационих система такође су различита, од тзв. имовинског, преко политичког до компјутерског и других форми високотехнолошког криминала: неовлашћен упад у информациони систем државних и недржавних актера; копирање, преиначавање, физичка крађа или уништавање пословних података; намерно изазивање дисфункције информационих система; електронска шпијунажа; преусмеравање финансијских средстава на приватне рачуне; навођење одређених параметара информационих система на „самоуништавање“; извођење копјутерских саботажа, диверзија и терористичких напада и многи други.¹⁹

Најзад, ваља нагласити и то да до угрожавања великих информационих система долази и као последица природних катастрофа и елементарних непогода (земљотреси, поплаве, пожари, клизишта и сл.) и техничко-технолошких акцидената (пожари,

¹⁸ Упореди – Арежина-Ђерић Вера, „Специфичности мерења у политичким наукама“, Институт за политичке студије, Београд, 2009.

¹⁹ Види – Петровић, С.: *Компјутерски криминал*, МУП РС, Београд, 2001; Eagan, R.: *The Risks Assessment Methodology, Energy & Security: Global Challenges – Regional Perspectives*, Program of Atlantic Security Studies, Prague Security Studies Institute, Prague, 2005, p. 42–44.

експлозије, хаварије). Тада последице нарушене информационе безбедности по људе, односно по енергетску, економску, еколошку, националну, па и међународну безбедност, могу да буду несагледиве.

Последице угрожавања информационих система су различите по облику и интензитету, па их је и бесмислено набрајати и описивати. Истовремено, зависе и од тога о чијем информационом систему је реч (електропривреде, ПТТ саобраћаја, нуклеарне електране, оружаних снага, хемијске индустрије, авиокомпанија итд.). Из аспекта националне безбедности, пригодна је њихова подела према значају штетних ефеката на примарне, секундарне и терцијалне последице.

Примарне последице односе се на материјалну штету насталу на самим информационим системима и подсистемима, на њихову техничку дисфункционалност, као и на угрожавање здравља и безбедности на раду.

Секундарне последице односе се на све последице које настају као ефекти наступелих примарних последица. Оне могу да се манифестују као деградација животне средине, угрожавање живота и здравља људи у већем обиму и на већем простору, угрожавање квалитета живљења људи, дисфункција појединих сектора привреде и државног система, потенцијално угрожавање спољнополитичке безбедности земље и друго.

Најзад, *терцијалне последице* су најчешће материјално-финансијског карактера, односно трошкови и коштање санације наступелих примарних и секундарних последица.

О могућностима заштите информационе безбедности

Начелно, националне информационе ресурсе је могуће штитити на нивоу појединца, сопственим механизмима државних и недржавних актера који поседују информационе системе, механизмима националног система безбедности и механизмима међународне сарадње.

Појединац би, кроз развој тзв. *информационе културе*, која је интегрална компонента безбедносне културе²⁰, у доброј мери могао да штити сопствене информационе ресурсе, односно информационе ресурсе субјеката у којима је ангажован (запослен). Наравно да сви они не би могли да се одупру специјализованим „компјутерским криминалцима“, али би могли да им отежају у реализацији њихових намера (онемогућавањем физичког приступа рачунарским системима неовлашћеним лицима, постављањем шифри на персоналне рачунаре, чувањем копија важних података на облицима спољне меморије, уздржавањем од прикључивања на информационе мреже рачунара у којима су похрањени важни подаци, уградњом антивирус програма „firewall“ баријера итд.). Нажалост, наше друштво не спада у ред „информатички писменија“.

Даље, на нивоу државних и недржавних субјеката морале би да постоје организационе јединице које су специјализоване за информациону подршку њиховом раду. Ако нема посебних јединица за заштиту информационих система оне би, истовремено, штитиле мреже и базе података од неовлашћеног упада, крађа података и „компјутерског вандализма“. Истовремено, морале би да буду обучене за обезбеђивање

²⁰ Види – Стајић, Љ.; Мијалковић, С.; Станаревић, С.: *Безбедносна култура младих – како безбедно живети*, Драганић, Београд, 2006, стр. 156–159.

доказа о злоупотреби информационих технологија до доласка државних органа који спроводе истрагу. Њихови припадници би требало да буду чланови извесних струковних организација и удружења у оквиру чијих програма би се перманентно едуковали и стручно усавршавали. На овом нивоу, наша земља поседује добре информационе стручњаке, али не и развијене механизме сарадње.

