Strategos, 3(2), 2019, 37-49
UDK 32
UDK 355/359
Izvorni znanstveni rad[1]

STRATEGOS

Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura

Gordan Akrap

Sažetak

U ovom se radu problematizira mjesto, važnost i uloga ulaganja u funkcioniranje, zaštitu i oporavak kritične infrastrukture, nacionalne i međunarodne, u kontekstu suvremenih hibridnih prijetnji i proračunskih obrambenih izdvajanja. S obzirom na to da će u budućim ratovima primarna meta napada biti određena kritična infrastruktura (ili više njih) , pri čemu će kao sredstvo napada poslužiti kiber prostor, ulaganja u zaštitu kritične infrastrukture potrebno je sagledati kroz prizmu proračunskih obrambenih izdvajanja.

Ključne riječi

Kritična infrastruktura, hibridne prijetnje, operacije utjecaja, obrambena proračunska izdvajanja

Abstract

This paper discusses the place, importance and role of investments in the work, protection and resiliency of critical infrastructure, national and international, in the context of modern hybrid threats and budget defence expenditures/allocations. Considering that in future wars the primary target of the attack is going to be critical infrastructure (one or more), and cyberspace will be a tool for conducting attack(s),

1 Članak je primljen u uredništvo 12. rujna 2019. i prihvaćen za objavu 3. prosinca 2019.

investments in the protection and resiliency of critical infrastructure should be observed through the prism of budget defence expenditures/allocations.

Keywords

Critical Infrastructure, Hybrid threats, Influence operations, Defence Budget Expenditures

Uvod

Povijest je pokazala da se pozitivan razvoj države i društva temelji na procesima koji su poznati kao industrijske revolucije. Predvodnici industrijskih revolucija postaju u tom procesu nositelji razvoja, stvarajući preduvjete za kreiranje novih vrijednosti. Oni koji ne uspiju uhvatiti korak s vremenom i razvojem osuđeni su na ovisnost o drugima, na teške i zahtjevne unutarnje i vanjske izazove s kojima će se teško moći suočiti. U procesima razvoja i novih industrijskih revolucija bitnu ulogu imaju kritične infrastrukture (KI-jevi) te će ta uloga s vremenom biti sve veća.

Razvoj terminologije KI-jeva pratio je razvoj, važnost i utjecaj KI-jeva (kako na pojedinačnoj, tako i na općoj i zajedničkoj razini) na pojedince, skupine, zajednice, društva, države i međunarodne zajednice. Istodobno je rasla i razvijala se međuovisnost različitih KI-jeva (na nacionalnoj i međunarodnoj razini) te njihov pozitivan utjecaj na gospodarski, politički, kulturni, sigurnosni i svaki drugi aspekt djelovanja i življenja.

Međutim, sve ono što je dobro i korisno za ljudski rod može se i treba upotrijebiti protiv njega kad se za tim pokaže potreba.[2] Stoga, shvaćajući važnost KI-jeva, države su pokrenule procese kojima su pokušale utvrditi sektore u kojima se mogu nalaziti KI-jevi, sektorska i međusektorska mjerila za određivanje toga što jesu i što nisu KI-jevi, međusobne ovisnosti i moguće negativne kaskadne učinke, analize rizika i prijetnji, kao i prijedloge

2 Liang, Q.; Xiangsui, W. 1999. *Unrestricted Warfare.* PLA Literature and Arts Publishing house. Peking. 25 str. http://www.scribd.com/doc/5714/Unrestricted-Warfare (pristupljeno 19. listopada 2009.).

uspostave zaštitnih mjera. S obzirom na činjenicu da suvremene sigurnosne prijetnje, uz nove paradigme napada, izravno ciljaju KI-jeve, potrebno je razmotriti mogućnost da se ulaganje u zaštitu, održivost i oporavljivost KI-jeva smatra ulaganjem u proračunska obrambena izdvajanja.

