KIBERNETSKA SIGURNOST I SUSTAV BORBE PROTIV KIBERNETSKIH PRIJETNJI U REPUBLICI HRVATSKOJ

Hrvoje Vuković *

SAŽETAK: Kibernetski prostor određujuće je obilježje suvremenog života i ključno područje svjetskog gospodarstva. Dnevno se zabilježe deseci tisuća manje ili više opasnih napada u kibernetskom prostoru, a vodeće zemlje svijeta, kao i međunarodne organizacije, kojih je član i Republika Hrvatski, pokazuju rastuću svijest o potrebi djelovanja s ciljem povećanja stupnja sigurnosti kibernetskog prostora. Mnoge od njih već imaju svoje nacionalne strategije kibernetske sigurnosti i uspostavljane sustave. Mnoge od njih imaju svoje nacionalne strategije kibernetske sigurnosti i uspostavljane sustave. Kako u ovoj temi znanstvena literatura na hrvatskom jeziku oskudijeva potrebno je početi uvodom, definiranjem osnovnih pojmova i kategorizacijom ugroza u kibernetskom prostoru, te ispitivanjem sustava kibernetske sigurnosti Republike Hrvatske.

* Ovaj rad izvadak je iz završnog rada „Kibernetsko ratovanje i kibernetski terorizam – sustavi borbe protiv kibernetskih prijetnji“ koji je obranjen na specijalističkom poslijediplomskom studiju na Fakultetu političkih znanosti Sveučilišta u Zagrebu. Stavovi izneseni u radu izraz su osobnog mišljenja autora i ne predstavljaju stavove institucije u kojoj autor radi.

KLJUČNE RIJEČI: cyber, kibernetska sigurnost, kibernetski prostor, kibernetske prijetnje, kibernetski rat, kibernetski terorizam, kibernetski kriminal, kibernetska špijunaža, kritična infrastruktura, informacijska sigurnost, informatička sigurnost.

Summary: Cyberspace is a determining feature of modern life and the key area of world economy. Daily there are tens of thousands of cyber attacks with varying degrees of harmfulness, and the leading countries and international organizations, whose member is also the Republic of Croatia, are showing increased awareness about the need to increase cyber security. Many of them have already developed national strategies and set up systems. As scientific literature on this subject is scarce in Croatian, I will begin with an introduction, defining the basic concepts and categorizing cyber threats, as well as examining the cyber security system in the Republic of Croatia.

Keywords: cyber, cyber security, cyber space, cyber threats, cyber war, cyber terrorism, cyber war, cyber espionage, critical infrastructure, information security, information security.

Uvod

S obzirom da se pojedinci i zajednice diljem svijeta povezuju, socijaliziraju i organiziraju i putem kibernetskog prostora, on je postao određujuće obilježje suvremenog života. Od 2000. do 2010. broj korisnika Interneta, te najrasprostranjenije mreže kibernetskog prostora, porastao je s 360 milijuna na 2 milijarde korisnika.

Sva domaća i međunarodna poslovanja već se temelje na trgovini robama i uslugama koje se u današnje vrijeme zahvaljujući kibernetskom prostoru koji je postao inkubator novih oblika poslovanja, napretka u znanosti i tehnologiji, širenja informacija, te novih društvenih mreža, odvijaju u sekundama. Stoga je kibernetski prostor danas i ključno područje svjetskog gospodarstva.

Učinkovitost i sigurnost kritičnih infrastruktura zemalja razvijenog svijeta, pa tako i Republike Hrvatske, uključujući energetiku, bankarstvo i financije, promet, komunikacije itd. ovise o kibernetskom prostoru, industrijskim nadzornim sustavima, te o ranjivoj informatičkoj tehnologiji.

Dnevno su u svijetu odviju deseci tisuća različitih manje ili više opasnih napada u kibernetskom prostoru. Aktivnosti vodećih zemalja svijeta i međunarodne organizacije u posljednjih nekoliko godina, a posebno u proteklih nekoliko mjeseci potvrđuju rastuću svijest o učestalosti i razornosti tih napada. Sjevernoatlantski savez svojim novim strateškim konceptom daje naglasak opasnostima u kibernetskom prostoru, uvrštavajući kibernetske prijetnje među ugroze koje čine sigurnosno ozračje u nadolazećim razdobljima.

William J. Lynn, zamjenik američkog ministra obrane, napisao je 2008. "as a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain in warfare . . . [which] has become just as critical to military operations as land, sea, air, and space".[1] Godine 2009. američki predsjednik Barack Obama američku digitalnu infrastrukturu proglasio je „strateškom nacionalnom imovinom“, a u svibnju 2010. Pentagon je ustrojio U.S. Cyber Command (USCYBERCOM), na čelu s generalom Keithom B, Alexanderom, ravnateljem Agencije za nacionalnu sigurnost (National Security Agency - NSA), kako sa svrhom obrane američkih, u početku vojnih, a danas već i civilnih, mreža, tako i sa svrhom napada na mrežne sustave drugih zemalja.[2]

Velika Britanija uspostavila je središte za kibernetsku sigurnost i operacije u kibernetskom prostoru unutar Government Communications Headquarters (GCHQ), britanskog ekvivalenta NSA-u. Kina je najavila kako do sredine 21. stoljeća namjerava pobijediti u kibernetskom ratu.[3] I mnoge druge zemlje, kao što su Njemačka, Francuska, Rusija, Iran i druge pripremaju se za sukobe u kibernetskom prostoru. O sposobnostima Rusije već

1 William J. Lynn III „Defending a New Domain – The Pentagon's Cyberstrategy“, Foreign Affairs, 2010. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

2 USCYBERCOM ustrojen je nakon Operacije Buckshot Yankee iz 2008. - operacije čišćenja vojnih računalnih sustava od crva koji je izvršio do sad najveće kompromitiranje nekog vojnog sustava. Pretpostavlja se kako je crv agent.btz strana obavještajna služba pomoću USB diska postavila na vojni laptop negdje na Bliskom istoku odakle se crv učitao u povjerljive vojne sustave (U.S. Central Command). Maliciozan kod ostao je neprimjetan, a omogućavao je slanje podataka na strane servere. Operacija odbacivanja napada trajala je 14 mjeseci.

3 Cyberwar: War in the fifth domain, THE ECONOMIST, London, 1.7.2010.

svjedoče njezini (iako nedokazani) napadi na Estoniju 2007. i Gruziju 2008. Jedna od posljedica traume koju je Estonija doživjela je i uspostava NATO Cooperative Cyber Defence Centre of Excellence u listopadu 2008. u Estoniji (Tallin).

