Kaznenopravni aspekti kibernetičkog ratovanja

Rakonić, Isabella

REPUBLIKA HRVATSKA

SVEUČILIŠTE U ZAGREBU

P R A V N I F A K U L T E T

Student:

Isabella Rakonić

Naslov diplomskog rada:

KAZNENOPRAVNI ASPEKTI KIBERNETIČKOG RATOVANJA

Kolegij:

KAZNENO PRAVO

Mentor:

Doc. dr. sc. Aleksandar Maršavelski

Zagreb, srpanj 2019.

IZJAVA O IZVORNOSTI

Ja, Isabella Rakonić, izjavljujem da je ovaj rad izvorni rezultat mog vlastitog rada te da se u njegovoj izradi nisu koristili drugi izvori od onih navedenih u radu.

SADRŽAJ

1. UVOD

"Si vis pacem, para bellum" obično se prevodi "ako želite mir, pripremite se za rat".[1] Povijesno gledajući, rat se vodio na razne načine. Od korištenja velikih skupina vojnih snaga i sofisticirane tehnike i oružja, zatim domorodačkih snaga koje koriste prosto oružje do malih skupina boraca za slobodu koje su bile voljne boriti se protiv policije i cijele nacionalne vojske. Drugim riječima, rat dolazi u raznim oblicima i veličinama. Svake godine sve veći postotak ekonomije odlazi sa medija kao što su telefoni i telegrafi, na nove medije poput interneta i druge privatne ili polujavne mreže, a sustavi koji su nekoć bili nedostupni široj ljudskoj masi, kao što su kontrole u elektranama, sada su teoretski dostupni svima.[2] Iz tog razloga internet se pretvorio u potencijalno mjesto ratovanja. Hakeri putem kibernetičkog prostora napadaju informacijske sustave kako od državne tako i privatne važnosti. U najmanju ruku ti napadi svode se na krađu informacija, no namjera počinitelja ne staje uvijek isključivo na šteti u virtualnom prostoru već se može proširiti i na fizički svijet. Koristeći internet kao bojno polje, uz zadovoljavajuće financije i opremu, male skupine napadača mogu napasti industrijski sektor, grad ili čak državu te tako ozbiljno ugroziti gospodarsku aktivnost.[3] Time je internet učinio same strategije ratovanja jeftinijima, jednostavnijim za provedbu i konačno, upotrebljivim u svakom dijelu svijeta. Kibernetičke prijetnje i u Hrvatsku ulaze na velika vrata, na što ukazuju hakerski napadi na Ministarstvo vanjskih i europskih poslova.[4] Iako se hakeri nisu domogli traženih podataka, sama činjenica hakerskog napada ozbiljno ugrožava nacionalnu sigurnost. Koji zakon upravlja tim napadima? Razni autori takve i slične napade nazivaju "kibernetičkim ratovanjem" sugerirajući da se mogu primijeniti ratni zakoni. Ipak, kibernetički napadi ne izgledaju u potpunosti kao napadi tokom tradicionalnog rata. Suradnja na međunarodnom planu kao i razmjena obavještajnih podataka, ključni su za učinkovitu prevenciju kibernetičkih prijetnji i napada. Iako su kibernetičke prijetnje posljednjih godina često posebno naglašene u modernim vojnim doktrinama velikih sila i NATO-a, one su i dalje obavijene tajnom.[5] U odgovoru na kibernetičke prijetnje i napade, NATO Centar za suradnju u kibernetičkoj obrani pokrenuo je veliki istraživački projekt ispitivanja međunarodnog prava u sferi kibernetičkog rata i donio Priručnik o međunarodnom pravu koji se primjenjuje u

[1] Publius Flavius Vegetius Renatus, De re militari, 400. god pr. Kr.
[2] Libicki, Martin, *Conquest in Cyberspace: National security and information warfare*; Ujedinjeno Kraljevstvo, 2007.
[3] Erbschloe, Michael, Vacca, John, *Information warfare: How to survive cyber attacks*; SAD, 2001.
[4] Kezerić, Ana – Maria, Analiza prijetnji i rizika *cyber* sigurnosti Republike Hrvatske: Ranjivost informacijske sigurnosti; Zagreb 2017., str 2.
[5] Duić, Cvrtila, Ivanjko, *International cyber security challenges*; Republika Hrvatska 2017.

kibernetičkom ratovanju u Tallinu. Ovaj rad razmatra pitanje pravne regulative navedenog pojma kibernetičkog ratovanja, za kojeg i dalje ne postoji jedinstvena službena definicija. Prvo, rad pojašnjava što je kibernetički rat i što je i zašto je važna kibernetička sigurnost, te se fokusira na izgradnju zakonodavnog okvira kibernetičkog ratovanja. Razmatraju se nedavna međunarodna nastojanja da se direktno reguliraju kibernetički napadi, kao i već postojeća međunarodna regulativa. Drugo, rad razmatra pitanje kibernetičke sigurnosti u Republici Hrvatskoj te domaća tijela i kaznenopravnu regulativu primjenjivu na kibernetičko ratovanje. No, osnovna poruka je jednostavna: kibernetički prostor je vlastiti medij s vlastitim pravilima. Nešto što danas funkcionira neće nužno biti djelotvorno i sutra te se načela regulacije kibernetičkog ratovanja moraju stalno iznova promišljati.[6] Ovaj rad, između ostalog, je poticaj tog promišljanja.

2. PRAVNA REGULACIJA

2.1 Kibernetički rat i kibernetički napadi

"Kibernetsko ratovanje" postalo je zloslutna fraza koja se koristi posebno u medijima, ali i u kontekstu međunarodnog prava u različitim kontekstima koji nisu svi prikladni.[7] Uporaba i zlouporaba kibernetičkog prostora bez granica utječu na vitalne državne interese u fizičkom svijetu, uključujući nacionalnu sigurnost, javnu sigurnost ili gospodarski razvoj. Kao takav, kiberprostor se proteže daleko izvan domene unutarnjih poslova bilo koje države.[8] Ako se doslovno shvati, sve što je povezano u kibernetičkom prostoru može biti cilj - kao što je kvarenje financijskih podataka, destabilizacija ključne komunalne infrastrukture, uzemljenje zrakoplovne tvrtke ili izazivanje vrtnje satelita iz orbite.[9] Kibernetički napadi ukoliko se izvode ispravno, onda samo kibernetičko oružje može biti poražavajuće kao i konvencionalno oružje i može prouzročiti znatne kolateralne štete, uključujući civilne žrtve.[10] „Kibernetičke aktivnosti koje u konačnici rezultiraju smrću, ozljedom ili značajnim uništenjem smatrati će

[6] Libicki, Martin, Cyberdeterrence and cyberwar; SAD, 2009.
[7] Ziolkowski, Katharina, 'Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force' , 2012 4th International Conference on Cyber Conflict; 2016., str. 296.
[8] Perritt, Henry 'The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance'; 1998., str. 165.
[9] Clarke, Richard, Robert, Knake. Cyber war: the next threat to national security and what to do about it. SAD, 2012., str. 70
[10] Adkisson, James, And others Law of Armed Conflict: Implications for Navy Cyber Strategy; SAD, 2012.

se uporabom sile".[11] Primjeri poput otvaranja brane i tako nanošenjem štete od poplava, uzrokovanjem sudara zrakoplova ometanjem kontrole zračnog prometa i sl. samo su neki od mogućih posljedica kibernetičkih napada. Ukoliko se uporaba kibernetičkog oružja podiže na razinu uporabe sile u tradicionalnom ratu radit će se o kibernetičkom ratovanju.[12] Međutim, Sjedinjene Američke Države naglašavaju da ne mora nužno doći do štete u fizički vidljivom obliku da bi se radilo o kibernetičkom ratu. Bitno je da se radi o radnjama nacionalne države sa ciljem da prodre u računala ili mreže drugih zemalja u svrhu uzrokovanja štete ili poremećaja i da je jačina napada takva da dovodi do značajnih uništenja, poremećaja ili čak gubitka života.[13] To je značajan prag jer prema međunarodnom pravu, zemljama je dopušteno koristiti silu kako bi se obranile od oružanog napada. Iz toga slijedi da ukoliko je neka država bila pogođena kibernetičkim napadom značajnih razmjera, vlada te države je u mogućnosti da koristeći se svojim pravom samoobrane uzvrati udarac uporabom svoje standardne vojske: na hakiranje se može odgovoriti i raketnim napadima. Kibernetički napadi imaju nekoliko obilježja koja ih razdvajaju od tradicionalnog korištenja sile, što ima implikacije za primjenu postojećeg pravnog okvira na korištenje sile na njih. Kibernetički napad može trajati samo dijelove sekunde, a izvor napada može biti maskiran. Pravni okvir ima svoje korijene u tradicionalnijim načinima vođenja rata između nacionalnih država, a neki od problema koji proizlaze iz *cyber* napada su između ostalog, u vezi s nedržavnim akterima i mogućnošću preventivne samoobrane.

Upad u informacijske informacijske sustave i podatkovne mreže je jedan od najučinkovitijih načina prikupljanja velike količine informacija. Današnje kritične infrastrukturne mreže ključni su ciljevi kibernetičkih napada jer su narasli do točke u kojoj upravljaju sustavima zapovijedanja i kontrole, upravljaju logistikom te su generalna okosnica sposobnosti informiranja, a ono najvažnije je da danas većina sustava za zapovijedanje i kontrolu ima u sebi ugrađene čipove ili su povezani s globalnom informacijskom mrežom (npr. protuzračna artiljerija vođena je računalnim sustavima te se ispaljuje i prilagođava svoj let uz pomoć GPS sustava).[14] Ujedno, ovaj način je jedan od sigurnijih za "napadača". On se može obavljati iz velike udaljenosti, prikriven brojnim slojevima zaštite, prave lokacije, identiteta i namjera "napadača". Zbog navedenih razloga, kao dio ofenzivnog obavještajnog rada, pojedine države prikupljaju podatke o drugim državama provaljivanjem u njihove zaštičene informacijske i

[11] Primjedbe Harolda Hongju Koha, pravnog savjetnika američkog State Departmenta na USCYBERCOM-ovoj međuagencijskoj pravnoj konferenciji, 18. Rujan 2012.
[12] Theohary, Catherine A., Rollins, John W., Cyberwarfare and Cyberterrorism: In brief; SAD, 2012.
[13] Clarke, Richard A., Cyber War; SAD, 2010.
[14] Andress, *What is Cyber Warfare?* ; SAD, 2011.

komunikacijske sustave kako bi dobili što više podataka o procesima donošenja odluka u tim državama. Republika Hrvatska također je meta pokušaja prikupljanja podataka u kibernetičkom prostoru. Pritom je mjera napadača dvojaka: prikupiti podatke o sigurnosnim, političkim, gospodarskim i drugim procesima te podake Euroatlantskih asocijacija kojih je RH članica.[15]

2.2 Izgradnja zakonodavnog okvira kibernetičke sigurnosti

Postoji širok spektar trenutno prihvaćenih definicija kibernetičke sigurnosti. Međunarodna organizacija za standardizaciju definira ju kao očuvanje povjerljivosti, integriteta i dostupnosti informacija u kibernetičkom prostoru.[16] U nizozemskoj Strategiji kibernetičke sigurnosti iz 2011. navodi se da kibernetička sigurnost znači biti slobodan od opasnosti ili štete uzrokovane prekidom, ometanjem ili padom informatičko-komunikacijskih tehnologija (engl. ICT) ili zlouporabom ICT-a.[17] Nadalje, šteta prouzročena kibernetičkim napadom može se sastojati od „ograničavanja dostupnosti i pouzdanosti ICT-a, kršenja povjerljivosti informacija pohranjenim u ICT-u ili oštećenja integriteta tih informacija“[18] Dakle, u navedenoj definiciji kibernetičke sigurnosti možemo zamijetiti sva tri aspekta informacijske sigurnosti, odnosno, sigurnosnu trijadu. [19] Kibernetička sigurnost je 95 posto informacijske sigurnosti.[20] Razlika između njih je činjenica da informacijska sigurnost uključuje sigurnost informacija i po pitanju nedigitalnih medija (papira), odnosno, sigurnost informacija u tradicionalnom obliku, dok se s druge strane, kibernetička sigurnost fokusira se isključivo na sigurnost informacija u digitalnom obliku.[21] Kibernetička sigurnost štiti podatke i integritet računalne imovine koja pripada mreži ili se povezuje s mrežom organizacije. Jednostavno rečeno, sve se svodi na obranu imovine od prijetnji različitih aktera kibernetičkim napadom.