Kritična infrastruktura

Različite države različito su definirale sektore u kojima se na temelju postojećih mjerila mogu utvrditi nacionalni i/ili međunarodni KI-jevi. Međutim, svaka je država definirala informacijsko-komunikacijski, energetski i vodno-prehrambeni sektor kao sektore koji sadržavaju KI-jeve. Normalno i neometano funkcioniranje svih drugih sektora, odnosno KI-jeva koji se nalaze u njima, u manjoj ili većoj mjeri temelji se na neometanom i pouzdanom radu triju prethodno navedenih infrastruktura. Funkcionalnost KI-jeva može imati različite učinke na stanovništvo, društvo i državu, kako na pojedinačnoj razini, tako i na zajedničkoj razini. Pojava kriza na lokalnoj razini prouzročenih problemima u djelovanju KI-jeva lako može postati međunarodni problem za čije je rješavanje potrebno pokretanje brojnih aktivnosti kojima se treba spriječiti pojava, odnosno širenje mogućih negativnih učinaka.

Važnost KI-jeva za normalno funkcioniranje društva i države, odnosno njihova korist, ujedno je i njihov bitan nedostatak. Taj se podatak dobiva sagledavanjem cijelog niza sukoba koji su obilježili kraj 20. st. i početak 21. st. U prošlosti su napadi na KI-jeve bili u funkciji napada na druge ciljeve, no danas je došlo do promjene paradigme napada. Planiranje postojećih i budućih sukoba i ratova neumitno podrazumijeva i napade na KI-jeve, i to kao na primarne ciljeve napada kojim se napadnutoj strani pokušava nametnuti vlastita volja a da se pritom ne pokrenu vojni efektivi. U tom je smislu potrebno sagledati utjecaj suvremenih sigurnosnih izazova hibridne naravi na sigurnost, koju je potrebno definirati i kao stanje i kao proces.

Republika Hrvatska donijela je Zakon o kritičnim infrastrukturama (NN 56/13), kojim se uspostavio definicijski okvir, ali koji nije dovoljno uspješno proveden u praksu. Dodatni razlog zašto je potrebno ozbiljno raditi na

izmjenama i dopunama Zakona (ako ne i na potpuno novom zakonu) jest promjena postojećeg shvaćanja ovisnosti društva i države o normalom i sigurnom funkcioniranju KI-jeva, uloge i važnosti integracijskih procesa države te javnog, privatnog i akademskog sektora u cijelom nizu aktivnosti u zaštiti KI-jeva.

Hibridne prijetnje i hibridne operacije

Hibridne operacije podrazumijevaju cijeli niz aktivnosti usmjerenih prema postizanju stanja informacijske nadmoći i oblikovanja napadnutog cilja u skladu s napadačevim potrebama. Hibridne prijetnje, kao skup mogućih pojavnih oblika pojedinih hibridnih operacija, podrazumijevaju usmjereno i organizirano djelovanje prema pojedinoj ciljanoj publici[3] u cilju iskorištavanja (poticanja, produbljivanja) njezinih ranjivosti, stvaranja novih ranjivosti, poticanja osjećaja podjele, nesigurnosti, defetizma, nemoći, beznađa, dvojbenosti, sumnjičavosti, narušavanja i urušavanja demokratskih struktura i procesa te slabljenja i kontroliranja obrambenog sustava. Te se prijetnje mogu ostvariti primjenom različitih procesa i sustava, uključujući i one koji su dio KI-jeva: gospodarski, ekonomski, energetski, politički, kulturni, sportski, sigurnosni, medijski, informacijsko-komunikacijski itd. Suvremene hibridne prijetnje u samoj svojoj biti te procesu planiranja, pripreme, vođenja, upravljanja i praćenja imaju ishodište u korištenju izvještajno-sigurnosnog sustava. To je vektor djelovanja u koji je potrebno usmjeriti sustav za preventivno djelovanje kako bi se pravodobno uočila mogućnost hibridnog napada provođenjem nekih aktivnosti iz spektra hibridnih prijetnji, kao i tematskog područja (jednog ili više njih) koje će se vjerojatno iskoristiti kao sredstvo postizanja cilja.