На државном нивоу, у погледу спречавања и сузбијања појава којима се угрожавају национални информациони ресурси, морала би да постоји извесна правна регулатива и специјализовани субјекти безбедности. У погледу правне регулативе, наша земља не спада у ред оних које овом проблему поклањају заслужену пажњу.

Наиме, у погледу правне регулативе, осим Кривичног законика²¹, не постоји нарочита регулатива којом се штити овако важна национална вредност. Нажалост, и поред указивања наших еминентних стручњака на ову потребу²², у нашој земљи још увек не постоји *национална стратегија заштите кибер-простора*. У *Стратегији националне безбедности Републике Србије*²³ информациони ресурси, онако како их овде представљамо, помињу се на свега неколико места. Наиме, констатује се да је „тенденција повећаног коришћења информационо-комуникационих технологија праћена константним повећањем ризика од *високотехнолошког криминала и угрожавања информационих и телекомуникационих система*. Ризик у овом погледу постоји од угрожавања споља, али и у могућности злоупотребе података о грађанима и правним лицима.“ Даље, наводи се и да је „политика технолошког развоја усмерена на превазилажење технолошког заостајања и достизање нивоа технолошке развијености који ће бити у функцији развоја друштва и јачања националне безбедности. У том смислу потребна је целовита интеграција у међународни систем комуникација и информација, уз развој стратешког партнерства са државама које су носиоци савремених технологија.“ Најзад, помињу се и „могућности очекивања бројних нових изазова, ризика и претњи који се односе на злоупотребу нових технологија и научних достигнућа у области информатике...“.

Осим ове (последње) констатације, у *Стратегији одбране Републике Србије* додаје се још само то да „потенцијали одбране земље обухватају све људске, материјалне, енергетске, финансијске, информационе и духовне ресурсе.“²⁴

Када је реч о националном систему заштите информационих ресурса, у оквиру система безбедности наше земље успостављен је подсистем за супротстављање високотехнолошком криминалу. Он је конципиран је *Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала*.²⁵ Њиме се уређује образовање, организација, надлежност и овлашћења посебних организационих јединица државних органа ради откривања, кривичног гоњења и суђења за кривична дела високотехнолошког криминала.

Под високотехнолошким криминалом подразумева се вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари,

²¹ *Службени гласник РС*, број 85/2005. О појединим кривичним делима биће више речи у тексту који следи.

²² Види – Петровић, С.: О неопходности националне стратегије заштите кибер-простора, *Наука – Безбедност – Полиција*, број 2, Криминалистичко-полицијска академија, Београд, 2006, стр. 3–28.

²³ Са званичног сајта Владе Републике Србије: www.srbija.gov.rs).

²⁴ Са званичног сајта Владе Републике Србије: www.srbija.gov.rs).

²⁵ *Службени гласник РС*, број 61/2005.

рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском (рачунарски програми и ауторска дела) облику, и то:

– кривична дела против безбедности рачунарских података која су инкриминисана Кривичним закоником (Оштећење рачунарских података и програма (члан 298), Рачунарска саботажа (члан 299), Прављење и уношење рачунарских вируса (члан 300), Рачунарска превара (члан 301), Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302), Спречавање и организирање приступа јавној рачунарској мрежи (члан 303), Неовлашћено коришћење рачунара или рачунарске мреже (члан 304), Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (члан 304а) и кривична дела против интелектуалне својине, имовине и правног саобраћаја.

Ради обављања унутрашњих послова у вези са сузбијањем кривичних дела из области високотехнолошког криминала, образована је *Служба за борбу против високотехнолошког криминала* која функционише у оквиру Министарства унутрашњих послова. Служба поступа по захтевима посебног тужиоца, у складу са законом.

За поступање у предметима кривичних дела из области високотехнолошког криминала, за територију Републике Србије месно је и стварно надлежно Окружно јавно тужилаштво у Београду. У оквиру њега образује се *Посебно одељење за борбу против високотехнолошког криминала*. Његовим радом руководи *посебни тужилац за високотехнолошки криминал*, који има сва права и дужности као јавни тужилац.

За поступање у предметима кривичних дела из области високотехнолошког криминала надлежан је Окружни суд у Београду, за територију Републике Србије. У оквиру њега образује се *Веће за борбу против високотехнолошког криминала* које суди у првом степену. За одлучивање у другом степену надлежан је непосредно виши суд.