[15] Mišljenje sigurnosno – obavještajne agencije RH, http://www.soa.hr, preuzeto 14. lipnja 2019.
[16] *Cybersecurity Best Practices Guide, for IIROC Dealer Members*; Kanada 2018.
[17] *Dutch national cyber security agenda* - https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-1, preuzeto 15. Lipnja 2109.
[18] *Dutch Ministry of Security and Justice*, 2011
[19] Kezerić, Ana – Maria, Analiza prijetnji i rizika cyber sigurnosti Republike Hrvatske: Ranjivost informacijske sigurnosti; Zagreb, 2017., str 26.
[20] Košutić, Dejan, Primjena normi informacijske sigurnosti na primjeru HEP-a. U: Krajcar, Slavko (ur) Energetska sigurnost i kritična infrastruktura (161-171). Zagreb: Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva. , 2009.
[21] Košutić, Dejan, Primjena normi informacijske sigurnosti na primjeru HEP-a. U: Krajcar, Slavko (ur) Energetska sigurnost i kritična infrastruktura (161-171). Zagreb: Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva. , 2009.

Kibersigurnost je pitanje koje ne ovisi samo o pravnoj regulaciji nego uključuje niz tehnoloških, procesnih, organizacijskih te konačno pravnih mjera.[22] Isto tako, borba protiv kibernetičkog kriminala, odnosno njegovo spriječavanje, otkrivanje i sankcioniranje, postaje sve važnije pitanje za pravnu znanost, zakonodavstvo i pravnu praksu. S druge strane, postoji potreba da se ostvari balans između zahtjeva učinkovitosti sankcioniranja kibernetičkog kriminala i zahtjeva zaštite temeljnih ljudskih prava i sloboda.[23]

Zakonska regulativa po pitanju informacijske i kibernetičke sigurnosti u Republici Hrvatskoj, kao i zaštite kritične (informacijske) infrastrukture više je rezultat pritiska NATO- a i međunarodne zajednice, a manje vlastitih nastojanja i uviđanja potrebe za reguliranjem tih pitanja. [24] Ažuriranim okvirom za politiku kibernetičke obrane (2018) nastojati će se razviti ciljevi u okviru kojih bi se utvrdila minimalna razina kibersigurnosti i povjerenja koju treba postići.[25] Međutim, to će se ograničiti na kiberobranu dok ciljevi kojima se definira željena razina otpornosti za EU u cjelini nisu utvrđeni. Ishodi se rijetko mjere i tek je nekolicina područja politike evaluirana.[26] To je djelomično posljedica nedavne provedbe mnogih mjera, zakonodavnih ili nekih drugih, što onemogućuje potpunu procjenu njihovog učinka. Utvrđivanje valjanih kriterija procjene koji mogu pomoći u mjerenju učinka čini izazov. Štoviše, stroga evaluacija još nije postala opća norma u području kibersigurnosti. Trenutačne ovlasti ENISA-e[27] neobuhvaćaju ocjenjivanje i praćenje stanja kibersigurnosti i pripravnosti u EU-u.[28] Oblikovanje politike utemeljene na dokazima ovisi o dostupnosti dovoljno pouzdanih podataka i statistika za praćenje i analizu trendova i potreba. Međutim, u nekim su područjima, na primjer u radu okvira ciklusa politike EU-a razvijeni posebni parametri koji se upotrebljavaju za suzbijanje teškog i organiziranog kriminala. Samo nekoliko država članica redovito prikuplja podatke o pitanjima povezanima s kibersigurnošću, što onemogućuje

[22] Dragičević, Kaspersen, Schwerha, *Article 15: Conditions and Safeguards under the Budapest Convention on Cybercrime*; 2012. Str. 3.

[23] Ibid. Str 3

[24] Kezerić, Ana – Maria ,Analiza prijetnji i rizika cyber sigurnosti Republike Hrvatske: Ranjivost informacijske sigurnosti; Zagreb 2017., str 6.

[25] Izazovi u pogledu djelotvornosti kibersigurnosne politike EU-a ; http://www.eca.europa.eu, preuzeto 15. lipnja 2019.

[26] Služba Europskog parlamenta za istraživanje, transatlantic cyber-insecurity and cyber crime. Economic impact and future prospects (transatlantska kibernetička nesigurnost i kiberkriminal. Gospodarski učinak i budući izgledi), PE 603.948, prosinac 2017.

[27] *European Network and Information Security Agency* ili skraćeno ENISA agencija je Europske unije koja se bavi pitanjima sigurnosti informacija i informacijskih mreža

[28] Izazovi u pogledu djelotvornosti kibersigurnosne politike EU-a; http://www.eca.europa.eu, preuzeto 16. Lipnja 2019.

uspoređivanje.[29] Nažalost, EU je do sada do sada u nedostatnoj mjeri, pa samim time i bez većih rezultata upozoravao na potrebu za objedinjavanjem statističkih podataka na europskoj razini, dodatno, nepostojanje kodificirane definicije kiberkriminala gotovo je nemoguće utvrditi relevantne europske pokazatelje koji bi pomogli u praćenju i evaluaciji. [30] Zaključno, brzina kojom se pojavljuju nove tehnologije i prijetnje daleko nadmašuju brzinu izrade i provedbe zakonodavstva EU-a. Pri osmišljavanju postupaka Unije nije se imalo u vidu digitalno doba: ključni je prioritet razviti inovativne i fleksibilne postupke kojima bi se zajamčio politički i zakonodavni okvir koji odgovara potrebi za boljim predviđanjem i oblikovanjem budućnosti (što znači utemeljen na načelima i što je vise moguće tehnološki neutralan).[31]

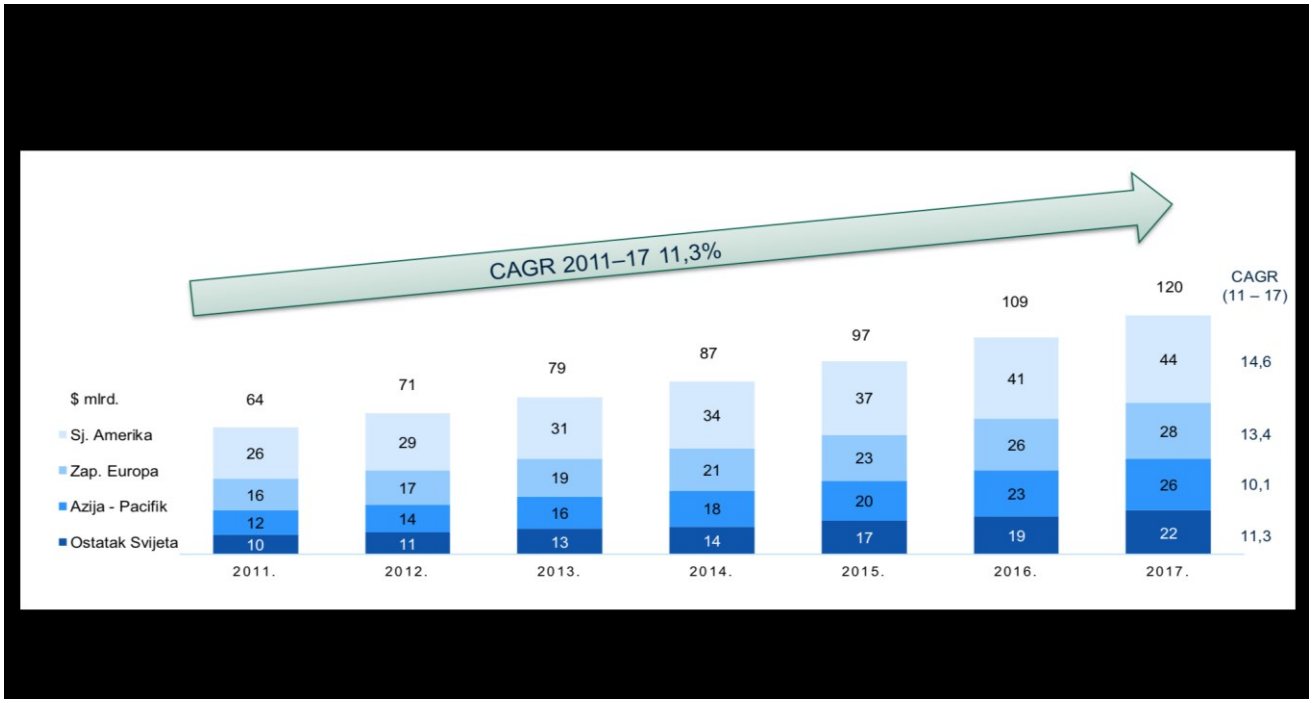
Ekonomija kibernetičke sigurnosti primjenjuje načela ekonomije na analizu problema kibernetičke sigurnosti.[32] Često se smatra da se informacijska sigurnost svodi na tehničke mjere, ali Anderson i Moore (2006) opisali su to pitanje na sljedeći način: „Ljudi su shvatili da je neuspjeh sigurnosti uzrokovan često, lošim poticajima ali ujedno i lošim dizajnom.[33] Ovo znači da su potrebni bolji poticaji kako bi se povećala ulaganja u kibernetičku sigurnost umjesto da se fokusiraju samo na tehničke mjere. Sa financijskog aspekta EU želi postati najsigurnije digitalno okruženje na svijetu. Da bi se ostvarila ta ambicija moraju se uložiti znatni napori, čvrsti financijski temelji i dobro financijsko upravljanje.[34] Svaka organizacija i vlada moraju znati koliko je potrebno uložiti u kibernetičku sigurnost i koliko je dovoljno. Gledajući dostupnu literaturu, treba napomenuti da je malo pozornosti posvećeno brzoj disciplini, naime, ekonomiji kibernetičke sigurnosti koja osigurava neke zanimljive i relevantne modele za mjerenje ulaganja u kibernetičku sigurnost kroz kompromise troškova i koristi.[35] Procjenjuje se da ukupna globalna potrošnja na kibersigurnost, izračunata kao postotak BDP-a iznosi otprilike 0.1% u EU. Usporedbe radi, u Sjedinjenim Američkim Državama potrošnja je veća I iznosi otprilike 0.35% (uključujući i privatni sektor) izražena