Ministarstvo vanjskih i europskih poslova Republike Hrvatske u proteklih nekoliko godina zabilježilo je iznimno povećanje aktivnosti u međunarodnim organizacijama (UN, OESS, NATO, EU) koje se odnose na kibernetske prijetnje, iz čega se može zaključiti kako pitanje kibernetske sigurnosti postaje sve značajnije pitanje u međunarodnim odnosima.

Republika Hrvatska, iako svojim zakonodavstvom ne uspostavlja zaseban sustav sigurnosti kibernetskog prostora, njegovu sigurnost provodi prije svega kroz sustav informacijske sigurnosti, ali i druge sigurnosne sustave.

Do sada nisu napravljena istraživanja o ovisnosti kritične infrastrukture Republike Hrvatske o informatičkim tehnologijama, mrežama i kibernetskom prostoru, te njenoj ranjivosti spram kibernetskih ugroza. Time se otvara niz pitanja vezanih za razinu i kvalitetu spremnosti sustava da odgovori na ozbiljne ugroze u kibernetskom prostoru.

Pojmovna određenja

Za pojam cyber još ne postoje precizne definicije. Rječnik stranih riječi navodi kako je cyber prvi element u riječima koji označava nešto vezano uz svijet prividne stvarnosti koji nastaje pomoću računala.[4] Prema pojmovniku National Security Agency (NSA) cyber je prefiks koji se koristi kako bi se osoba, stvar ili ideja svrstala kao dio računalnog ili informacijskog doba.[5]

Za pojam cyber još ne postoji ni ustaljen odgovarajući prijevod na hrvatski jezik. Naime, u Republici Hrvatskoj učinjena je terminološka zbrka kada se prevodila konvencija Convention on Cybercrime.6 Hrvatski prijevod konvencije glasi Konvencija o kibernetičkom kriminalu, iako riječ kibernetika (engl. Cybernetics) nije istoznačnica riječi cyber.7 Stoga neki autori smatraju kako je pridjev

4 Anić, Vladimir — Goldstein, Ivo: Rječnik stranih riječi, Zagreb, 2004.

5 http://www.nsa.gov/about/faqs/terms_acronyms.shtml

6 Konvenciju o kibernetičkom kriminalu donijelo je Vijeće Europe 23. studenoga 2001., a stupila je na snagu 1. srpnja 2004. RH je konvenciju potpisala 17. 10. 2002.

7 Pojam "cyber" korišten je po prvi put 1834. godine kada ga je francuski fizičar André-Marie Ampere (1775.-1836.) istaknuo kao oznaku "cybernétique", koja je označavala znanost o vladanju u njegovom sustavu ljudskog znanja. Sam pojam "cyber" ima dva korijena u grčkom jeziku: u riječi kubernetes koja znači upravitelj te u riječi kubernan koja

„kibernetički“ pogrešan prijevod, te kako se pojam cyber treba odvojiti od pojma kibernetika.8 Kibernetiku bi najkraće mogli definirati kao "sustavno proučavanje komunikacije i upravljanja u organizacijama svih vrsta".[9] Dakle, kibernetika je znanstvena disciplina, a cyber se, kako je navedeno u pojmovniku NSA-e, odnosi na svijet koji nastaje pomoću računala. Autor ovog članka nastavlja se na mišljenje nekih hrvatskih autora kako se pojam cyber odgovarajuće može prevesti pojmom kibernetski, stoga će se taj pojam koristiti u ovom članku.

Kibernetski prostor

U listopadu 2006. Združeni stožer oružanih snaga SAD-a definirao je kibernetski prostor kao „područje koje karakterizira upotreba elektroničkog i elektromagnetskog dijapazona za pohranjivanje, modificiranje i razmjenjivanje podataka putem mrežnih sustava i povezanih fizičkih infrastruktura“.[10] Korisnici kibernetskog prostora poput domaćinstva, korporacija, sveučilišta, vlada, oružanih snaga itd. kreću se kibernetskim prostorom kako bi izgradili ili dostigli informacijska odredišta koja se dijele, stječu i nadziru putem mrežnih sustava u kojima povezanost čine obične telefonske linije, mikrovalni uređaji, satelitske uzlazne i silazne veze, optička vlakna, kablovi, tranzistori i mikročipovi.[11] Internet je najpoznatiji i najrasprostranjeniji

---

znači upravljati. Moderno korištenje pojma kibernetika počelo je u vrijeme Drugog svjetskog rata. Sam pojam kibernetika (engl. Cybernetics, fran. Cybernetique, njem. Kvbernetik) skovao je matematičar Norbert Wiener u istraživanju teleologičkih mehanizama, a popularizirao ga je u knjizi “Cybernetics, or control and communication in the animal and machine” objavljenoj 1948. Drugi smjer iz kojeg se razvio pojam “cyber” je književnost. Riječ “cyberpunk” prvi se put pojavila u kratkoj priči “Cyberpunk” autora Brucea Bethkea, a objavljena je 4. studenog 1983. u magazinu “Amazing” koji objavljuje znanstvenofantastične priče.

8 Goran Vojković i Marija Štambuk-Sunjić s Pravnog fakulteta u Splitu u članku „Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske“, Zbornik radova Pravnog fakulteta u Splitu, Vol.43 No.1, Split, 2006.

9 Deutsch, Karl W.: The Nerves of Government: Moñels of Political Communication and Control, 2nd ed.. New York, 1966., str. 76.

10 Michael W. Wynne: Cyberspace as a Domain in Which the Air Force Flies and Fights, govor s C4ISR Integration Conference 2006., dostupno na http://www.af.mil/library/speeches/speech.asp?id=283

11 Natasha Solce „The Battlefield of Cyberspace: The inevitable New Military Branch—The Cyber Force“ u Journal of Science & Technology, 293, Albany Law School, 2008.

mrežni sustav. U kibernetskom prostoru, informacije su dostupne u realnom vremenu i njihova bitna odrednica postaje temporalnost, ovisnost o vremenu, a ne o prostoru. Za brze promijene u kibernetskom prostoru potrebno je vrlo malo vremena.[12]

Ugroze u kibernetskom prostoru - podjela

Maliciozne kibernetske aktivnosti dijele se na: 1. kibernetski kriminal, 2. kibernetsku špijunažu, 3. kibernetski terorizam i 4. kibernetsko ratovanje.