Најзад, у погледу међународне сарадње, наша земља такође није укључена у све видове међународне интеграције. Ангажовање наше земље у Интерполу и сличним видовима међународне полицијске сарадње није довољно. У том смислу, предстоји нам укључивање и интензивирање сарадње у оквиру бројних међувладиних и међународних невладиних струковних организација и тела.

ЗАКЉУЧАК

Неспорно је да на прагу трећег миленијума готово сва добра, вредности и интереси појединаца, група, држава и међународне заједнице на неки начин могу да се назову и *кибер-добрима*. Савремена информациона технологија бесповратно трансформише индустријско у информатичко друштво, почев од електронске куповине и плаћања, „школовања на даљину“, преко електронске државне управе (*e-government*) до дигитализације средстава националних система безбедности, оружаних снага и међународног повезивања држава и нација. Електронска будућност, о којој су други тако дуго и пуно говорили, постала је наша свакодневица.

Међутим, упоредо са бројним олакшањима, технотронизација друштва са собом носи и бројне ризике и претње, повећавајући рањивост поменутих кибер-добра од разних појава људског, природног и техничко-технолошког порекла које могу довести до њихове деструкције. Због тога, национални информациони ресурси се у савременој теорији националне безбедности с правом сматрају једном од виталних националних вредности, а њихово одржање и развој – једном од примарних националних интереса.

Како стратешке вредности траже стратешку заштиту, у савременој теорији и пракси безбедности развијен је концепт *информационе безбедности*. Њиме се протезира заштићеност националних информационих ресурса и потенцијала од физичког угрожавања, уз одсуство опасности које могу да угрозе информациону стабилност и самосталност. У основи овог новог концепта требало би да буде извесна *национална стратегија информационе безбедности*, која би била интегрална компонента *стратегије националне безбедности*. О доследном спровођењу ове стратегије требало би да се стара извешан специјализован и професионалан институционализовани подсистем националне безбедности, подржан одређеним законским и подзаконским прописима. Најзад, о информационој безбедности морали би да брину и појединци, првенствено одговорна лица у значајним информационим системима, али и политички одлучиоци који ће олакшати повезивање домаћих информационих стручњака и организација са истородним организацијама у иностранству, односно са међународним струковним организацијама.

Како су у овој сфери информационе безбедности наше земље евидентни бројни недостаци и пропусти (непостојање националне стратегије информационе безбедности, непостојање институционализованих субјеката који су специјализовани за развој информационе културе грађана и националних информационих ресурса, рестриктивно кривично законодавство које не прати све изазове и претње информационој безбедности, непостојање законских прописа који би подржали наведене сфере информационе безбедности, правна нерегулисаност организације и надлежности недржавног сектора безбедности итд.), предстоји нам озбиљна реконцептуализација система националне безбедности и дефинисање националних правних и стратегијских оквира за заштиту кибер-простора, уз уважавање домета развијене иностране и домаће теорије и праксе, али и посебности домаћих информационих потреба, прилика и околности.

ЛИТЕРАТУРА

1. Art, R. J.: The Fungibility of Force, *The Use of Force – Military Power and International Politics*, (eds. Art, R. J.; Waltz, K. N.), Rowman&Littlefield Publishers Inc., Oxford, 2004.
2. Арежина-Ђерић Вера, „Специфичности мерења у политичким наукама“, Институт за политичке студије, Београд, 2009.
3. Арежина Вера, „Еколошка безбедност – основа међунационалних безбедности“, Криминалистичке теме – часопис за криминалистику, криминологију и сигурносне студије, Сарајево, 2008.
4. Baylis, J.: International and Global Security in the Post-Cold War Era, *The Globalization of World Politics* (eds. Baylis, J.; Smith, S.), Oxford Press, New York, 2001. pp. 253–276, у: *Реформа сектора безбедности* (ур. Хаџић, М.), Институт Г 17 плус и Центар за цивилно-војне односе, Београд, 2003.
5. Burke, A.: Aporias of Security, *Alternatives: Global, Local, Political*, Vol. 27, No. 1, 2002.
6. Бжежински, З.: *Велика шаховска табла*, ЦИД, Подгорица, 2001.
7. Eagan, R.: The Risks Assessment Methodology, *Energy & Security: Global Challenges – Regional Perspectives*, Program of Atlantic Security Studies, Prague Security Studies Institute, Prague, 2005.