[29] Izazovi u pogledu djelotvornosti kibersigurnosne politike EU-a; http://www.eca.europa.eu, preuzeto 16. Lipnja 2019.
[30] Iznimka je članak 14. (praćenje i statistički podatci) direktive 2013/40/EU Europskog parlamnta i Vijeća od 12. Kolovoza 2013 o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2015/222/PUP
[31] Europska komisija, Mehanizam za znanstveno savjetovanje, Znanstveno mišljenje 2/2017, 24. Ožujka 2017.
[32] IPACSO, FP7, Deliverable 4.1, State-of-the-art of the Economics of Cyber-security and privacy, at 9, http://ipacso.eu/downloads/public-deliverables.html, preuzeto 16. Lipnja 2019.
[33] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.477.2090&rep=rep1&type=pdf, preuzeto 16. Lipnja 2019.
[34] Izazovi u pogledu djelotvornosti kibersigurnosne politike EU-a ; http://www.eca.europa.eu
[35] Brangetto, Pascal, Kert-Saint Aubyn, Mari, Economic Aspects of National Cyber Security Strategies; Estonija, 2015.

kao postotak BDP-a, potrošnja Savezne vlade SAD-a iznosi otprilike 0.1%[36] ili otprilike 21 milijardu američkih dolara predviđenih u proračunu za 2019. godinu.[37] U odnosu na navedeni podatak, potrošnja u EU niska je i neustanovljena te često ne postoje usklađeni vladini programi kojima bi se ona podupirala. Unatoč tome procjenjuje se da se javna potrošnja EU na kibersigurnost kreće između 1 i 2 milijarde eura godišnje.[38] Europska unija i njezine članice moraju znati koliko zajednički ulažu kako bi mogle utvrditi koje nedostatke ukloniti. U potrazi za informacijom o iznosu potrošnje RH za zaštitu kibersigurnosti naišla sam na poražavajući podatak da osim što država ne razlučuje razliku između potrošnje na kibersigurnost i potrošnje na područje informacijske tehnologije je gotovo nemoguće dobiti podatke bilo u javnom ili u privatnom sektoru zato što je ured za reviziju izvjestio da nema centralizirani uvid u državnu potrošnju na području kibersigurnosti.[39] Jednako tako RH kao i ostale članice EU nije obvezala javne subjekte da u svojim financijskim planovima odvojeno prijavljuju izdatke za kibersigurnost. Smatram da je centralizirani pregled potrošnje važan radi transparentnosti i postizanja bolje koordinacije jer bez toga je tvorcima politike u Europskoj uniji gotovo nemoguče riješiti problem nedostatka ulaganja u kibersigurnost koji bi trebao dovesti do korisnih ishoda i utvrditi kako je potrošnja usklađena sa potrebama u svrhu ispunjavanja cilja.[40] Zanimljiv je podatak da je Europska unija odlučila izdvojiti za komponentu kibersigurnosti u razdoblju od 2021. – 2027. iznos od 2 milijarde eura u okviru

[36] *Atlantic Council, Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures* (Nexus rizika: prijetnja od kibernetičkih rizika? gospodarske koristi i troškovi alternativnih kiberbudučnosti), 10. Rujna 2015.
[37] Bijela kuća, *Cybersecurity spending fiscal year 2019* (Potrošnja na kibersigurnost u fiskalnoj godini 2019.)
[38] Europska komisija, Radni dokument službi komisije: Procjena učinka priložena Prijedlogu uredbe Europskog parlamenta i Vijeća o uspostavi programa Digitalna Europa za razdoblje 2021-2027, SWD(2018) 305 FINAL, 6. Lipnja 2018.
[39] Europska komisija, ibid 19. COM2018 (603) FINAL, 12. Rujna 2018
[40] Izazovi u pogledu djelotvornosti kibersigurnosne politike EU-a ; http://www.eca.europa.eu, preuzeto 16. Lipnja 2019.

novog predloženog programa Digitalna Europa.



Slika 1. Globalni očekivani rast industrije kibernetičke sigurnosti

Izvor: Alixpartners (2012)

Bez obzira radi li se o klimatskim promjenama, terorizmu ili kibernetičkim napadima, niti jedan globalni izazov s kojim se suočava međunarodna zajednica ne može samostalno riješiti niti jedan međunarodni akter, neovisno o njegovoj moći. Svi takvi suvremeni izazovi zahtjevaju okvir za međunarodnu suradnju. To je međunarodno pravo koje 'pruža takav okvir, obrazac i strukturu za međunarodno društvo'.[41] Uporaba i zlopuporaba kibernetičkog prostora utječe na vitalne državne interese u fizičkom svijetu, uključujući nacionalnu i javnu sigurnost te gospodarski razvoj. Kao takav, kibernetički prostor se proteže daleko izvan domene unutarnjih poslova pojedine države.[42] Iako niti jedan sveobuhvatan međunarodnopravni okvir trenutno ne upravlja svim kibernetičkim napadima, mnoštvo napora ulažu razne države poput Sjedinjenih Američkih Država i drugih država kako bi uspostavile kontrolu ove rastuće prijetnje. U nastavku ćemo istražiti pojedine pravne mehanizme internacionalnog značaja regulacije kritičnog pitanja kibernetičke sigurnosti i kibernetičkog ratovanja. Nepostojanje specifičnog kibernetičkog sustava pravila međunarodnog prava ne znači da ne postoje

[41] Henkin, Louis, *How Nations Behave*; SAD, 1978., str. 5.
[42] Perrit, Henry H., *The internet as a threat to sovereignty? Thoughts on internet role in strenghtening national and global governance*, Sjedinjene Američke Države, 1998., str. 5.

zakonska pravila koja bi se primjenjivala na kibernetičke aktivnosti. Države prihvaćaju da se općenito primjenjiva pravila međunarodnog prava primjenjuju i na ponašanje država u kibernetičkom prostoru.[43] Ako međunarodno pravo treba biti učinkovita struktura upravljanja, ono mora biti prilagodljivo novim fenomenima bez potrebe da se svaki put iznova izrađuje cijeli okvir propisa.[44] U nastavku ćemo obratiti pažnju na najznačajnije pravne regulative kibernetičkog rata.

2.3 Tallinnski priručnik

Kako je intenzitet militarizacije virtualnog prostora rastao, rasla je i potreba za izradom dokumenta o međunarodnom pravu primjenjivom na kibernetičko ratovanje, koji bi detaljno razradio način na koji postojeće norme međunarodnog prava primjenjivati na kibernetičko ratovanje, kao novu formu vođenja rata, svijetu i dalje relativno nepoznatu. Upravo iz tog razloga, 2009.godine na poziv NATO CCDCOE *(Cooperative Cyber Defence Centre of Excellence)*[45] sastaje se međunarodna skupina od otprilike dvadeset stručnjaka koja pune tri godine radi na donošenju takvog pravnog dokumenta, da bi konačno 2013.godine ugledao svijetlo dana pod nazivom Tallinnski priručnik ***(The Tallinn Manual*** - *Tallinn Manual on the International Law Applicable to Cyber Warfare).* 2017. godine objavljeno je drugo prošireno izdanje poznato pod nazivom Tallinn 2.0.

Po svojoj prirodi Tallinnski priručnik je je akademska, neobvezujuća studija o tome kako se međunarodno pravo (posebice *jus ad bellum* i međunarodni humanitarni zakon) primjenjuju na kibernetički sukob.[46] Iako „neobavezujući“ i više referentnog značaja, ovaj priručnik nudi autoritativno tumačenje prirode i odnosa postojećih međunarodnih zakona na cyber ratovanje. On praktično nudi pravne smjernice napadačima, onima koji se brane i pravnim ekspertima, kako i kada se računalni napadi mogu klasificirati slično kao oružani napadi, u pogledu važećih međunarodnih zakona. Izraz „oružani napad“ ima precizno značenje u međunarodnom pravu i ne mogu se svi računalni, pa čak i ozbiljniji, napadi podići na nivo oružanog napada. Definicija ove granice je izazov koji Tallinnski priručnik pokušava definirati i riješiti, ali ovaj delikatni proces će očito još prilično trajati. Ono što je sigurno je

[43] Mačak, Kubo, *Is the international law of cyber security in crisis?;* Ujedinjeno Kraljevstvo, 2016, str. 132.
[44] CfUS, *international strategy for Cyberspace* (broj 24) str 9.
[45] https://ccdcoe.org/, preuzeto 26. ožujka 2018.
[46] https://en.wikipedia.org/wiki/Tallinn_Manual, preuzeto 26. ožujka 2018.

da će u budućnosti konvencionalni ratovi uvijek biti praćeni i računalnim ratom, odnosno oni to već neko vrijeme jesu.[47]

Prije same analize strukture Priručnika, pojasniti ću ukratko odakle naziv *Tallinn Manual.* Nakon napada na Estoniju 2007. godine, NATO je postao zainteresiran za značenje globalnog kibernetičkog ratovanja. NATO CCDCOE uspostavljen je upravo u Tallinnu iz razloga što je Tallinn bio mjesto prvog kao takvog prepoznatog slučaja međunarodnog kibernetičkog ratovanja.[48] Neki komentatori su nazvali ovaj napad „*Web War I.*" i upućuju na Estoniju kao „E-stoniju" s obzirom na njezinu ovisnost o cyber-prostoru. [49] Do 2007. godine izvršeno je 98% svih bankarskih transakcija u Estoniji elektronski i preko 80% poreznih prijava učinjeno je *online.* U to vrijeme Estonija je bila jedna od najnaprednijih nacija u svijetu, ispred Sjedinjenih Država i Južne Koreje. Ruski su napadi već oslabjeli podijeljenu naciju pa je NATO bio prisiljen to primijetiti. Treba naglasiti činjenicu da je već na prvi pogled uočljivo da je sastav Međunarodne skupine bio (pretežito) ograničen na predstavnike zemalja članica NATO-a zainteresiranih za tu materiju. To znači da, iako su sudionici bili pripadnici različitih nacija, nije bilo pokušaja da se osigura ujednačena geografska raspodjela.[50] Kriteriji za njihovo sudjelovanje temeljili su se na njihovim vještinama na području relevantnog prava te na njihovim sposobnostima za analizu osjetljivosti kibernetičkog konteksta u kojem bi takvo pravo bilo primijenjeno.[51] Dakle stvaraoci toga međunarodnog dokumenta nisu predstavljali odraz svih svjetskih pravnih kultura, nego su dolazili iz (pretežito) zapadnih zemalja.[52]

Sada ću objasniti detaljnije ono najbitnije – strukturu i sadržaj Tallinnskog priručnika. Glavnom sadržaju Priručnika prethodi popis svih članova Međunarodne skupine i ostalih sudionika, zatim detaljan popis korištenih pravnih izvora te uvodni dio koji se sastoji od nekoliko kratkih poglavlja. Uvod ističe da pravila mjerodavna za kibernetičke operacije (uključivši i tradicionalne operacije elektroničkog ratovanja, poput elektroničkog ometanja) nisu obuhvaćena i objašnjava da je radio takva isključenja u tome što su te teme već dobro proučene i shvaćene u tradicionalnim pravilima prava oružanog sukoba.[53] Nakon uvoda slijedi

[47] Pleskonjić, Dragan, *Cyberwar: Pearl Harbor*, Tallinn Manual, Srbija, 2009.