Kibernetski napadi javljaju se u dvije forme s obzirom na njihov cilj: (1) napad usmjeren na podatke i (2) napad usmjeren na nadzorne sustave. Krađa i kvarenje podataka dovodi do sabotiranja usluga i to je čest oblik napada putem Interneta i računala. Napadi koji su usmjereni na kontrolne sustave koriste se sa svrhom manipuliranja fizičkom infrastrukturom (npr. opskrbom električnom energijom, željezničkim prometom ili vodnim zalihama). To se čini na način da se putem Interneta ili drugačije penetrira u sustave. Tako je, na primjer, u ožujku 2000. bivši zaposlenik preko Interneta neovlašteno ušao u elektronički nadzorni sustav pumpi i otpustio milijun litara otpadnih voda u vodni sustav Maroochy Shire u Queenslandu, u Australiji.[13] Trebalo mu je 45 pokušaja da uspješno penetrira u sustav. Dakle, 44 pokušaja ostala su nezamijećena.[14] Jedanaest godina kasnije pojavile su se prve analize Stuxneta, visoko sofisticiranog oblika malicioznog koda sposobnog djelovati neopaženo protiv industrijskih nadzornih sustava dok uništava zadane ciljeve, te kojem više nije potreban Internet da bi inficirao željeni sustav.[15]

12 Uzimajući u obzir temporalnost informacija u kibernetskom prostoru, Rain Ottis, Peeter Lorents s Cooperative Cyber Defence Centre of Excellence, iz Tallinna, iz Estonije u članku „Cyberspace: Definition and Implications“ 2010. predlažu definiciju: kibernetski prostor je o vremenu ovisan niz međupovezanih informacijskih sustava i ljudskih korisnika koji su u interakciji s tim sustavima. Članak dostupan na http://www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf

13 Dawson, Robert Edward: Secure communications for critical infrastructure control systems, Masters by Research thesis, Queensland University of Technology, 2008.

14 Kako su dijelovi kritičnih infrastruktura sve više u vlasništvu privatnih tvrtki, postavlja se pitanje sigurnosne svijesti tih tvrtki, kao i nametanja sigurnosnih standarda.

15 Stuxnet je programiran tako da napada SCADA sustave (Supervisory control nad dana acquisitin) koji zadovoljavaju određene kriterije. Ako su kriteriji na zaraženom sustavu zadovoljeni, Stuxnet će preuzeti industrijski nadzorni sustav i izazvati pokvariti i uništit ciljanu opremu.

Potrebno je istaknuti kako fizički oblici kibernetskog terorizma, kibernetskog ratovanja, kibernetske špijunaže i kibernetskog kriminala često izgledaju isto ili slično.

Lech J. Janczewski i Andrew M. Colarik navode primjer kada netko provali u bolničku bazu podataka i prepiše lijek pacijentu koji je alergičan na taj lijek. Kao rezultat, pacijent umire. Ako je namjera napadača bila nauditi pacijentu ili ubiti ga iz nekih osobnih razloga, riječ je o kaznenom djelu ubojstva izvedenom pomoću računalne tehnologije, dakle o kibernetskom kriminalu. Ako napadač kasnije obznani kako je spreman učiniti još takvih djela, ukoliko mu se ne ispune neki zahtjevi, riječ je o kibernetskom terorizmu. No, ako je taj napadač još i agent strane protivničkih struktura, tada se djelo može označiti kao kibernetsko ratovanje.

Dakle, tek je namjera napadača ono što djelo može okarakterizirati kao kibernetski terorizam, kibernetski rat ili kibernetski kriminal.

Kibernetski terorizam

Kibernetski terorizam označava promišljene, političke motivirane napade izvršene od strane nacionalnih skupina ili prikrivenih čimbenika, odnosno pojedinaca, usmjerene protiv informacijskih ili računalnih sustava, računalnih programa, te podataka, a koji rezultiraju nasiljem nad neborbenim metama.[16] U kolovozu 1997. teroristička skupina Internet Black Tigers (IBT), specijalna frakcija Oslobodilačkih tigrova tamilske domovine, nasilne nacionalističke skupine iz Sri Lanke posvećene stvaranju nezavisne države etničkih Tamila, napala je e-mail sustave nekoliko veleposlanstava Sri Lanke diljem svijeta. Preplavljujući te email račune s oko 800 emailova na dan, IBT je onesposobio mrežu veleposlanstava skoro dva tjedna. Poslani e-mailovi sadržavali su sljedeću poruku „We are the Internet Black Tigers and we're doing this to interrupt your communications". Skupina je izjavila kako je cilj napada suprotstavljanje promidžbi vlade Sri Lanke. Iako ovaj napad nije prouzročio u bilo kojem smislu velike gubitke, mnogi stručnjaci za terorizam smatraju ga značajnim događajem budućeg razvoja kibernetskog terorizma i terorističkih

16 Prvu definiciju ponudio je američki Center for the Study of Terrorism and Irregular Warfare, Monterey, CA u studiji „Cyberterror: Prospects and Implications" izrađenoj 1999. za potrebe Defense Intelligence Agency: "Kibernetski terorizam (eng. Cyber terrorism) je protupravno uništavanje ili ometanje digitalnog vlasništva u pokušaju zastrašivanja ili prisiljavanja vlada ili društava kako bi se ostvarili politički, religijski ili ideološki ciljevi."

metoda, a obavještajne zajednice smatraju ga prvim napadom na mreže jedne zemlje.[17] Od tada do danas zabilježeni su brojni slučajevi kibernetskih terorističkih napada.

Kao podvrsta terorizma, kibernetski terorizam koristi informatiku kao oružje, metodu ili metu kako bi se postigao teroristički cilj. Kibernetski terorizam odvija se u kibernetskom prostoru, ali uključuje fizičko uništavanje nekog uređaja, sustava uređaja ili nekog procesa u kojem sudjeluje informatička komponenta. Značajna karakteristika kibernetskog terorizma je prednost da, s obzirom na uloženo, poluči nerazmjeran učinak u uništavanju, uskraćivanju, obmanjivanju, krvarenju, iskorištavanju i remećenju.