Plastičan primjer suvremenih shvaćanja trajne uporabe hibridnih prijetnji i operacija utjecaja jest i sadržaj koji je u svojem radu 2013. istaknuo načelnik stožera Oružanih snaga Ruske Federacije general Valerij Gerasimov.[4]

3 Ciljana publika koju se izlaže djelovanju hibridnih operacija može biti pojedinac, skupina, zajednica i društvo.

4 Bajarūnas, Eitvydas (Ambassador at Large for Hybrid Threats Ministry of Foreign Affairs

U tom je radu naglasio promjenu paradigme napada u novim sukobima, koji ne moraju prerasti u ratove, u kojima prevladavaju aktivnosti iz spektra informacijskog ratovanja u odnosu na ratovanje klasičnim kinetičkim ubojitim sredstvima u omjeru 4 : 1 u korist informacijskog ratovanja. Druga novina u ruskoj strategiji koju naglašava general Gerasimov jest prihvaćanje činjenice da se aktivnosti iz spektra hibridnih prijetnji mogu i trebaju planirati i provoditi bez prestanka (24/7) i bez obzira na to vlada li stanje apsolutnog mira, krize, rata ili poraća. Iako je takvo stajalište pobudilo zanimanje široke javnosti, potrebno je jasno reći da na Zapadu nije nepoznato da operacije nekinetičkim sredstvima (operacije utjecaja) imaju iznimno važno mjesto u sukobima u odnosu na operacije u kojima se upotrebljavaju kinetička ubojita sredstva. To pokazuje cijeli niz medijskih aktivnosti[5] kojima je Zapad izlagao stanovništvo i vodstvo država koje su se od kraja Drugoga svjetskog rata pa sve do raspada Sovjetskog Saveza i Istočnog bloka nalazile iza željezne zavjese.

Kiber prostor

Analizom kriza, sukoba i ratova koji se događaju u posljednjih desetak godina (tzv. Arapsko proljeće, Ukrajina, Sirija, Venezuela, migrantska kriza 2015.) te pojedinih političkih procesa (predsjednički izbori u SAD-u 2016. i Francuskoj 2018. te referendum o Brexitu 2016.) potrebno je izvući određene zaključke. Oni nam trebaju kako bismo u budućnosti mogli pravodobno predvidjeti pojavu, narav i kontekst kriza i sukoba, identificirati moguće napadače, njihove ciljeve, metode, modele, sredstva, komunikacijske kanale

of Lithuania). 2017. *Countering hybrid threats and building resilience: case of Lithuania* (ppt prezentacija).

5 Dio hladnoratovskih operacija utjecaja kojima se pokušavalo utjecati na stajališta, mišljenja, percepciju i odluke stanovništva i vodstva država Istočnog bloka jesu osnivanja i djelovanja radijskih postaja kao što su Radio Liberty, Radio Free Europe, Radio Marty, Radio in American Sector in Berlin, Voice of America i Radio Asia. Tadašnji Sovjetski Savez osnovao je Radio Moskvu kako bi pokušao parirati zapadnim medijima. Više o hladnoratovskim operacijama utjecaja može se naći u: Akrap, G. (2011.) *Informacijske strategije i operacije u oblikovanju javnog znanja* (doktorska disertacija). Filozofski fakultet Sveučilišta u Zagrebu. Zagreb.

te angažirane osobe i organizacije. Može se tvrditi da je informacijsko-komunikacijski sektor primarno područje sukobljavanja različitih subjekata koji pokušavaju doći do položaja informacijske nadmoći, a tako će biti i u budućnosti. Postizanjem takva stanja napadač može uspješno nadzirati i oblikovati kognitivne procese odnosno utjecati na procese razmišljanja i odlučivanja ciljanih publika. Svrha je natjerati ciljanu publiku da donosi odluke koje joj kratkoročno i dugoročno mogu nanijeti ozbiljne štete.

Jedno od ključnih sredstava koje napadači, sadašnji i budući, koriste u postizanju tog cilja jesu i aktivnosti u kiber prostoru. Taj prostor definiramo kao četverodimenzionalni prostor (zemljopisna rasprostranjenost, logičke mreže, ljudski čimbenik sa svojim stvarnim i virtualnim identitetima te umjetna inteligencija) u kojemu svaka od utvrđenih dimenzija ima svoju ulogu, važnost i odgovornost, ali i osjetljivost na različite podražaje. Praksa je pokazala da, s gledišta sigurnosti, ljudski čimbenik predstavlja najkritičniju točku cijelog kiber prostora. To je i razlog zašto se najviše pozornosti u planiranju i provođenju napadnih djelovanja pridaje prikupljanju izvještajno-sigurnosnih podataka o osobama koje su na neki način povezane s ciljem koji se namjerava postići.