[48] Sovjetski vojni memorijal u Tallinnu ima tešku sudbinu. U travnju 2007. su vlasti Estonije odlučile premjestiti "brončanog vojnika" i grobove 12 vojnika na vojničko groblje izvan grada. Ova je odluka izazvala masovne demonstracije Rusa u Tallinnu te je pogoršala bilateralne odnose između Rusije i Estonije.

[49] Waxman, Matthew, *Cyber Attacks as Force*, SAD, 2011., str. 43.

[50] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, str. 4.

[51] Ibid, str. 4.

[52] Ibid, str.11.

[53] McGhee, E., J., *The Schmitt Analaysis, Tallinn Manual and US Cyber Policy*, Journal of Law & Cyber Warfare, vol. 2, izd. 1., 2013., str. 84.

glavni sadržaj Priručnika, koji se dijeli na dva dijela, i to dio I.; koji razmatra pitanja međunarodnog prava kibernetičke sigurnosti, i dio II.; koji razmatra pitanja prava kibernetičkog oružanog sukoba. U dijelu I. poglavlje prvo razmatra pitanje država i kibernetičkog prostora, uključujući suverenost, sudsku nadležnost i kontrolu te državnu odgovornost; poglavlje drugo razmatra uporabu sile (uključujući njezinu zabranu) i pravo samoobrane. U dijelu II. poglavlje treće razmatra općenita pitanja prava oružanog sukoba; poglavlje četvrto razmatra pitanja postupanja u neprijateljstvima; poglavlje peto razmatra pitanja stanovitih osoba, objekata i aktivnosti; poglavlje šesto bavi se okupacijom; poglavlje sedmo bavi se neutralnošću.

Sadržajno smatram osobito pohvalnim to da se htjelo stvoriti doktrinarni rad koji bi bio od koristi državama u formiranju vlastitih stajališta i njihovu djelovanju u kibernetičkom prostoru. Nisu se davale preporuke niti definirala najbolja praksa, nije se ulazilo u političke sfere.[54] Autoritet Tallinnskog priručnika najbolje je sažeo njegov glavni urednik riječima da taj Priručnik nije službeni dokument, nego rad skupine neovisnih stručnjaka, koji su pri njegovoj izradi sudjelovali isključivo u svojem osobnom svojstvu. Neovisno o znanju i dugogodišnjem iskustvu članova Međunarodne skupine ostaje činjenica da Tallinnski priručnik nije međunarodno obvezujući dokument, nego tekst obuhvaćen pod pojmom "međunarodni priručnik".[55] Dakle treba ga karakterizirati ni manje ni više nego kao konsenzus akademskog rada skupine međunarodnih stručnjaka koji su posvetili tri godine identifikaciji postojećeg prava primjenjivog na kibernetičko ratovanje.[56]

Proučavajući Priručnik i istražujući različita stajališta i komentare na rezultat donošenja takvog dokumenta, voljela bih skrenuti pozornost na segment Priručnika koji je bio u mnogim člancima i knjiga kritiziran kao nejasan; naime, Tallinnski priručnik je izvanredan dokument, dijelom zbog širine problema koji pokriva, a dijelom zbog toga što se pomiče pojam kibernetičkog rata do krajnjih granica i čini ga živim više nego ikada. Unatoč tome znanstvenici smatraju da problematika nastaje kod primjene zakona o državnom suverenitetu. Kao što je Priručnik napomenuo, međunarodno pravo obično razlikuje nadležnost propisivanja, presuđivanja i provođenja zakona. Nadležnost za provođenje i rješavanje obično je ograničena na ono što država ima pod svojom kontrolom, uključujući stranu imovinu i strane osobe u državnom dosegu. Nadležnost za propisivanje je šira, uključuje i zakonodavne

[54] Gladyshev, P., Marrington, A., Baggili, I., *Digital Forensics and Cyber Crime: Fifth International Conference*, Revised Selected Papers, Moskva, 2014., str. 131.

[55] Prpić, Ratimir, *Osvrt na Tallinnski Priručnik u Međunarodnom pravu primjenjivom na kibernetičko ratovanje;* Zagreb, 2017.

[56] Ibid, str. 56.

korake kako bi se zaštitili građane države kod kuće ili u inozemstvu, regulira se ponašanje na tlu države, sprječavaju se napade protiv države, i tako dalje. S obzirom na te prilično temeljne razlike, čini se da je podosta osjetljivo da Tallinnski priručnik 2.0 započne s pregledom zakona nadležnosti.

Kao i prvo izdanje, drugo izdanje Priručnika također upozorava u prvom pravilu: „Država može kontrolirati internetsku infrastrukturu i djelovanje na svom suverenom području." Na prvu pomisao jasno, zar ne? – država ima ovlasti kontrolirati stvari unutar svog teritorijalnog dosega. No, što znači reći da država može kontrolirati internetsku „aktivnost" unutar svog teritorija?[57] Uzeti ću za primjer jednu od najvećih internetskih stranica na svijetu – Google. U situaciji u kojoj Europski sud pravde odluči da Google mora ukloniti određene *web* rezultate jer se bavio kibernetičkom aktivnošću u Hrvatskoj, primjenjujući Tallinnski priručnik, odnosi li se ta odluka samo na google.hr, ili na ostatak Europe (google.es, google.fr, itd.) ili možda čak na cijeli svijet? Čak i ako opseg riječi „aktivnost" nije nejasan, postavlja se pitanje: što odredba o nadležnosti sugerira da Hrvatska može učiniti kako bi prisilila Google da se pridržava pravila? Nije jasno zašto su autori odlučili započeti priručnik sa temom nadležnosti koja ne igra veliku ulogu u borbi protiv kibernetičkog napada, jer kako sam već spomenula ranije u radu, posljedice i žrtve mogu narasti i povećati se u svega nekoliko minuta. Da ne ulazim u nagađanja, ostavit ću ova pitanja otvorenima i zaključiti da ukoliko dvije ili više država imaju nadležnost nad istom osobom ili predmetom u odnosu na događaj, treba položiti svoje nade u to da će potencijali sukob nadležnosti riješiti na sudu, zakonskim načelima, izbjegavajući oružani kontakt. Osim ovog problema postoji još nekoliko mana Priručnika, no unatoč tome smatram da njegova jedinstvenost proizlazi iz primjene *lex lata* na (relativno) novo tehnološko okružje jer je kibernetička tehnologija (kakvu danas poznajemo) novina u odnosu na tradicionalna pravila međunarodnoga prava. Kibernetički napadi (i svaka druga uporaba kibernetičke tehnologije u svrhu zlonamjernog iskorištavanja digitalnih prednosti) danas predstavljaju novi i stvarni oblik opasnosti za državu, društvo i pojedinca. U tim je okolnostima bilo nužno donijeti dokument koji bi državama pružio barem smjernice prilikom provođenja njihovih tuzemnih i međunarodnih interesa u kibernetičkom prostoru (i svim drugim mogućim oblicima korištenja kibernetičke tehnologije).[58]

[57] Keane, Andrew, Woods, *The Tallinn Manual review*, USA, 2017.
[58] Op. cit. bilj., 115., str. 58.

2.4 Internacionalni režimi koji direktno reguliraju kibernetičke napade

2.4.1 Ujedinjeni narodi

S obzirom na ulogu UN- a, posljednjih 13 godina održavali su se pregovori sa ciljem uspostave međunarodnog pravnog okvira koji uređuje kibernetičku sigurnost. Nažalost, u lipnju prošle godine ti su pregovori naglo prekinuti zbog spora u kojem su se Kina, Kuba i Rusija osjetile ugroženima od strane zapadnih zemalja. Raspodjela među pravnim i vojnim stručnjacima u UN-u, uz stare hladnokrvne linije, pojačala je nepovjerenje u vrijeme diplomatske napetosti u vezi sa *cyber* napadima, primjerice sjeckanje Američkog demokratskog nacionalnog odbora (DNC) iz 2016. godine. Taj je prekid navodno koordinirala ruska obavještajna služba i s namjerom pomoći predsjedničkoj kampanji Donalda Trumpa.[59] Unatoč sudjelovanju stručnjaka iz 25 zemalja i svim naporima UN-a s obzirom na novu političku struju u SAD-u, pregovori o kibernetičkog sigurnosti su za sada daleko od konačnog dogovora i mira. Između zemalja vlada velika netrpeljivost i UN je za nekoliko medija izrazio svoju zabrinutost po tom pitanju. Glavni tajnik Antonio Gutteres je početkom godine u Lisabonu pozvao globalna pravila da smanje utjecaj elektronskog ratovanja na civile, budući da masivni kibernetički napadi vjerojatno postaju prve salve u budućim ratovima: „Epizode *cybe*r - ratovanja između država već postoje. Ono što je još gore je da nema regulatorne sheme za tu vrstu ratovanja, nije jasno kako se na to odnosi Ženevska konvencija ili međunarodni humanitarni zakon.“[60] Stručnjaci se nadaju da će UN poslužiti kao platforma znanstvenicima i vladama za izradu pravila i uspostavu dogovora kako bi se spriječili veći sukobi i ono najgore - civilne žrtve.