S obzirom da su teroristi ograničenih sredstava, za pretpostaviti je kako ih kibernetski napadi sve više privlače, jer zahtijevaju manje ljudstva i manje resursa, dopuštaju fizičku odsutnost od mjesta napada, kao i veću mogućnost da napadači ostanu nepoznati, a u kombinaciji s klasičnim terorističkim napadom[18] povećavaju učinkovitost terora.[19]

Kibernetski rat

Kibernetski rat (eng. Cyberwar ili Cyberwarfare) prema enciklopediji Britannica rat je koji se vodi pomoću računala i mreža koje ih povezuju. Poduzet je od strane država ili drugih od njihove strane angažiranih subjekata protiv drugih država.[20] Kibernetsko ratovanje najčešće se provodi protiv vladinih i vojnih mreža sa svrhom ometanja, uništavanja ili onemogućavanja njihove upotrebe. Kibernetsko ratovanje ne bi se trebalo poistovjetiti s terorističkih korištenjem kibernetskog prostora, niti s kibernetskom špijunažom, a ni s

17 http://www.start.umd.edu/start/data_collections/tops/terrorist_organization_profile.asp?id=4062

18 Pokazalo se kako je kombiniranje kibernetskog terorizma s fizičkim najučinkovitije korištenje kibernetskog terorizma. Na primjer, onemogućavanjem komunikacijskog sustava hitnih službi tijekom fizičkog terorističkog napada, povećao bi se učinak fizičkog napada.

19 No, svaka uporaba informatičke tehnologije od strane terorista ne može se klasificirati kao kibernetski terorizam. Definicije kibernetskog terorizma i kibernetsko-terorističke potpore ne uključuju zakonitu upotrebu informatičke tehnologije. Iako zakonita upotreba informatičkih tehnologija može pospješiti komunikaciju među teroristima ili povećati koordiniranost terorističke skupine, prema definicijama takva upotreba ne spada u kibernetski terorizam.

20 Često se koristi i pojam „informatički rat“. Autor ovog rada mišljenja je kako je to neprecizan pojam s obzirom da on implicira korištenje informatičke tehnologije u svrhu vođenja rata, no ne i nužno ratovanje u kibernetskom prostoru, a što je krucijalno za kibernetski rat.

kibernetskim kriminalom. Iako se slične taktike koriste u sva četiri oblika djelovanja, pogrešno bi bilo sve ih definirati kao djela kibernetskog ratovanja. Neke države koje su se upustile u kibernetsko ratovanje, mogle bi se također upustiti i u razorne djelatnosti kao što je kibernetska špijunaža, no te djelatnosti same po sebi ne čine kibernetski rat.

Često se kibernetski rat poistovjećuje s informacijskim ratom i informatičkim ratom. Informacijski rat predstavlja postupke poduzete kako bi se postigla informacijska superiornost utjecanjem na informacije protivnika, procese temeljene na informacijama, informacijske sustave i računalne mreže dok se u isto vrijeme brane vlastite informacije, procesi temeljeni na informacijama, informacijski sustavi i računalne mreže.[21] Dakle, može se reći kako je kibernetski rat dio informacijskog rata (ostali dijelovi su primjerice promidžbeni rat, psihološki rat itd.).

Informatički rat prema mišljenju autora ovog članka nepotreban je pojam koji unosi zbrku u literaturu. Informatički rat implicira kako je riječ o ratu koji se vrši pomoću informatičke tehnologije, a kako se gotovo svako moderno bojno djelovanje vrši pomoću informatičke tehnologije, besmisleno je govoriti o informatičkom ratu.

Primjeri kibernetskog rata su takozvani Prvi mrežni rat (eng. Web War 1) u kojem su 2007. u Estoniji DDOS-om napadani serveri estonske vlade, ministarstava, medija, banaka i tvrtki, što je rezultiralo isključivanjem tih subjekata s Interneta na određeno vrijeme, te vrlo sličan ruski napad na servere kojim su se koristila brojna vladina tijela, mediji i poslovni subjekti Gruzije, a koji je tekao istovremeno s bojnim djelovanje ruskih snaga spram gruzijskih.[22]

Kibernetski kriminal

Uz prethodna dva pojma postoji i pojam kibernetski kriminal, koji se definira kao kriminal izveden pomoću računalne tehnologije, a u kibernetskom prostoru. Kibernetski kriminal obuhvaća prijevare na polju internetskog bankarstva i prijevare na Internetu s kreditnim karticama, a procjenjuje se kako je s godišnjom stopom rasta od oko 40 posto i s trenutnom zaradom od oko 100 milijardi dolara riječ o

21 The Chairman of the Joint Chiefs of Staff Instruction (CJCSI), broj 3210.01, 2. siječnja 1996.

22 DDOS (eng. Distributed Denial-of-service) – napad kojim se sprječava pristup računalom sustavu koristeći preopterećivanje računalne mreže slanjem mnogostrukih zahtjeva prema poslužitelju, tako da se zaustavi legitimni promet prema tim poslužiteljima.

najbrže rastućem sektoru globalnog organiziranog kriminala. Potrebno je naglasiti da pod pojam kibernetska kaznena djela treba svrstavati samo kaznena djela kod kojih je uporaba računala ili računalne mreže bitna za biće kaznenog djela, a ne sva kaznena djela u kojima se na neki način kao sredstvo izvršenja pojavljuje računalo s pripadnom perifernom opremom. Tako primjerice kazneno djelo krivotvorenja novca ne spada pod kibernetski kriminal bez obzira što se počinitelj prilikom krivotvorenja novca služio računalnom tehnologijom.

Regulativni okvir sustava borbe protiv kibernetskih prijetnji u RH

Može se reći kako u RH ne postoji uspostavljen jedinstven sustav borbe protiv kibernetskih prijetnji koji bi djelovao na svim onim razinama i u svim dijelovima kritične infrastrukture gdje te prijetnje postoje, no postoje različiti sigurnosni sustavi pod čije područje djelovanja spada i borba protiv kibernetskih prijetnji. Primjerice, subjekti unutar bankarskog sektora posjeduju vlastite sigurnosne sustave, pa tako i sustave borbi protiv kibernetskih prijetnji. Ti sustavi ne oslanjaju se na druge (npr, državne) sigurnosne sustave.[23] Regulativni okvir sustava borbe protiv kibernetskih prijetnji u RH, koji se tiče državnih i javnih informacijskih sustava, predstavlja skup propisa koji se svrstavaju pod regulativni okvir koji uređuje informacijsku sigurnosti, a čije je donošenje u nadležnosti državnog sektora. Prije prikaza zakona i pravnih propisa potrebno je istaknuti kako ti propisi fenomene kibernetskih prijetnji u toj formulaciju ne spominju, no može se reći kako oni predstavljaju temelj za uspostavu sustava borbe protiv kibernetskih prijetnji.