Kiber prostor ujedno je prostor kojim se pojedine (ili brojne) ciljane publike najbrže mogu izložiti djelovanju različito oblikovanih (dez)informacija. Objavljivanje informacijskog sadržaja s upitnom razinom istinitosti, točnosti i potpunosti, autora čije su vjerodostojnost i pouzdanost problematične, vrlo je često prikriveno drugim djelovanjima i informacijama koje u neiskusnih čitatelja (odnosno primatelja oblikovanih poruka) mogu pridonijeti dezinformiranosti. S takvim primateljem dezinformacija može se lako manipulirati te je on potencijalno štetan za svoju okolinu.

Kiber prostor nova je bojišnica te će u sagledivoj budućnosti biti primarna bojišnica svih suvremenih sukoba. U to više nema nikakve sumnje. Taj prostor obilježavaju sukobi različitih intenziteta između različitih subjekata koji mogu, ali i ne moraju, biti svjesni takva stanja. Za razliku od stvarnog svijeta, u kojemu postoje pravila ratovanja i međunarodno prihvaćene institucije koje te procese na neki način mogu kontrolirati i penalizirati, napadačko djelovanje u kiber prostoru nije ograničeno. U njemu ne postoje

međunarodno prihvaćene norme ponašanja ni pravila sukobljavanja i ratovanja, a još manje međunarodno priznate i prihvaćene institucije koje bi takva pravila pratile i po potrebi sankcionirala njihovo kršenje. S obzirom na nepostojanje takvih pravila i zlouporabu prava u kiber prostoru u različitim demokratskim procesima, jača svijest o potrebi za definiranjem pravila sukobljavanja i ratovanja, odnosno ponašanja u kiber prostoru. Ta pravila trebaju i smiju odrediti samo subjekti međunarodnog prava, a ne tvrtke i korporacije koje taj prostor pokušavaju monopolizirati (kao što su Facebook, Alphabet i sl.).

Država treba biti nadležna za pravo i mogućnost odgovora na napade koji se događaju u kiber svijetu ili iz njega dolaze. Pravo na represiju i reakciju ne smije se prepustiti ni jednom privatnom ili korporativnom entitetu. Država, odnosno međunarodna organizacija, mora uz pomoć javnog, privatnog i akademskog sektora raditi na razvijanju modela preventivne aktivne obrane s mogućnosti ranog prepoznavanja, pouzdanog i nedvojbenog identificiranja kiber napadača te odgovarajućeg odgovora na sve sigurnosne izazove i krize u kiber prostoru. U tom smislu treba raditi na snažnoj i potpunoj integraciji znanja, sposobnosti i mogućnosti između svih dionika sustava domovinske sigurnosti (državnog, privatnog, javnog i akademskog sektora) – kako na nacionalnoj razini, tako i na odgovarajućoj međunarodnoj razini.

Suvremene sigurnosne prijetnje i izazovi

Iz svega navedenoga može se zaključiti sljedeće:

- Primarni cilj svih budućih neprijateljskih aktivnosti bit će nastojanje napadača da stvori stanje informacijske nadmoći u informacijsko-komunikacijskom prostoru.
- Kako bi se taj cilj ostvario, napadač će napadati sljedeće tri ključne kritične infrastrukture (nacionalne i međunarodne): informacijsko-komunikacijska (uključujući kiber prostor), energetska, vodno-prehrambena.
- Najučinkovitije sredstvo za ostvarivanje stanja informacijske nadmoći jest stjecanje nadmoći u kiber prostoru.