2.4.2 NATO

NATO je svoju borbu protiv kibernetičkih napada započeo puno prije napada na Estoniju 2007. godine. Tijekom operacija na Kosovu 1999. godine članice NATO-a i vojne snage doživjele su sirove kibernetičke napade, uključujući uskraćivanje usluga i napade na *web*

[59] Owen, Bowcott, *The Guardian*

[60] https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4, preuzeto 02. travnja 2019.

stranice.[61] Ti napadi nisu toliko negativno utjecali na operacije na Kosovu, ali su se dogodili u vrijeme kada je politička i vojna zabrinutost o kibernetičkoj sigurnosti rasla. 2002. godine je na summitu NATO- a u Pragu identificirana potrebu da NATO ojača svoje sposobnosti da se obrani od *cyber* napada i utemeljen je *Cyber Defense program.*[62] Ovaj je program stvorio NATO *Computer Incident Response Capability* (NCIRC) kako bi NATO bio efikasniji i uspješniji u borbi protiv kibernetskih prijetnji. [63] Nedugo nakon toga, 2005. godine NATO je uključio *cyber* prijetnju u Dokument o političkim smjernicama i još više istaknuo potrebu za zaštitu informacijskih sustava na summitu u Rigi što samo navodi na zaključak da je NATO izrazio veliku zabrinutost zbog opasnosti koje se rađaju iz ovisnosti o kibernetskom prostoru. Isprva se činilo kako NATO ima sve pod kontrolom, ali napad na Estoniju je pokazao neadekvatnost NATO- a na pravovremenu reakciju. Tek tada, na summitu u Bukureštu (2008. godine) i u Lisabonu (2010. godine) je NATO nastavio davati važnost *cyber* obrani usvojivši tzv. Strateški koncept (2010. godine),[64] *The Cyber Defense Concept, Policy, and Action Plan* (2011. godine),[65] i Chicago summit deklaraciju (2012. godine). Kroz ove razvojne politike NATO je uspostavio ili poticao stvaranje mehanizama za implementaciju (uz NCIRC) za stvaranje strategije poboljšanja obrane protiv *cyber* napada kako unutar Saveza tako i u državama članicama NATO- a. Pošto je priroda kibernetike vrlo promjenjiva i brzo evoluira, NATO je usvojio pojačanu politiku i akcijski plan kako bi pratio daljnji razvoj. Plan je usvojen na novom summitu 2014.godine u Walesu, kada je utvrđeno da je dio cyber obrane temeljni zadatak kolektivne obrane Saveza, te da je zapravo najveći prioritet zaštita komunikacijskih i informacijskih sustava u vlasništvu i upravi Saveza.[66] Na službenim stranicama NATO saveza mogu se saznati detalji o aktivnom radu Saveza, gdje se pojašnjava da trenutna politika također omogućava pojednostavljeno upravljanje kibernetskom obranom, postupke za pomoć savezničkim državama kao odgovor na cyber napada i integraciju cyber obrane u operativno planiranje, uključujući planiranje civilnih izvanrednih stanja. Nadalje,

[61] Healey, Jason, Leendert van Bochoven, *Atlantic Council, NATO's Cyber Capabilities*, Yesterday, Today, and Tomorrow, at 2, 2012.

[62] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf, preuzeto 02. travnja 2019.

[63] Op. cit. 121.

[64] NATO, Lisbon Summit Declaration para. 2, 2010. http://www.nato.int/nato_static/assets/pdf/pdf_2010_11/2010_11_11DE1DB9B73C4F9BBFB52B2C94722EAC_PR_CP_2010_0155_ENGSummit_LISBON.pdf., preuzeto 03. travnja 2019.

[65] NATO, Defending the Networks: The NATO Policy on Cyber Defence, 2011. http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914- policy-cyberdefence.pdf [hereinafter NATO Policy on Cyber Defence]., preuzeto 03. travnja 2019.

[66]https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf, preuzeto 03. travnja 2019.

politika definira načine kako unaprijediti aktivnosti svijesti, obrazovanja, osposobljavanja i iskustva, te potaknuti daljnji napredak različitih inicijativa suradnje, uključujući one s partnerskim zemljama i međunarodnim organizacijama. Također predviđa jačanje NATO suradnje s industrijom, uključujući razmjenu informacija, razmjenu najboljih praksi i istraživanje inovativne tehnologije kako bi se poboljšala kibernetička obrana. Saveznici su se također obvezali na poboljšanje razmjene informacija i međusobnog povezivanja pomoć u sprječavanju, ublažavanju i oporavku od cyber napada. Na summitu u Varšavi u srpnju, o državama i vladama država članica NATO-a očekuje se da priznaju kibernetički prostor kao operativnu domenu, pored zraka, kopna i mora. Obrada kibernetičkog prostora kao operativne domene omogućit će Savezu bolju zaštitu svoje misije i operacije, s više usredotočenosti na obuku i vojno planiranje. Također NATO ima u planu pružiti bolji okvir upravljati resursima, vještinama, sposobnostima i koordinacijama odluka. To neće promijeniti misije ili mandat NATO-a, što jest obrambeni. Kao i u svim operativnim područjima, aktivnosti NATO-a su obrambene, proporcionalne i u skladu s međunarodnim pravom. Savez također pozdravlja napore poduzete u drugim međunarodnim forumima kako bi razvile norme odgovornog ponašanja države i mjere za izgradnju povjerenja za promicanje transparentnijeg i stabilnog kiberprostora za međunarodnu zajednicu.

NATO- ov NCIRC štiti vlastite mreže Saveza osiguravanjem centralizirane i cjelogodišnje podrške za cyber obranu na različitim mjestima NATO- a. Obrađuje i izvješćuje o incidentima, te širenjem važnih informacije povezanih s incidentima upravlja sigurnošću i korisnicima. NCIRC također održava *Rapid Reaction Teams,*[67] koji mogu biti razmješteni kako bi podržali zaštitu NATO- a ili savezničkih mreža. NATO pomaže saveznicima u njihovim nastojanjima da zaštiti svoje kritične mreže i infrastrukturu dijeljenjem informacija i najboljim prakse. Memorandum o razumijevanju o *cyber* obrani između NATO- a i svake od 29 članica određuju aranžmane za razmjenu različitih informacija vezanih uz kiberbranu i pomoć za poboljšanje prevenciju cyber incidenta, otpornost i sposobnosti reagiranja.

Da bi se olakšalo širenje Saveza i zajednički pristup razvoju sposobnosti za cyber obranu, NATO također razvija ciljeve za provedbu nacionalnih sposobnosti cyber obrane savezničkih zemalja kroz proces NATO-ov tzv. Plan obrane. Kroz 2018. godinu dogovorit će se daljnji ciljevi cyber obrane. [68]

[67] https://www.nato.int/cps/en/natolive/news_85161.htm, preuzeto 10. travnja 2019.
[68] Op. cit. bilj. 126.

2.4.3 Vijeće Europe

2001.godine Vijeće Europe, shvaćajući ozbiljnost *cyber* prijetnje donosi Konvenciju o kibernetičkom kriminalu. Otvorena je za potpisivanje u Budimpešti, 23. 11. 2001. državama članicama i država nečlanicama koje su sudjelovale u njihovom sastavljanju. Otvorene su za pristup ostalim državama nečlanicama. Više od 100 drugih zemalja trenutačno koristi konvenciju kao modelni zakon, posebno „zemlje u razvoju“ npr. Brazil, zemlje Kariba, Indija, Nigerija, Pakistan, itd.

Konvencija je stupila na snagu 1. srpnja 2004. i prvi (i do danas ostaje vodeći) međunarodni ugovor o računalnim zločinima. Protokol o rasističkim i ksenofobnim djelima u kibernetičkom prostoru dodan je Konvenciji i potpisan u siječnju 2003. godine; stupio je na snagu prvog dana ožujka 2006.

Konvencija nastoji nastaviti zajedničku kriminalističku politiku usmjerenu na zaštitu društva od cyber kriminala, osobito usvajanjem odgovarajućeg zakonodavstva i poticanjem međunarodne suradnje. Odredbe Konvencije odnose se na kršenje autorskih prava, prijevaru na računalu, dječju pornografiju i kršenje sigurnosti mreže, nezakonitog pristupa, ometanju podataka, ometanju sustava, zlouporabi uređaja, krivotvorenju računala, itd. Sve države koje ratificiraju ili pristupaju Konvenciji suglasne su osigurati da njihovi nacionalni zakoni kriminaliziraju tamo utvrđene postupke.[69]Konvencija o kibernetičkom kriminalu Vijeća Europe, bez obzira na brojne kritike, prvi je potpisani i široko prihvaćeni multilateralni sporazum posebno usmjeren na probleme kompjuterskog kriminala. Konvencija polazi od promjena nastalih neprekidnom globalizacijom računanih mreža, mogućnosti da računalne mreže i elektroničke informacije budu iskorištene za počinjenje kaznenih djela i da dokazi vezani uz ta djela budu pohranjeni i prenošeni putem tih mreža, potrebe za zaštitom legitimnih interesa prilikom korištenja i razvitka informatičkih tehnologija te spoznaje da učinkovita borba protiv kibernetičkog kriminala zahtijeva povećanu, brzu i uhodanu međunarodnu suradnju u kaznenopravnim predmetima.[70]

Konvencija obuhvaća tri glavna područja: 1. usklađivanje materijalnog kaznenog zakona u području cyber kriminala, 2. usklađivanje procesnog prava i 3. donošenje pravila

[69] Killerby, Margaret, *The Convention on Cybercrime,* USA, 2006.

[70] Škrtić, Dražen, *Implementacija odredbi Konvencije o kibernetičkom kriminalu u hrvatsko Kazneno i Kazneno procesno pravo,* Karlovac, 2014.

međunarodne pravosudne suradnje, te je podijeljena u četiri poglavlja: 1. upotreba pojmova, 2. pitanja materijalnog i postupovnog prava, 3. prekogranična pitanja i 4. završne odredbe. [71] Republika Hrvatska je jedna od prvih država koja je potpisala i ratificirala Konvenciju o kibernetičkom kriminalu.

2.4.4 Organizacija Američkih Država

Prema Organizaciji Američkih Država u svom izvješću „Trendovi u kibernetičkoj sigurnosti Latinske Amerike i Kariba" objavljenom u lipnju 2014. godine, Latinska Amerika i Karibi imaju najbrže rastuće internetsko stanovništvo u svijetu s čak 147 milijuna korisnika koji rastu svake sekunde.[72] Organizacija Američkih Država (OAS) tek je nedavno započela s prvim koracima u regulaciji kibernetičkih napada. U travnju 2004. godine Organizacija Američkih Država donijela je rezoluciju kojom se navodi da zemlje članice trebaju „procijeniti preporuku provedbe načela Konvencije Vijeća Europe o kibernetičkom kriminalu iz 2001. godine i razmotriti mogućnost pristupanja toj konvenciji".[73] Organizacija Američkih Država je također usvojila „sveobuhvatnu Strategiju kibernetičke sigurnosti američkih zemalja" kojoj je cilj između ostalog usvojiti „politike i zakonodavstvo protiv kibernetičkih kriminala koji će štititi korisnike interneta i spriječiti kaznenu zlouporabu računala i računalnih mreža uz poštovanje privatnosti i individualnih prava korisnika interneta".[74] U tu svrhu Organizacija Američkih Država okupila je grupu stručnjaka koja „pomaže državama članicama u izradi i donošenju zakona koji kažnjavaju kibernetičko kriminalno djelovanje, zaštitu informacijskih sustava i sprječavanje korištenja računala za nezakonite aktivnosti".[75] Bitno je za napomenuti da spomenuta skupina stručnjaka daje isključivo smjernice; Organizacija Američkih Država nema jedinstvene zakone koji uređuju borbu protiv kibernetičkih napada i kibernetičkog kriminala. OAS- ova radna skupina za kibernetički kriminal je na sastanku održanom u siječnju 2010. godine preporučila državama članicama da uspostave državna tijela za istragu i progon kibernetičkih zločina, te da donesu domaća