Prije navođenja nacionalnih zakona i propisa, važno je istaknuti značaj i mjesto koje u hijerarhiji propisa zauzimaju multilateralni i bilateralni ugovori koji se tiču područja informacijske sigurnosti, tehničke zaštite, odnosno informatičke sigurnosti, a koje Republika Hrvatska sklapa s drugim državama i međunarodnim organizacijama. Prije svega ovdje treba spomenuti Konvenciju o kibernetskom kriminalitetu Vijeća Europe. Konvencija o kibernetskom

23 Kako je jedna od temeljnih postavki suvremenog društveno-političkog uređenja nemiješanje države u područje privatnog biznisa, a kako je u velikoj mjeri kritična infrastruktura RH u privatnom vlasništvu, otvara se pitanje sigurnosti te infrastrukture. Privatne tvrtke motivirane su profitom, a sigurnosni sustavi, ako ih za poslovanje ne smatraju neophodnim, mogu tvrtkama iziskivati određene troškove i tako umanjiti zaradu.

kriminalu iz 2001. prvi je međunarodni ugovor o zločinima počinjenima putem Interneta i drugih računalnih mreža. Posebno se bavi kršenjem autorskih prava, računalnim prijevarama, dječjom pornografijom i povredama sigurnosti mreže. Ona također sadrži niz ovlasti i postupaka za povećanje razine informacijske i mrežne sigurnosti.[24] Glavni cilj konvencije nastavak je zajedničke kaznene politike usmjerene na zaštitu društva od kibernetskog kriminala (eng. cyber crime), a posebno usvajanje odgovarajućeg zakonodavstva i jačanje međunarodne suradnje. Nadopunjena je dodatnim protokolom koji svako objavljivanje i promidžbu rasizma i ksenofobije putem računalnih mreža označava kao kazneno djelo. Do danas, Konvenciju je ratificiralo 37 zemalja, a 10 ju je potpisalo bez ratifikacije. Republika Hrvatska ratificirala je Konvenciju te njezine odredbe unijela u svoj Kazneni zakon donošenjem Zakona o izmjenama i dopunama kaznenog zakona, a koji je stupio na snagu 1. listopada 2004. Zakoni kojima se propisuju okviri, ciljevi i dosezi sigurnosne politike u području informacijske, a tako i kibernetske, sigurnosti su Zakon o sigurnosno-obavještajnom sustavu (NN 79/06 i 105/06), Zakon o tajnosti podataka (NN 79/07), Zakon o informacijskoj sigurnosti (NN 79/07), Zakon o zaštiti osobnih podataka (NN 41/08), Zakon o tajnosti podataka (NN 79/07), Zakon o elektroničkoj trgovini (NN 173/03), Zakon o elektroničkim komunikacijama (NN 73/08) i Zakon o kaznenom postupku. Uredba Vlade RH kojom se propisuju i mjere kibernetske sigurnosti je Uredba o mjerama informacijske sigurnosti (NN 46/08).

Slijede pravilnici UVNS-a, koji imaju podzakonsku razinu i obvezu primjene na nacionalnoj razini: Pravilnik o standardima sigurnosti podataka, Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava i Pravilnik o standardima sigurnosti poslovne suradnje (UVNS, svibanj 2008., Neklasificirano).

Ispod regulativnog okvira, kojim se propisuje sigurnosna politika, implementacijski je okvir s odredbama koje se odnose na provedbenu politiku. Tu spadaju pravilnici kojima se propisuju standardi tehničkih područja sigurnosti informacijskih sustava. To su pravilnici ZSIS-a: Pravilnik o standardima sigurnosti informacijskih sustava, Pravilnik o postupanju s kriptografskim dokumentima i kriptografskom opremom za zaštitu klasificiranih podataka, Pravilnik o prevenciji i odgovoru na računalno-sigurnosne ugroze i

24 Pregled EU propisa na području informacijske sigurnosti, Centar informacijske sigurnosti, travanj 2012.

Pravilnik o sigurnosnoj akreditaciji (ZSIS, kolovoz/studeni 2008., Neklasificirano) te pravilnici nCERT-a, naputci i upute UVNS-a, ali i interni akti pojedinih tijela, čija obveza donošenja proizlazi iz zakonskih i podzakonskih akata kojima se propisuje sigurnosna politika.

Informacijska sigurnost i kibernetske prijetnje

Prema Zakonu o informacijskoj sigurnosti informacijska sigurnost „je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda“.[25] Područja informacijske sigurnosti su: sigurnosne provjere, sigurnost podataka, fizička sigurnost, sigurnost informacijskih sustava i sigurnost poslovne suradnje. Može se reći kako se u Zakonu o informacijskoj sigurnosti, u članku 2. navodi…“Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini“, a pojam „tehnička razina“ odnosi, među ostalim, i na mjere koje čine sustav borbe protiv kibernetskih prijetnji. U okvire te „tehničke razine“ spada informatička sigurnost.[26]

Informatička sigurnost samo je jedan dio informacijske sigurnosti koji se bavi tehnološkom zaštitom (npr. antivirusi, vatrozidovi, kriptiranje i sl.). Međutim informatička sigurnost ne pokriva npr. upravljanje ljudima koji su često vrlo velik izvor rizika itd. Drugim riječima, informacijska sigurnost skup je raznih aktivnosti koje uključuju organizacijske i pravne metode, upravljanje ljudskim resursima, fizičku i tehničku zaštitu, informatičku (IT) sigurnost itd.[27] Dakle, tehnička razina realizacije mjera informacijske sigurnosti, odnosno informatička sigurnost, pojmovi su koji grade i sustav borbi protiv kibernetskih prijetnji.

Sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj

Tijela u RH u čiji djelokrug, između ostalog, spada i provedba i borba protiv kibernetskih prijetnji su Ured Vijeća za nacionalnu sigurnost (UVNS), Zavod za sigurnost

25 Zakon o informacijskoj sigurnosti, Narodne novine, broj 79/07
26 Isto.
27 http://www.sigurnost.info/sta-pitanja-topmenu-48/7-faq-s/158-da-li-su-informacijska-sigurnost-i-informati-sigurnost-iste-stvari

informacijskih sustava (ZSIS), Nacionalni CERT (nCERT), Odjel za visokotehnološki kriminalitet Ministarstva unutarnjih poslova, te i regionalno Središte za kibernetsku sigurnost unutar Centra za sigurnosnu suradnju RACVIAC.