8. Johansen, R. C.: Building World Security: The Need for Strengthened International Institutions, *World Security – Challenges for a New Century* (eds. Klare, M. T.; Chandrani, Y.), St. Martin's Press, New York, 1998.
9. Jordan, T.; Taylor, P.: *Hackivism and Cyberwars – Rebels with a Cause?*, Routledge, London, 2008.
10. Karatzogianni, A.: *The Politics of Cyberconflict*, Routledge, London, 2008; Williams, M.: *Virtually Criminal*, Routledge, London, 2008.
11. Keohane, R. O.; Nye, J. S. Jr.: Power, Interdependence and the Information age, *Perspectives on World Politics* (eds. Little, R.; Smith, M.), Routledge, London–New York, 2006.
12. Kissinger, H.: *Дипломатија I*, Верзал Прес, Београд, 1999.
13. Кривични законик Републике Србије, *Службени гласник РС*, број 85/2005.
14. Мијалковић, С.: *Национална безбедност*, Криминалистичко-полицијска академија, Београд, 2009.
15. Мијалковић С.: Безбеденост државе и концепти међународне безбедности, *Дефендологија – теоријско-стручни часопис за питања заштите, безбједности, одбране, образовања, обуке и оспособљавања*, број 25–26, Дефендологија центар за безбједносна, социолошка и криминолошка истраживања, Бања Лука, 2009.
16. *Националне вриједности и национални интереси у информацијском добу*, <http://zaklada-hanzekovic.ijf.hr/2003/slucaj.pdf>.
17. Nye, J. S. Jr.: Limits of American Power, *Political Science*, Vol. 117, No. 4., The Academy of Political Science, New York, 2002/2003.
18. Павловић, В.: Интерес, *Енциклопедија политичке културе* (група аутора), Савремена администрација, Београд, 1993.
19. Петровић, Л.: Информациона сигурност у савременом свету, *Инфо М – Часопис за информационе технологије и мултимедијалне системе*, број 24, Факултет организационих наука, Београд, 2007.
20. Петровић, С.: *Компјутерски криминал*, МУП РС, Београд, 2001.
21. Петровић, С.: О неопходности националне стратегије заштите кибер-простора, *Наука – Безбедност – Полиција*, број 2, Криминалистичко-полицијска академија, Београд, 2006.
22. Симић, Д. Р.: *Наука о безбедности – савремени приступи безбедности*, Службени лист СРЈ и Факултет политичких наука, Београд, 2002.
23. Стајић, Љ.; Мијалковић, С.; Станаревић, С.: *Безбедносна култура младих – како безбедно живети*, Драганић, Београд, 2006.
24. *Стратегија националне безбедности Републике Србије*, Београд, фебруар 2010. године (са званичног сајта Владе Републике Србије: www.srbija.gov.rs).
25. *Стратегија одбране Републике Србије*, Београд, фебруар 2010. године (са званичног сајта Владе Републике Србије: www.srbija.gov.rs).
26. Тадић, Љ.: *Политиколошки лексикон*, Завод за уџбенике и наставна средства, Београд, 1996.
27. Таталовић, С.: *Национална и међународна сигурност*, Политичка култура, Загреб, 2006.
28. *Technologies of (In)Security – The Surveillance of Everyday Life* (eds. Aas, K. F.; Gundhus, H. O.; Lomell, H. M.), Routledge, London, 2008.
29. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *Службени гласник РС*, број 61/2005.

CORELATION OF INFORMATION AND NATIONAL SECURITY

Assistant professor, Saša Mijalković, PhD
Academy of Criminalistic and Police Studies, Belgrade

Assistant professor, Vera Arežina-Đerić, PhD
Academy for Diplomatic and Security Studies, Belgrade

Assistant professor, Goran Bošković, PhD
Academy of Criminalistic and Police Studies, Belgrade

Abstract: Modern conceptions of national security requires the use of digitized and conceptual knowledge in achieving, protection and improvement of vital national values and interests. Regardless they refers to the (possible) use of political, economic, military, or informational elements of national power, the state will be more effective if you establish control over international communications network nodes and of resources in the form of valuable information. Regarding the interdependence of the global information, the state will strive to be the primary architect and intermediaries in information network operations, which will ensure their safety. Therefore, the national information resources become vital national values, and the security and integrity of the cyber-space, ie. *information security* becomes one of vital national interest.

Keywords: information security, power states, cyber-space, national security.