[71] https://narodne-novine.nn.hr/clanci/medunarodni/2002_07_9_119.html, preuzeto 11. travnja 2019.
[72] „*Latin American and Caribbean Cybersecurity Trends*," Report, Washington, DC: Organization of American States Secretariat for Multidimensional Security, 2014. http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-reportlamc.pdf, preuzeto 12. travnja 2019.
[73] Organizacija Americkih Drzava IV(8), AG/RES. 2040 (XXXIV-O/04), 2004. http://www.oas.org/juridico/english/ga04/agres_2040.htm, preuzeto 15. travnja 2019.
[74] Organizacija Američkih Država, *A comprehensive Inter – American Cybersecurity Strategy: A multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity,* Dodatak A, 2004.
[75] Ibid.

zakonska rješenja koja kriminaliziraju kibernetičke napade i pri tome pomažu u međunarodnoj suradnji na istrazi i progonu takvih zločina.[76] Radna skupina je pregledala napretke država postignute u provedbi navedenih mjera na svojim sljedećim sastancima.[77] Najaktualniji napori u sferi kibernetičkog kriminala Organizacije Američkih Država jesu pokretanje svjetskog mjeseca svjesnosti o kibernetičkoj sigurnosti u listopadu 2017. godine.[78] Tijekom predstavljanja projekta međunarodni stručnjaci i vlade fokusirali su se na ključna pitanja kibernetičke sigurnosti. Program je imao različite teme, no najbitnije je istaknuti održavanje sigurnosti građana na mreži, te kooperacija vlade i privatnog sektora na postizanju većih razina sigurnosti interneta, kako je to istaknuo glavni tajnik Organizacije Američkih država, Luis Almagro.[79] OAS je započeo koristan regionalni razgovor o zajedničkim strategijama za borbu protiv dijela kibernetičkih napada koji čine kibernetički kriminal. Ipak, bitno je napomenuti da još nije razvijen generalni aktivni program za rješavanje kibernetičkih napada medu članicama OAS-a.

2.4.5. Šangajska Organizacija za Suradnju

U neposrednim godinama nakon osnivanja 2001. godine, Šangajska Organizacija za suradnju (SCO) privukla je veliku pozornost međunarodne zajednice. SCO uključuje Kinu, Rusku Federaciju i države srednje Azije, Kazahstan, Kirgistan, Tadžikistan i Uzbekistan. Njezine otvorene aktivnosti usmjerene su na transnacionalne prijetnje te gospodarski i infrastrukturnu suradnju.[80] Šangajska Organizacija za suradnju također je poduzela značajne preliminarne korake prema suradnji u području kibernetičke sigurnosti. Pitanje kibernetičkog rata dodatno se komplicira činjenicom da države imaju različite koncepcijske pristupe i prioritete u raspravi o definicijama. Članovi Šangajske organizacije za suradnju definirali su kibernetički rat kao širenje informacija "štetnih za duhovnu, moralnu i kulturnu sferu drugih država".[81] Za razliku od zapadnih zemalja koje imaju različite prioritete i otvorene su prema slobodi govora i protoku informacija, države SCO-a strahuju da bi sloboda informiranja i prodiranje političkih ili vjerskih ideja kroz kibernetičke mreže mogla destabilizirati nacionalna društva i

[76] Šesti sastanak Radne skupine za Kibernetički kriminal, 2010. Washington DC. http://oas.org/juridico/english/cyb_VIrec_en.pdf, preuzeto 20. travnja 2019.
[77] Ibid.
[78] http://www.oas.org/en/media_center/press_release.asp?sCodigo=AVI-129/17, preuzeto 20. travnja 2019.
[79] Ibid.
[80] Bailes, Alyson J.K., Dunay, Pal, Guang, Pan, Troitskiy, Mikhail, *The Shanghai Cooperation Organization*; Švedska, Svibanj, 2007.
[81] Šangajski sporazum o suradnji između država članica u suradnji na području osiguravanja međunarodne informacijske sigurnosti; članak 2, stavak 5, ; Rusija, 2008.

postati smrtna prijetnja opstanku državnog režima.[82] Organizacija u svojoj deklaraciji iz Ekaterinburga od 16. lipnja 2009. godine ističe da "značaj pitanja osiguravanja međunarodne informacijske sigurnosti kao jednog od ključnih elemenata zajedničkog sustava međunarodne sigurnosti"[83] Kao takva, Organizacija predstavlja potencijalno težište internacionalne pravne regulative u borbi protiv kibernetičkih napada.[84]

Na kraju ovog odlomka treba zaključiti da su međunarodne aktivnosti za reguliranje kibernetičkih napada i kibernetičke sigurnosti još uvijek u početnoj fazi tj. fazi rasta. Iako većina međunarodnih sporazuma nije otišla dalje od pukog raspravljanja o budućim strategijama, možemo izvesti zaključak da široko rasprostranjeni napori pokazuju kvantitativno i kvalitativno veći interes za uspostavom internacionalnih propisa za regulacijom kibernetičkih napada. Fokus bi za početak definitivno trebalo staviti na definiranje opsega aktivnosti koje bi trebalo rješavati internacionalnim sporazumima.[85] Budući napori međunarodne zajednice inspirirati će i domaće zakonodavce brojnih država u kvalitetnijoj regulaciji atraktivnog pitanja kibernetičkog ratovanja i kibernetičke sigurnosti. U sljedećem poglavlju razmatra se regulacija kibernetičke sigurnosti domaćim zakonima Republike Hrvatske.

3. RH vs. Kibernetički kriminal

3.1 Informacijska sigurnost u RH

Republika Hrvatska nema u svome zakonodavstvu zaseban sustav koji se bavi sigurnosti kibernetičkog prostora već isti štiti kroz sustav informacijske sigurnosti kao i druge sigurnosne sustave (primjerice subjekti unutar bankarskog sektora posjeduju vlastite

[82] Trezza, Carlo, *A Negotiation on Cyber Warfare*; Italija, 2013., str 4.
[83] Šangajska Organizacija za suradnju, Ekaterinburg, Deklaracija šefova država članica Šangajske organizacije za suradnju, Generalni konzulat Uzbekistana u New Yorku; 2009. Godine; dostupno na www.uzbekconsulny.org/news/572/
[84] Hathaway, A. Oona, Crootof, Rebecca, Levitz Phillip, Nix Haley, Nowlan Aileen, Perdue, William, Spiegel, Julia. *The Law of Cyber – Attack,* SAD, 2012., str. 53
[85] Hathaway, A. Oona, Crootof, Rebecca, Levitz Phillip, Nix Haley, Nowlan Aileen, Perdue, William, Spiegel, Julia. *The Law of Cyber – Attack,* SAD, 2012., str. 54

sigurnosne sustave, pa tako i sustave u borbi protiv kibernetičkih prijetnji).[86] Pojam "kibernetički" uveden je u pravni poredak RH ratifikacijom Budimpeštanske konvencije o kibernetičkom kriminalu[87] još 2002. Godine. Slijedom toga, uvriježilo se koristiti pojam "kibernetički" u obliku pridjeva za nešto što uključuje, koristi ili je povezano s računalima, odnosno internetom.[88] Bitno je ukazati na to da iako RH ne poznaje pojmove vezane uz kibernetičku sigurnost (uz iznimku kibernetičkog kriminala prethodno navedenu), shodno čemu se može ocijeniti kako takvu vrstu sigurnost provodi uglavnom kroz sustav informacijske sigurnosti jer u okvir tehničke razine mjera informacijske sigurnosti spada i informatička sigurnost, što je u hrvatskom sustavu informacijske sigurnosti najbliži pojam pojmu kibernetičke sigurnosti.[89] Republika Hrvatska, to jest njezino Ministarstvo vanjskih i europskih poslova se u posljednjih nekoliko godina angažira u međunarodnim organizacijama kao što su UN, OESS, NATO i EU unutar kojih se aktivno radi na kibernetičkoj sigurnosti. Iz toga se može zaključiti kako pitanje kibernetičke sigurnosti postaje sve značajnije u međunarodnoj zajednici i time važno za Republiku Hrvatsku. „Do sada nisu napravljena istraživanja o ovisnosti kritične infrastrukture Republike Hrvatske o informatičkim tehnologijama, mrežama i kibernetičkom prostoru, te njezinoj ranjivosti spram kibernetskih ugroza, čime se otvara niz pitanja vezanih uz razinu i kvalitetu spremnosti sustava da odgovori na ozbiljnije ugroze u kibernetskom prostoru."[90] Sigurnosno – obavještajna agencija Republike Hrvatske (SOA) u svom posljednjem izvješću na temelju analiza navodi kako je detektirano najmanje sedam pokušaja državno sponzoriranih kibernetičkih napada na zaštićene informacijske i komunikacijske sustave državnih tijela Republike Hrvatske.[91] Namjera napadača je dvojaka: prikupiti podatke o hrvatskim sigurnosnim, političkim, gospodarskim i drugim procesima, te podatke euroatlantskih asocijacija kojih je Republika Hrvatska članica.[92] Samo jedan od nekolicine slučajeva kibernetičkih napada u Republici Hrvatskoj desio se 2014. Godine kada je Hrvatska narodna banka izvjestila je da su hakeri ukrali preko 1,8 milijuna kuna na način što su pomoću malicioznog softvera došli do podataka na računalima građana RH i tako pristupili njihovim računima na internet bankarstvu.

---

[86] Vuković, Hrvoje, *Kibernetska Sigurnost i Sustav Borbe Protiv Kibernetskih Prijetnji u Republici Hrvatskoj*, Svezak 13, br. 3, 2012.

[87] Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu (NN broj 09/02) i Zakon o potvrđivanju dodatnog protokola uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava (NN broj 04/08)

[88] Nacionalna strategija kibernetičke sigurnosti; Zagreb, listopad 2015., NN108/2015.

[89] Ibid.

[90] Ibid.

[91] https://www.soa.hr/hr/vijesti/, preuzeto 23. travnja 2019.

[92] Ibid.

3.2. Zakoni i drugi oblici regulacije

U Republici Hrvatskoj postoji brojnost zakona, strategija, akcijskih planova, programa, uredbi i pravilnika koji uređuju pitanje informacijske (kibernetičke) sigurnosti kako na direktan tako i na indirektan način. Republika Hrvatska ratificirala je Konvenciju o kibernetičkom kriminalu Vijeća Europe iz 2001. godine, te je njezine odredbe unijela u svoj Kazneni zakon donošenjem Zakona o izmjenama i dopunama kaznenog zakona. Ostali zakoni kojima se vide dosezi Republike Hrvatske u sferi kibernetičke sigurnosti su **Zakon o sigurnosno - obavještajnom sustavu** (NN 79/06 i 105/06) kojim su osnovane Sigurnosno-obavještajna agencija (SOA) I Vojna sigurnosno-obavještajna agencija te Zavod za sigurnost informacijskih sustava. Ovim zakonom Ured Vijeća za nacionalnu sigurnost proglašen je "središnjim državnim tijelom odgovornim za utvrđivanje i provedbu aktivnosti vezanih za primjenu mjera i donošenje standarda informacijske sigurnosti u državnim tijelima u Republici Hrvatskoj".[93] Zatim **Zakon o tajnosti podataka** (NN 79/07) koji određuje stupnjeve tajnosti (vrlo tajno, tajno, povjerljivo, ograničeno), pojam klasificiranih i neklasificiranih podataka, mogućnosti pristupa tim podatcima te zaštita i nadzor istih. **Zakon o informacijskoj sigurnosti** (NN 79/07) uređuje "pojam informacijske sigurnosti, mjere i standarde informacijske sigurnosti, područja informacijske sigurnosti, nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti"[94] Ovaj zakon u svom sadržaju navodi sigurnosnu provjeru, fizičku sigurnost i sigurnost podataka, zatim određuje način postupanja s klasificiranim podatcima, te posljedice postupanja nakon neovlaštenog pristupanja i korištenja podatcima. **Zakon o zaštiti osobnih podataka** (NN 41/08) kojim se uređuje zaštita osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korištenjem istih u Republici Hrvatskoj. Svrha zaštite je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Drugi značajni zakoni su Zakon o elektroničkoj trgovini (NN 173/03), Zakon o elektroničkim komunikacijama (NN 73/08) i Zakon o kaznenom postupku.