Ured Vijeća za nacionalnu sigurnost[28]

Ured Vijeća za nacionalnu sigurnost središnje je državno tijelo RH za informacijsku sigurnost – hrvatski (eng. NSA - National Security Authority), iz čega proizlaze njegove nacionalne i međunarodne obveze i nadležnosti u području informacijske sigurnosti, pa tako i kibernetske sigurnosti. U tom smislu, UVNS propisuje, koordinira i usklađuje donošenje te nadzire primjenu mjera i standarda informacijske sigurnosti u okviru područja sigurnosnih provjera, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacijskih sustava i sigurnosti poslovne suradnje (kao tijelo nadležno za komunikaciju s privatnim sektorom, hrvatski DSA - Designated Security Authority). U području sigurnosti informacijskih sustava UVNS je nadležan za organizaciju i upravljanje područjem sigurnosti informacijskih sustava (politika), ZSIS za tehničku implementaciju (provedbu) u segmentu tehničkih standarda sigurnosti informacijskih sustava, sigurnosnih akreditacija klasificiranih informacijskih sustava, upravljanja kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka te koordinaciji prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava u državnim tijelima (Vladin CERT), dok je CARNet (Nacionalni CERT) zadužen za provedbu prevencije i zaštite od ugroza sigurnosti javnih informacijskih sustava.

Nadalje, UVNS izdaje nacionalne, NATO i EU sigurnosne certifikate za fizičke osobe te certifikate poslovne sigurnosti za pravne osobe, nužne za pristup nacionalnim, NATO i EU klasificiranim podacima stupnja tajnosti „Povjerljivo“, „Tajno“ ili „Vrlo tajno“. UVNS koordinira i usklađuje rad svih drugih tijela koja imaju određene funkcije u sklopu politike informacijske sigurnosti. Od posebnog značaja kada se radi o kibernetskoj sigurnosti potrebno je spomenuto koordinaciju rada ZSIS-a, te CARNet-a (Hrvatska akademska i istraživačka mreža) odnosno Nacionalnog CERT-a.[29]

UVNS ima obvezu trajno usklađivati propisane mjere i standarde informacijske sigurnosti u RH s međunarodnim

28 Vidi Zakon o sigurnosno-obavještajnom sustavu RH, NN 79, 2006.
29 National Computer Emergency Response Team

standardima i preporukama informacijske sigurnosti te sudjelovati u nacionalnoj normizaciji područja informacijske sigurnosti.[30]

Zavod za sigurnost informacijskih sustava (ZSIS)[31]

ZSIS je središnje državno tijelo za tehnička područja sigurnosti informacijskih sustava u državnim tijelima, tijelima jedinica lokalne i područne (regionalne) samouprave te u pravnim osobama s javnim ovlastima, koje u svom djelokrugu koriste klasificirane podatke. Tehnička područja sigurnosti informacijskih sustava obuhvaćaju standarde sigurnosti informacijskih sustava, sigurnosne akreditacije klasificiranih informacijskih sustava, upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka te koordinaciju prevencije i odgovore na računalne ugroze sigurnosti informacijskih sustava u državnim tijelima (Vladin CERT). ZSIS trajno usklađuje standarde tehničkih područja sigurnosti informacijskih sustava u RH s međunarodnim standardima i preporukama te sudjeluje u nacionalnoj normizaciji područja sigurnosti informacijskih sustava. Može se reći kako je CERT ZSIS-a ono tijelo koje provodi borbu protiv kibernetskih ugroza u onim tijelima nad kojim ZSIS ima nadležnost. U djelokrug rada CERT ZSIS-a spada u prvom redu pružanje pomoći tijelima državne vlasti u Republici Hrvatskoj u primjeni preventivnih mjera (proaktivno djelovanje) s ciljem smanjenja rizika od računalno-sigurnosnih incidenata te, u slučaju nastanka istih, njihovo otklanjanje odnosno posredovanje pri otklanjanju (reaktivno djelovanje).[32] CERT tim ZSIS-a registriran je 21. travnja 2009. godine od strane organizacije Trusted Introducer u TF-CSIRT mreže CERT timova.[33]

CERT ZSIS-a održava i koordinira komunikaciju s abuse službama (abuse eng. zloupotreba, kršenje sklopljenog dogovora) davatelja usluga pristupa Internetu u Hrvatskoj, kao i s predstavnicima pravosuđa i policije.[34]

30 Zakon o informacijskoj sigurnosti, Narodne novine, broj 79/07

31 Vidi Zakon o sigurnosno-obavještajnom sustavu RH, NN 79, 2006.

32 Računalno-sigurnosni incident je, prema definiciji iz Pravilnika o koordinaciji prevencije i odgovora na računalno-sigurnosne incidente, svaki događaj koji kompromitira bilo koji aspekt računalne sigurnosti, odnosno koji za posljedicu ima gubitak povjerljivosti, cjelovitosti i raspoloživosti podatka, zlouporabu ili oštećenje informacijskog sustava ili informacija, uskraćivanje usluge ili onemogućavanje rada informacijskog sustava te svaka nezakonita radnja čiji se dokazi mogu pohraniti na računalni medij.

33 Task Force -Computer Security Incident Response Teams

34 Zakon o informacijskoj sigurnosti, Narodne novine, broj 79/07

Nacionalni CERT

Nacionalni CERT osnovan je u skladu sa Zakonom o informacijskoj sigurnosti RH s ciljem prevencije i zaštite od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj. Prema Pravilniku o radu Nacionalnog CERT-a, on se bavi incidentom, ako se jedna od strana u incidentu nalazi u RH (odnosno, ako je u .hr domeni ili u hrvatskom IP adresnom prostoru).

Nacionalni CERT u okviru svog djelovanja provodi proaktivne i reaktivne mjere. Proaktivnim mjerama djeluje prije incidenta i drugih događaja koji mogu ugroziti sigurnost informacijskih sustava, a u cilju sprečavanja ili ublažavanja mogućih šteta. Informacije o proaktivnim mjerama javno se objavljuju. Reaktivnim mjerama djeluje se na incidente u Republici Hrvatskoj te druge događaje koji mogu ugroziti računalnu sigurnost javnih informacijskih sustava u Republici Hrvatskoj. Nacionalni CERT surađuje s relevantnim tijelima (Zavod za sigurnost informacijskih sustava - ZSIS CERT, Ured Vijeća za nacionalnu sigurnost i Ministarstvo unutarnjih poslova RH), a također i sa stranim CERT-ovima preko članstva u Forum of Incident Response and Security Teams (FIRST) i radnoj skupini Task Force - Computer Security Incident Response Teams (TF-CSIRT). NCERT i ZSIS surađuju na prevenciji i zaštiti od računalnih ugroza sigurnosti informacijskih sustava te sudjeluju u izradi preporuka i normi iz područja informacijskih sustava u Republici Hrvatskoj.