- Pravila sukobljavanja i ratovanja u kiber prostoru ne postoje, što znači da nema metoda, radnji, ciljeva i sredstava koji su zabranjeni. Ne postoji međunarodno prihvaćen sustav ni organiziranost nadzora i kontrole nad procesima i aktivnostima u tom prostoru. Time se znatno otežava organiziranje učinkovitih obrambenih mjera, posebno na pasivnoj preventivnoj razini.
- Budući napadi bit će hibridne naravi. U njima će prednjačiti uporaba nekinetičkih sredstava (operacije utjecaja, informacijske i medijske operacije, uporaba različitih politika kao izvora prijetnji), dok će se uporaba kinetičkih ubojitih sredstava (vojnih, oružanih) upotrebljavati tek kad se iscrpe sve mogućnosti primjene nekinetičkih metoda i modela napada. Dodatna je prednost tih napada jednostavnija mogućnost njihova učinkovitog poricanja, odnosno otežano identificiranje stvarnog napadača i njegovih namjera.
- U pripremi, planiranju, vođenju i nadzoru napada napadač mora koristiti, ako želi biti učinkovit, sposobnosti izvještajno-sigurnosnog sustava, i to u svim fazama djelovanja. Budući da se djelovanja izvještajno-sigurnosnog sustava na prikupljanju i obradi nužnih podataka mogu lakše uočiti, potrebno je obratiti pozornost na njih jer se njihovim ranim otkrivanjem stvaraju uvjeti za postupanja u učinkovitoj preventivnoj aktivnoj obrani.
- Najranjiviji dijelovi svakog sustava i procesa jesu ljudi, zbog čega je njihovoj sigurnosti, stalnom procesu obrazovanja, obučavanja i usavršavanja te razvoju ukupne društvene sigurnosne kulture potrebno posvetiti posebnu i trajnu pozornost.

Suočavanje sa suvremenim sigurnosnim prijetnjama i izazovima

Što se može i treba napraviti kako bi se pouzdano i pravodobno moglo prepoznati napadne namjere te organizirati učinkovitu obranu? Odgovor nije ni lak ni jednostavan te podrazumijeva organiziranje cijelog spektra aktivnosti koje se, po sadašnjim zakonodavnim pravilima, vrlo često nalaze na rubu zakonitosti. Istaknut ćemo samo ključne aktivnosti koje upućuju na potrebu za sustavnim pristupom u suočavanju sa suvremenim sigurnosnim prijetnjama i izazovima:

- Razvoj obrazovnog sustava koji će buduće stanovnike, a time i one koji će doći u situaciju da će tijekom života donositi različite vrste odluka uime drugih i za njihove potrebe, naučiti ispravno tumačiti informacije te znati raspoznati neistinu od istine. U procesima prepoznavanja i razlikovanja istine od neistine ne smijemo se oslanjati samo na algoritme i umjetnu inteligenciju, koji se već pokušavaju primijeniti za pravodobno uočavanje dezinformacijskih aktivnosti. Ljudi moraju biti ti koji će donositi konačne odluke.
- Trajno sigurnosno osposobljavanje, obučavanje i obrazovanje ljudi uključenih u pojedine procese zaštite kritičnih infrastruktura jer će one biti prva meta napada hibridne naravi svih budućih napadača.
- Postizanje stanja digitalnog suvereniteta na razini zemalja članica EU-a i NATO-a te na razini integracijskih organizacija, uz poštovanje stečenih prava i sloboda pojedinaca i zajednica, izbjegavajući ponavljanje ruskog i kineskog modela stvaranja izolacionističkog i represivnog digitalnog suvereniteta.
- Subjekt međunarodnog prava (država, relevantna međunarodna organizacija) mora preuzeti svoju zakonodavnu ulogu i propisati jasna i obvezujuća pravila ponašanja u kiber prostoru te pravila, načine i metode kažnjavanja uočenih i prepoznatih nedopuštenih aktivnosti u kiber prostoru bez obzira na to tko ih je počinio.
- Stalno ulaganje materijalnih i ljudskih resursa u kiber, tehničku i fizičku zaštitu KI-jeva – kako na nacionalnoj, tako i na međunarodnoj razini – te integriranje tih zaštita s obzirom na integriranost i visoku međuovisnost KI-jeva. Potrebno je poticati investiranja privatnog sektora u učinkovitu zaštitu KI-jeva koji su u njihovu vlasništvu ili kojima upravljaju. To je pitanje vrlo zahtjevno jer su brojni KI-jevi u vlasništvu privatnih tvrtki ili one njima upravljaju. Stoga je potrebno pronaći način kako definirati i razdvojiti ulaganja držanog i privatnog sektora u cilju zaštite i oporavka KI-jeva. Jedno je od mogućih rješenja priznavanje ulaganja privatnih tvrtki u procese zaštite i oporavka KI-jeva na nacionalnoj razini kao budućih poreznih olakšica koje bi država mogla pripisati ulaganjima vlastitih sredstava u obrambene svrhe.