Nacionalni program informacijske sigurnosti iz 2005. Godine definira ciljeve informacijske sigurnosti na razini RH, nadležnosti i poslove pojedinih institucija u području informacijske sigurnosti kao i potrebnu međusobnu koordinaciju čimbenika informacijske

[93] Hrvatski Sabor, 2006.
[94] Hrvatski Sabor, 2007.

sigurnosti.[95] U prvom planu ovaj dokument bavi se organizacijskim i upravljačkim aspektima uvođenja sustava informacijske sigurnosti u RH. Nacionalni program informacijske sigurnosti od 2005, godine do danas bio je uspješan na polju pravnog i institucionalnog uređenja informacijske sigurnosti jer su upravo iz njega proizašli brojni propisi koji kasnije donose nužne izmjene i poboljšanja u regulaciji materije, no ipak plan o edukaciji i razvoju sigurnosne kulture, za sve razine formalnog obrazovanja i šireg građanstva, kako je naveden u programu, nije u potpunosti ispunjen.

Uredba Vlade RH kojom se propisuju i mjere kibernetičke sigurnosti je Uredba o mjerama informacijske sigurnosti (NN 46/08). Republika Hrvatska je 29. Rujna 2015. godine usvojila **Nacionalnu strategiju kibernetičke sigurnosti i Akcijski plan za njezinu provedbu**.[96] Nacionalna strategija kibernetičke sigurnosti je prva sveobuhvatna strategija na području kibernetičke sigurnosti u Republici Hrvatskoj, ali i najopsežniji i najsustavniji strateški dokument koji se odnosi na kibernetičku sigurnost na zapadnom Balkanu.[97] Cilj strategije je „...postići uravnoteženi i koordinirani odgovor različitih institucija koje predstavljaju sve sektore društva prema sigurnosnim prijetnjama u suvremenom kibernetičkom prostoru. Strategija prepoznaje vrijednosti koje treba zaštititi, nadležne institucije i mjere za sustavnu provedbu takve zaštite“.[98] Kao područja kibernetičke sigurnosti dobro su prepoznati elektronička komunikacijska infrastruktura i usluge, kritična komunikacijska i informacijska infrastruktura i upravljanje kibernetičkim krizama te kibernetički kriminal.[99] Strategija definira područja koja smatra najbitnijima, a to su: zaštita podataka, tehnička koordinacija u obradi računalnih sigurnosnih incidenata, međunarodna suradnja i obrazovanje i podizanje svijesti o sigurnosti u kibernetičkom prostoru.[100] Također, Strategija predviđa stvaranje Nacionalnog vijeća za kibernetičku sigurnost koji će imati velike nadležnosti u praćenju i koordinaciji provedbe Strategije. Osim toga, Vijeće će izdavati periodične procjene sigurnosti i definirati plan djelovanja u slučaju kibernetičke krizne situacije.[101] U Akcijskom

[95] Nacionalni program informacijske sigurnosti u RH; Zagreb, Ožujak 2005.
[96] Službeni glasnik Republike Hrvatske, Odluka Vlade o usvajanju Nacionalne strategije kibernetičke sigurnosne zaštite i Akcijskog plana za provedbu Strategije, NN 108/2015, www.uvns.hr, preuzeto 25. travnja 2019.
[97] Klaić, Aleksandra, *A Method for the Development of Cyber Security Strategies,* Hrvatska, 2015.
[98] https://enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/croatian-cyber-security-tratego/view, preuzeto 26. travnja 2019.
[99] Kezerić, Ana – Maria, Analiza prijetnji i rizika *cyber* sigurnosti Republike Hrvatske: Ranjivost informacijske sigurnosti; Zagreb 2017., str 29.
[100] Protrka, Nikola, Marić, Kristijan, Plecas, Mihael, *Challenges and Aspects of Cyber Security of the Republic of Croatia,* Acta Economica et Turistica; broj 3. 2017.
[101] Op. cit. bilj. 147.

planu za provedu Strategije ciljevi su razrađeni kroz konkretne mjere, rokove, nositelje provedbe mjera te pokazatelje uspješnosti provedbe, te su predviđene 74 mjere za implementiranje informacijske sigurnosti na području javnih elektorničkih komunikacija, elektroničke uprave, elektroničkih financijskih usloga, kritične komunikacijske i informacijske infrastrukture i upravljanja krizama, kibernetičkog kriminaliteta, zaštite podataka tehničke koordinacije u obradi računalnih sigurnosnih incidenata, međunarodne suradnje i obrazovanja, istraživanja, razvoja i jačanja svijesti o sigurnosti u kibernetičkom prostoru.[102] U skladu s Akcijskim planom za provedbu Nacionalne strategije kibernetičke sigurnosti Policijska akademija preuzela je ulogu educiranja, istraživanja i podizanja svijesti o sigurnosti kibernetičkog prostora.[103] Iako strategija propisuje potrebu snažnog javno-privatnog partnerstva, zasada nema dokaza o takvima u Republici Hrvatskoj.[104] Strateško planiranje kibernetičke sigurnosti u Republici Hrvatskoj vođeno je smjernicama koje su predviđene od strane ENISA-e, vodećeg tijela Europske Unije na području kibernetičkih pitanja.[105] Prema Izvješću o provedbi strategije nacionalne sigurnosti Republike Hrvatske iz siječnja 2019. godine stanje sigurnosti u RH je stabilno i nema vidljivog potencijala njegovog značajnog narušavanja, a glavni izazovi su nedovoljno stavilno jugoistočno susjedstvo i krizna žarišta u europskom okruženju. Početkom 2018. Godine pristupilo se jačanju kapaciteta kroz ustrojavanje novih ustrojstvenih jedinica Ministarstva unutarnjih poslova u Ravnateljstvu policije i to Službe kibernetičke sigurnosti i Odjela za informacije o putnicima u zračnom prometu.Prilagođavajući se novim sigurnosnim izazovima i prijetnjama poput prijetnji u kibernetičkom prostoru, hibridnih prijetnji i informacijskog ratovanja, kao i u cilju povećanja učinkovitosti i djelotvornosti te prilagođavanja novim strateškim aktima, Vojna sigurnosno-obavještajna agencija provela je preustroj i optimizaciju radnih procesa, aktivnosti i postupaka.[106]

3.3 Kaznena djela u sferi kibernetičkog ratovanja

[102] Kezerić, Ana – Maria, Analiza prijetnji i rizika *cyber* sigurnosti Republike Hrvatske: Ranjivost informacijske sigurnosti; Zagreb 2017., str 29.
[103] Op. cit. bilj. 151.
[104] Op. cit. bilj. 147.
[105] Cvitić, Ivan, Dragan, Peraković, Dragan, Periša, Marko, *An Overview of the Cyber Security Strategic Management in Republic of Croatia,* 2018.
[106] Izvješće o provedbi strategije nacionalne sigurnosti Republike Hrvatske, Vlada Republike Hrvatske; Siječanj 2019.

Kazneni zakon koji je u primjeni od 1. siječnja 2013. godine, za razliku od prethodnih kaznenih zakona donosi novinu u vidu posebne glave u kojoj su propisana kaznena djela iz područja računalnog kriminaliteta.[107] Glava dvadest i peta (XXV.) nosi naziv "Kaznena djela protiv računalnih sustava, programa i podataka". S obzirom da su u novi kazneni zakon preneseni opisi stavaka pojedinih kaznenih djela iz prethodnog kaznenog zakona, tako *de facto* novi kazneni zakon nije donio novine u odnosu na prethodni. U glavi XXV. predviđene su kazne i opisana su određena kaznena djela s područja računalnog kriminaliteta koje RH kriminalizira. Iz perspektive kibernetičkog ratovanja značajna su djela neovlaštenog pristupa, ometanja rada računalnog sustava, oštećenja računalnih podataka, neovlaštenog presretanja računalnih podataka,

3.3.1 Neovlašteni pristup

Članak 266. Kaznenog zakona propisuje kažnjavanje počinitelja djela neovlaštenog pristupa koje je ujedno opisano u ovom članku na način da se kažnjava osobu koja neovlašteno pristupi računalnom sustavu ili računalnim podacima i to kaznom zatvora do jedne godine. Kazneno djelo progoni se po prijedlogu. Zanimljiva je činjenica da ukoliko se sustav ostavi u potpunosti otvorenim neće biti kaznenog djela, što znači da ovaj članak štiti isključivo sustav koji ima zaštitne mjere.[108] U stavku dva navodi se kvalificirani oblik kaznenog djela neovlaštenog pristupa gdje je objekt radnje računalni sustav ili računalni podatci koji pripadaju tijelima državne vlasti, jedinicama lokalne ili područne (regionalne) samouprave, javne ustanove ili trgovačkog društva od posebnog javnog interesa, te se kažnjava kaznom zatvora do 3 godine. S obzirom da Konvencija o kibernetičkom kriminalu, čija je potpisnica Republika Hrvatska, u svom članku 11. stavku 2. traži da se kažnjava i pokušaj kaznenih djela iz ovog članka, Kazneni zakon propisuje kažnjavanje pokušaja u stavku 3. ovoga članka. Neovlašteni pristup daje hakerima mogučnost da pokvare, izmjene ili unište podatke stoga je to jedan od značajnijih načina kibernetičkih napada i ujedno dio kibernetičke sabotaže. Kibernetičku sabotažu definiramo kao dobivanjem pristupa mreži ili računalu ili sprječavanju

[107] Franjić, Siniša; Kaznena djela računalnog kriminliteta iz glave XXV. kaznenog zakona u RH; Pravne teme 10:105-114.; 2017.
[108] Franjić, Siniša; Kaznena djela računalnog kriminliteta iz glave XXV. kaznenog zakona u RH; Pravne teme 10:105-114.; 2017.

jednostavnog pristupa korisnicima sustava.[109] Neovlašteni pristup može se dobiti uz pomoć virusa ili malicioznog softvera postavljenog u računalni sustav.