Odjel za visokotehnološki kriminalitet

Unutar Službe gospodarskog kriminaliteta i korupcije Uprave kriminalističke policije Ministarstva unutarnjih poslova RH ustrojen je Odjel za visokotehnološki kriminalitet. Ovaj Odjel „sustavno analizira, prati i izučava fenomenološki i etiološki aspekt kaznenih djela kibernetičkog[35] (računalnog) kriminaliteta, te predlaže rješenja na planu podizanja razine učinkovitosti rada u suzbijanju kibernetičkog kriminaliteta; neposredno provodi složena kriminalistička istraživanja u području kaznenih djela počinjenih na štetu i pomoću računalnih sustava i mreža; obavlja forenzičku analizu i nadzor interneta; pruža specijaliziranu potporu drugim

35 Iako autor ovog članka pridjev cyber prevodi pridjevom kibernetski, u ovom citati iz Uredbe o unutarnjem ustrojstvu Ministarstva unutarnjih poslova (NN 070/2012) ostavljeni su izvorni pojmovi.

ustrojstvenim jedinicama policije; surađuje s drugim ustrojstvenim jedinicama Ministarstva, tijelima državne uprave i pravnim osobama, policijama drugih zemalja i međunarodnim institucijama u svom djelokrugu rada; sudjeluje u planiranju i izradi programa obuke policijskih službenika u čijem je djelokrugu rada problematika kibernetičkog kriminaliteta; sudjeluje u izradi normativnih akata, izvješća i drugih stručnih materijala iz područja kibernetičkog kriminaliteta te obavlja i druge poslove iz svoga djelokruga rada".[36] Ovaj Odjel središnja je jedinica za postupanje po kaznenim djelima na koja se odnosi Konvencija o kibernetičkom kriminalu i Protokol uz Konvenciju, koji se odnosi na širenje rasističkih i ksenofobnih sadržaja putem računalnih sustava (potpisan 28. siječnja 2003.). Zakonom o kaznenom postupku obuhvaćena su sva kaznena djela na koja se odnosi Konvencija i uz nju vezan Protokol. Također, RH je ratificirala i Fakultativni protokol uz Konvenciju o pravima djeteta, o prodaji djece, dječjoj prostituciji i dječjoj pornografiji (NN MU 5/02). Izmjenama Zakona o kaznenom postupku iz 2006. godine (NN 115/06) proširena je primjena izvidnih mjera (članak 180. ZKP) i na kaznena djela dječje pornografije na računalnom sustavu ili mreži, kaznena djela povrede tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava, kaznena djela računalnog krivotvorenja i kaznena djela računalne prijevare.

Regionalno središte za kibernetsku sigurnost

U Centru za sigurnosnu suradnju RACVIAC, od 12. do 14. prosinca 2011. održan je Radni stol pod nazivom „Cyber security project".[37] Na skupu je bilo oko 50-tak stručnjaka iz područja kibernetske sigurnosti, kao i predstavnici institucija zemalja Jugoistočne Europe, a na kojem je dogovoreno kako će RACVIAC, po uzoru na slična svjetska središta, u buduće služiti i kao regionalno središte za kibernetsku

36 Uredba o unutarnjem ustrojstvu Ministarstva unutarnjih poslova (NN 070/2012)

37 Na radnom stolu su međunarodno priznati stručnjaci s tog područja održali prezentacije. Među njima su bili predstavnici UN-ovog istraživačkog instituta za međuregionalni kriminal i pravdu (UNICRI), NATO-a, Centra za provedbu zakona u Jugoistočnoj Europi (SELEC), Mornaričke službe za kriminalističke istrage SAD-a (NCIS), Vijeća za regionalnu suradnju, Cyber DefCon-a, Saveznog ministarstva obrane i sporta Savezne Republike Austrije i Transformacijskog centra oružanih snaga Savezne Republike Njemačke.

sigurnost regije Jugoistočne Europe.[38] Na tragu posljednjih zbivanja i aktivnosti na međunarodnom planu i u regiji Jugoistočne Europe, koja se prepoznala kao regija s rastućim opsegom malicioznih kibernetskih aktivnosti, dok prema zaključcima sudionika radnog stola kibernetska sigurnost u zemljama regije nije na zadovoljavajućoj razini, javlja se potreba uspostavljanja regionalnog središta za kibernetsku sigurnost. U prvoj fazi, u središtu bi se provodile edukacijske i akademske aktivnosti, a druga bi uključivala edukativne i istraživalačke aktivnosti. Takva djelatnost omogućila bi regionalnim stručnjacima iz područja kibernetske sigurnosti da se, zajedno sa stručnjacima izvan regije JI Europe, susreću i razmjenjuju iskustva, znanja i najbolje prakse. Najznačajnija konkretna dobit uspostavljanja takvog centra za zemlje regije Jugoistočne Europe bila bi unapređivanje sposobnosti vlastitih stručnjaka iz područja kibernetske sigurnosti da se brže i usklađenije suprotstave ugrozama u kibernetskom prostoru, da ih neutraliziraju, ili umanje njihovu razornost. U širem smislu, to će dovesti do povećanja sigurnosne suradnje u regiji Jugoistočne Europe, što je razlog zbog kojeg je RACVIAC i osnovan. Prva takva aktivnost održana je u rujnu 2012. pod pokroviteljstvom NATO-vog Programa znanost za mir kao radni stol regionalnih i svjetskih stručnjaka s područja kibernetske sigurnosti, članova državnih institucija i međunarodnih organizacija, kao i akademske zajednice pod nazivom „Cyber defence strategies and policies“.