- Stvaranje odgovarajućeg obrambenog sustava i mehanizama integriranjem sposobnosti koje na nacionalnoj razini imaju državni, javni, privatni i akademski sektor te isto takva suradnja na međunarodnoj razini. Bitni dionici tog sustava jesu vlasnici i upravljači kritičnih infrastruktura o kojima ovisi normalno, sigurno i pouzdano svakodnevno funkcioniranje društva i države. Taj sustav mora biti pod isključivom kontrolom i nadzorom države ili odgovarajućih međunarodnih organizacija, odnosno onih koje imaju zakonsko pravo na primjenu sile i represije.
- Subjekt međunarodnog prava ne treba se ustručavati od toga da vodeću ulogu u procesima ranog prepoznavanja i reakcije na hibridne prijetnje u određenom trenutku i na određeno razdoblje prepusti drugom sektoru (privatnom, javnom, akademskom) ako je u tom trenutku i u tom procesu to najbolje rješenje, zadržavajući snažnu sastavnicu kontrole i nadzora nad djelovanjem zajedničkog tima. Suradnja mora biti obvezna za sve dionike tog procesa.
- Stvaranje sustava koji će moći osigurati sveobuhvatan odgovor (na preventivnoj razini) ranog prepoznavanja hibridnih prijetnji, njihova shvaćanja, aktiviranja i koordiniranja djelovanja zaštitnog sustava, praćenje i vođenje primjenom procesa reagiranja, učenja iz iskustava te prilagodbe, a po potrebi mijenjanja i prilagođavanja postojećeg sustava kako bi bio još učinkovitiji.
- Uspostavljeni sustav mora moći pouzdano izvršavati tri ključne aktivnosti: rano uočavanje i prepoznavanje nadolazećeg napada, nedvojbeno identificiranje napadača, omogućivanje primjerenog protudjelovanja s obzirom na uporabljena sredstva i njihov intenzitet u odnosu na planirane učinke.
- Donijeti standarde definiranja aktivne obrane u kiber prostoru i zaštite pojedinih KI-jeva, odnosno rješenja za to kako reagirati na koju vrstu podražaja (pri čemu se postavlja klasično pitanje treba li na napad kiber pištoljem odgovoriti napadom kiber atomskom bombom).

Rasprava i zaključak

Budući sukobi počet će (i nastaviti se odvijati) u kiber prostoru, što se može primijetiti i na suvremenim primjerima, i to različitim intenzitetom u vremenskom kontinuumu. Primarni ciljevi tih napada, koji nužno ne moraju prerasti u oružane sukobe, bit će kritične infrastrukture. Model napadačkih djelovanja koji će se primjenjivati bit će hibridne naravi.

Danas je bez jasno definiranih pravila teško organizirati učinkovitu obranu kiber prostora i zaštitu KI-jeva, čije se sigurno djelovanje temelji, između ostaloga, na integritetu, stabilnosti, sigurnosti i pouzdanosti kiber prostora, a u skorijoj budućnosti bit će još i teže. Stoga subjekti međunarodnog prava (države i međunarodne organizacije) trebaju prihvatiti činjenicu da je ulaganje u sveobuhvatnu zaštitu KI-jeva (kiber, tehnička, fizička) u cilju njihove zaštite od mogućih napadača, kao i njihova brzog i učinkovitog oporavka nakon izlaganja pojedinom sigurnosnom riziku, ulaganje u pojedinačnu i opću sigurnost. Kako na nacionalnoj, tako i na međunarodnoj razini. To se osobito odnosi na ulaganja u sektore KI-jeva, koji će biti primarni ciljevi budućih napada prijetnjama koje dolaze iz spektra hibridnog djelovanja: informacijsko-komunikacijski (kiber), energetski i vodno-prehrambeni. Naime, mogući negativni kaskadni učinak djelovanja na druge KI-jeve do kojeg može doći napadom na neki od triju prethodno navedenih KI-jeva može prouzročiti ozbiljne ljudske i materijalne gubite, odnosno potaknuti snažne valove nasilja i unutarnjih sukoba.