Zaključak

Republika Hrvatska, iako svojim zakonodavstvom ne uspostavlja zaseban sustav sigurnosti kibernetskog prostora, niti poznaje pojmove vezane uz kibernetsku sigurnost (izuzev kibernetskog kriminala), može se ocijeniti kako njegovu sigurnost provodi uglavnom kroz sustav informacijske sigurnosti. U okvir tehničke razine mjera informacijske sigurnosti spada i informatička sigurnost, što je u hrvatskom sustavu informacijske sigurnosti najbliži pojam

38 Održavanje ovog radnog stola u RACVIAC-u svjedoči kako je i u regiji Jugoistočne Europe podignuta svijest o ozbiljnosti ugroza u kibernetskom prostoru, koje uopće ne poznaju granice. Štoviše, regija Jugoistočne Europe prepoznata je kao regija s rastućim opsegom kibernetskog kriminala, dok se procjenjuje kako općenito kibernetska sigurnost u zemljama regije nije na zadovoljavajućoj razini. U tom smislu, zemlje regije moraju početi s pripremama kako bi bile u stanju odgovoriti na te prijetnje, a te pripreme moraju biti orijentirane prema budućnosti.

pojmu kibernetske sigurnosti. U području, dakle informacijske sigurnosti, koje dijelom obuhvaća kibernetsku sigurnost, UVNS je nadležan za organizaciju i upravljanje područjem sigurnosti informacijskih sustava (politika), ZSIS za tehničku implementaciju (provedbu) u segmentu tehničkih standarda sigurnosti informacijskih sustava, sigurnosnih akreditacija klasificiranih informacijskih sustava, upravljanja kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka, te koordinaciji prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava u državnim tijelima (Vladin CERT), dok je CARNet (Nacionalni CERT) zadužen za provedbu prevencije i zaštite od ugroza sigurnosti javnih informacijskih sustava. U Centru za sigurnosnu suradnju RACVIAC uz potporu NATO-vog Programa znanost za mir uspostavljen je regionalno Središte za kibernetsku sigurnost regije Jugoistočne Europe, kao edukacijsko-akademska platforma za razmjenu znanja, iskustva i najbolje prakse. Unutar Uprave kriminalističke policije Ministarstva unutarnjih poslova RH ustrojen je Odjel za visokotehnološki kriminalitet, ustrojstvena jedinica koja analizira, prati i izučava fenomenološki i etiološki aspekt kaznenih djela kibernetskog kriminaliteta, te suzbija kibernetski kriminal provodeći složena kriminalistička i forenzička istraživanja u području kaznenih djela počinjenih na štetu i pomoću računalnih sustava i mreža. Može se ocijeniti kako u djelokrug rada tog odjela spada kibernetska sigurnost u onom dijelu koji se prije svega odnosi na kibernetski kriminal. Slijedom prikazanog ostaje pitanje odgovara li takav necentraliziran sustav kibernetske sigurnosti koji djeluje u okviru drugih sigurnosnih sustava ozbiljnosti ugroza u kibernetskom prostoru, te hoće li RH, kao članica međunarodnih organizacija koje sve više paže posvećuju kibernetskoj sigurnosti, posebno Organizacije sjevernoatlantskog ugovora, u skoroj budućnosti promijeniti pristup kibernetskoj sigurnosti, te kakav će taj pristup biti.

Literatura

Anić V., Goldstein I., *Rječnik stranih riječi*, Novi Liber, Zagreb, 2005.

Choi R., Gangnon G., Iacobucci M., Mitchell M., Nelson B., *Cyberterror: Prospects and Implications*, Center for the Study of Terrorism and Irregular Warfare, Monterey, CA

Colarik A. M., Lech J. J., *Cyber Warfare and Cyber Terrorism,* IGI GLOBAL, Hershey, Pennsylvania 2008..

Cyberwar: War in the fifth domain, uvodnik, The Economist, London, 1.7.2010.

Dawson R. E., *Secure communications for critical infrastructure control systems*, Masters by Research thesis, Queensland University of Technology, 2008.

Deutsch K. W., *The Nerves of Government: Moñels of Political Communication and Control*, 2 izdanje, New York, 1966..

Konvencija o kibernetičkom kriminalitetu, Vijeće Europe, NN, Međunarodni ugovori broj 9, 2002.

Lynn W. J., *Defending a New Domain – The Pentagon's Cyberstrategy*, Foreign Affairs, Council on Foreign Relations, Tampa, FL, 2010.

Ottis R., Lorents P., *Cyberspace: Definition and Implications*, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonija, 2010.

Pregled EU propisa na području informacijske sigurnosti, Centar informacijske sigurnosti, travanj 2012.

Solce N.,*The Battlefield of Cyberspace: The inevitable New Military Branch—The Cyber Force* u Journal of Science & Technology, 293, Albany Law School, 2008.

Strateški koncept za obranu i sigurnost članica Organizacije sjevernoatlantskog sporazuma*,* Organizacija Sjevernoatlantskog ugovora, Lisabon 2010.

The Chairman of the Joint Chiefs of Staff Instruction, (CJCSI), broj 3210.01, 2. siječnja 1996.

Uredba o unutarnjem ustrojstvu Ministarstva unutarnjih poslova, NN 070/2012

Vojković G., Štambuk-Sunjić M., *Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske*, Zbornik radova Pravnog fakulteta u Splitu, Vol.43 No.1, Split, 2006.

Wynne M., W., *Cyberspace as a Domain in Which the Air Force Flies and Fights*, govor s C4ISR Integration Conference, Crystal City, Va. u The Air Force Magazine, The Air Force Association, Arlington,VA 2006.

Zakon o kaznenom postupku, NN broj 121, 2011.

Zakon o informacijskoj sigurnosti, NN, broj 79/07

Zakon o sigurnosno-obavještajnom sustavu RH, NN 79, 2006.

Internet poveznice

Košutić D., *Da li su informacijska sigurnost i informatička sigurnost iste stvari?*, URL: http://www.sigurnost.info/sta-pitanja-topmenu-48/7-faq-s/158-da-li-su-informacijska-sigurnost-i-informati-sigurnost-iste-stvari: pristup: 6. siječnja 2012.

The National Consortium for the Study of Terrorism and Responses to Terrorism, Centar izvrsnosti na University of Maryland za U.S. Department of Homeland Security: URL:http://www.start.umd.edu/start/data_collections/tops/terrorist_organization_profile.asp?id=4062, pristup: 6. siječnja 2012

URL:http://www.nsa.gov/about/faqs/terms_acronyms.shtml, pristup: 6. siječnja 2012.

URL:http://www.zsis.hr/site/CERTZSISa/Ukratko/tabid/65/Default.aspx, pristup: 6. siječnja 2012