Stoga se sva ulaganja države (te pojedina privatnog sektora) u zaštitu, povećanje otpornosti i pospješivanje oporavka ugroženih KI-jeva trebaju shvatiti i prihvatiti kao ulaganja u vlastitu i zajedničku obranu. Kao takva, ulaganja bi se trebala predstavljati kao proračunska obrambena izdvajanja, a tako bi se trebala tumačiti i računati. Na taj bi se način dao dodatni doprinos jačanju stanja pojedinačne i opće sigurnosti, jačala bi se strateška sigurnosna kultura države i sigurnosna kultura stanovništva, rasla bi razina povjerenja stanovništva u sposobnost institucija vlastite države (ali i međunarodne organizacije kojoj država pripada ako bi i ona sudjelovala u takvim aktivnostima), dodatno bi se smanjio manevarski prostor koji će napadač

pokušati iskoristiti za promicanje vlastitih ciljeva te bi se intenzivirala suradnja između državnog, javnog, privatnog i akademskog sektora. Razvoj, djelovanje, zaštita i sigurnost KI-jeva jedan su od temelja na kojima se može i treba graditi sigurno i demokratsko društvo integriranjem svih sposobnosti i znanja koja mu stoje na raspolaganju.

Referencije

Akrap, G. 2011. *Informacijske strategije i operacije u oblikovanju javnog znanja* (doktorska disertacija). Filozofski fakultet Sveučilišta u Zagrebu. Zagreb.

Bajarūnas, E. 2017. *Countering hybrid threats and building resilience: Case of Lithuania* (ppt prezentacija). Zagreb

Liang, Q.; Xiangsui, W. 1999. *Unrestricted warfare*. PLA Literature and Arts Publishing house. Peking. http://www.scribd.com/doc/5714/Unrestricted-Warfare (pristupljeno 19. listopada 2009.)

Zakon o kritičnim infrastrukturama, NN 56/13. https://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1134.html (pristupljeno 10. rujna 2019.)

O autoru

Dr. sc. Gordan Akrap diplomirao je na Fakultetu elektrotehnike i računarstva Sveučilišta u Zagrebu te je 2011. doktorirao na Odsjeku za informacijske znanosti i komunikologiju Filozofskog fakulteta u Zagrebu. Tema disertacije glasi „Informacijske strategije i operacije u oblikovanju javnog znanja". Ima znanstveno zvanje znanstvenog suradnika informacijskih znanosti i komunikologije. Dragovoljac je Domovinskog rata od 1990. Završio je veći broj stručnih seminara te jednogodišnji studij na Diplomatskoj akademiji MViEP RH. Aktivno je radio u sigurnosnom sustavu i diplomaciji RH. Nositelj je više odličja i medalja. Autor je nekoliko knjiga te znanstvenih i stručnih radova iz područja međunarodne, nacionalne i korporativne sigurnosti, izvještajno-sigurnosnih sustava, informacijskog ratovanja te Domovinskog rata. Aktivno je sudjelovao na brojnim međunarodnim simpozijima. Održao je niz predavanja

u Hrvatskoj i u inozemstvu o temama iz područja Domovinskog rata i strategija međunarodne, nacionalne i korporativne sigurnosti te međunarodnih odnosa. Od 2015. član je uprave međunarodne stručne organizacije International Intelligence History Association. Osnivač je i predsjednik zagrebačkog Instituta za istraživanje hibridnih sukoba. Pokretač je i glavni organizator međunarodnog foruma stručnjaka za zaštitu kritičnih infrastruktura od suvremenih sigurnosnih izazova i prijetnji pod nazivom Zagreb Security Forum, koji se održava od 2016.