3.3.2 Ometanje rada računalnog sustava

Ometanje rada računalnog sustava članak je 267. kaznenog zakona. Članak navodi da će se kazniti onaj tko onemogući ili otežа rad ili korištenje računalnog sustava, računalnih podataka ili programa ili računalnu komunikaciju. Propisana kazna zatvora za navedeno djelo je do tri godine. Također se navodi kažnjavanje pokušaja sukladno Konvenciji i kibernetičkom kriminalu čija je potpisnica Republika Hrvatska. U ovom zakonskom članku nalazimo jednu od specifičnosti vezanih uz računalni kriminalitet, a to je da se napadač može pustiti u distribuciju crva koji će se proširiti na tisuće drugih računala, koja će, onda bez znanja svojih korisnika, sudjelovati u napadu. To bi značilo da postoji mogućnost uporabe tuđe infrastrukture u počinjenju kaznenog djela, bez znanja vlasnika ili osoba koje koriste tu infrastrukturu.[110] Kibernetičke operacije i samim time kibernetički napadi odnose se, između ostalog, na ciljano korištenje digitalnog koda kako bi se ometalo rad računalnih programa s krajnjim ciljem da bi se oslabilo ili naudilo ciljanoj političkoj jedinici. U srpnju 2018. godine hakeri su ciljali kampanje najmanje dva kandidata američkih demokrata koristeći se DDoS[111] napadima kako bi prekinuli internet stranice kampanje.[112] Potencijalnim biračima bio je uskraćen pristup ključnim informacijama zbog provedenog ometanja rada.

3.3.3 Oštećenje računalnih podataka

U suvremenom gospodarskom poslovanju te u poslovanju javne uprave i drugih pravnih osoba sve češće se koriste elektroničke baze podataka te se brojne evidencije vode u elektroničkom obliku. Mnoge od tih baza podataka imaju iznimnu vrijednost, a njihova izmjena, uništenje ili brisanje čine takve podatke neupotrebljivim, te stoga mogu za posljedicu imati štetu velikih razmjera i društvene opasnosti.[113] Kibernetički rat postoji u vojnom i

[109] Clarke, Richard, Knake, Robert, *Cyber War: the next threat to national security and what to do about it*; SAD, 2012, str 79.
[110] Franjić, Siniša; Kaznena djela računalnog kriminliteta iz glave XXV. kaznenog zakona u RH; Pravne teme 10:105-114.; 2017.
[111] Eng. *Distributed denial of service* – distribuirano uskračivanje usluge
[112] *Cyber Attack Trends Analysis, Key insights to gear up for in 2019*.; 2019 *Security report*, SAD, 2019.
[113] Franjić, Siniša; Kaznena djela računalnog kriminliteta iz glave XXV. kaznenog zakona u RH; Pravne teme 10:105-114.; 2017.

obavještajnom području i odnosi se na vođenje vojnih operacija s cmetom informacija. To znači ometanje ili uništavanje informacijskih i komunikacijskih sustava s ciljem onesposobljavanja protivnika.[114] U Kaznenom zakonu članak 268. opisuje kazneno djelo oštećenja računalnih podataka na način da će se kaznom zatvora od tri godine kazniti onaj tko neovlaštenou cijelosti ili djelomično ošteti, izmjeni, izbriše, uništi, učini neupotrebljivim ili nedostupnim ili prikaže nedostupnim tuđe računalne podatke ili programe. U stavku drugom navodi se ujedno i kažnjavanje pokušaja navedenog kaznenog djela. Izmjena ili uništavanje podataka također je jedan od oblika kibernetičke sabotaže i ujedno (ali ne i nužno) posljedica neovlaštenog pristupa podatcima. Cilj se postiže uz pomoć virusa koji zaraze datoteku te uzrokuju štetu na datotekama ili uništenje istih primjenom programskih kodova.[115]

3.3.4 Neovlašteno presretanje računalnih podataka

Članak 269. opisuje kazneno djelo neovlaštenog presretanja računalnih podataka kao djelo koje se počinjava neovlaštenim presretanjem ili snimanjem nejavnih prijenosa računalnih podataka, uključujući i elektromagnetsku emisiju računalnog sustava, ali i na način da se drugome učine dostupnim tako pribavljeni podatci. Propisana je kazna zatvora do tri godine. Ovim stavkom izričito se zabranjuje prisluškivanje bežičnog prijenosa podataka, te prisluškivanje žičanog prijenosa koje je moguće izvesti bez izravnog priključenja na telekomunikacijski sustav.[116] Ovo kazneno djelo, u radovima inozemnih stručnjaka, smatra se djelom kibernetičke špijunaže. Navedena metoda kibernetičkog napada sastoji se od presretanja i preusmjeravanja prometa na lažne internetske stranice koje nisu poznate korisnicima.[117] Kibernetička špijunaža, pa samim time i neovlašteno presretanje računalnih podataka čest je oblik kibernetičkog napada među civilima, no nema velikog značaja među državnim subjektima.

[114] Schreif, Fred; *On Cyberwarfare*; SAD, 2015.
[115] Ozturk, Ozgur; *Digital Dark Side: Cyber warfare*; SAD, 2014.
[116] Franjić, Siniša; Kaznena djela računalnog kriminliteta iz glave XXV. kaznenog zakona u RH; Pravne teme 10:105-114.; 2017.
[117] Deibert, Ron, Rohozinski, Rafal, *Tracking Ghostnet: Investigating a cyber espionage network*; Kanada, 2009; str 19.

3.4 Tijela informacijske sigurnosti

Postoje brojna tijela u Republici Hrvatskoj koja se bave informacijskom sigurnosti, no ona najvažnija su Nacionalni CERT, Služba za sigurnost informacijskog sustava i Odjel za visokotehnološki kriminalitet. Među značajnim međunarodnim tijelima informacijske sigurnosti valjalo bi izdvojiti Agenciju Europske unije za mrežnu i informacijsku sigurnost te Europski centar za kibernetički kriminal.

2007. godine Republika Hrvatska je usvojila Zakon o informacijskoj sigurnosti kojim je predviđeno stvaranje nacionalnog CERT- a tzv. CARnet-a.[118] **Nacionalni CERT** je organizacija u Hrvatskoj koja se bavi očuvanjem informacijske sigurnosti.[119] CARnet je prethodnik Nacionalnog CERT-a osnovanog 1996. godine sa svrhom prikupljanja za očuvanje informacijske sigurnosti javnih informacijskih sustava na mreži podataka o računalno - sigurnosnim incidentima i rješavanju istih.[120] CERT reagira na računalno-sigurnosne incidente, te preventivnim djelovanjem radi na poboljšanju računalne sigurnosti informacijskih sustava, te objavljuje podatke o novim ugrozama. Godišnji izvještaj Nacionalnog CERT-a za 2018. godinu navodi kako su ostvareni značajni pomaci na području nacionalne i međunarodne suradnje, daljnjeg usavršavanje djelatnika te na području povećanja razine spremnosti na odgovor na sve složenije sigurnosne izazove.[121] Također postoji i vladin CERT pod nazivom ZSIS-CERT, koji se nalazi u Službi za sigurnost informacijskih sustava (ISBB). ISBB je središnje državno tijelo nadležno za tehnička područja informacijske sigurnosti državnih tijela Republike Hrvatske koja uključuje: stvaranje standarda informacijske sigurnosti, akreditacije sigurnosti, upravljanje kriptoznim materijalom koji se koristi za razmjenu klasificiranih informacija i koordinaciju prevencije, te uz sve navedeno odgovara na računalne prijetnje sigurnosti informacijskog sustava.[122] Uredbom o unutarnjem ustrojstvu Ministarstva unutarnjih poslova u Republici Hrvatskoj, koju je donjela Vlada RH u okviru PNUSKOKa, Službe gospodarskog kriminaliteta i korupcije, osnovan je **Odjel za**

[118] http://www.cert.hr/en/start, preuzeto 22. travnja 2019.
[119] https://www.cert.hr/onama/, preuzeto 22. travnja 2019.
[120] https://sigurnost.carnet.hr, preuzeto 23. travnja 2019.
[121] Godišnji izvještaj Nacionalnog CERT-a za 2018. godinu
[122] Minović, Adriana, Abusara, Adel, Eranda, Begaj, Erceg, Vladimir, Tasevski, Predrag, Radunović, Vladimir, Klopfer, Franciska, *Cybersecurity in The Western Balkans: Policy Gaps and Cooperation Opportunities;* Švicarska, 2016., str. 17.

visokotehnološki kriminal.[123] Djelokrug rada obuhvaća kako kaznena djela iz domene kibernetičkog kriminala koja Odjel prati, analizira i rješava, te izrađuje programe obuke policajaca za kibernetički kriminal.

2017. godine održana je i prva vojna vježba pod nazivom „Paukova mreža 2017" iz područja obrane od kibernetičkih napada na stacionirane i razmjestive komunikacijsko – informacijske sustave. „Cilj vježbe bio je uvježbati procese donošenja odluka, tehničke i operativne procedure i razmjenu informacija sudionika vježbe u području obrane od kibernetičkih napada", izjavilo je Ministarstvo obrane Republike Hrvatske.[124]

Političari u Republici Hrvatskoj govore u hibridnom ratu. „Po jednima, to je korištenje propagande, dezinformacija, hakerskih napada i informacijskog ratovanja da bi se ostvario neki politički, ekonomski i drugi ciljevima. Po drugima to je osmišljen, nadziran i centraliziran skup aktivnosti, otvoren ili prikriven, s kombinacijom vojnog i nevojnog djelovanja. Treća definicija je da je to kombinacija specijalnog rata i korištenja interneta"", rekao je državni tajnik u Ministarstvu unutarnjih poslova Robert Kopal. Premijer Andrej Plenković nedavno je ustvrdio kako se u Hrvatskoj vodi hibridni medijski rat te da postoji puno aktera koji žele destabilizaciju. Vlatko Cvrtila, stručnjak za sigurnost i obrambenu politiku smatra da se više radi o hibridnom djelovanju nego ratovanju – djelovanju preko medija, lažne vijesti, dezinformacije i slično.

Na kraju treba zaključiti da Republika Hrvatska ima strukturu obrane, no nedostaju joj resursi za bolju provedbu kako ističe Alen Delić, viši konzultant za informatičku sigurnost, „sustav uglavnom ima dobro postavljene organizacijske strukture, uključujući službe poput SOA-e, široj javnosti manje poznatog Zavoda za sigurnost informacijskih sustava, ali i dijelova Ministarstva unutarnjih poslova i Ministarstva obrane. Organizacijska nas struktura, međutim, neće obraniti".

[123] Republika Hrvatska, Ministarstvo unutarnjih poslova, Policijski nacionalni ured za suzbijanje korupcije i organiziranog kriminaliteta, Nadležnost i postupanje Ministarstva unutarnjih poslova u području zaštite prava intelektualnog vlasništva; Zagreb, studeni 2014.

[124] https://www.morh.hr/hr/vijesti-najave-i-priopcenja/vijesti/14506-provedena-vojna-vje%C5%BEba-paukova-mre%C5%BEa-2017.html, preuzeto 26. travnja 2019.

3. ZAKLJUČAK

U ovom radu sam pokušala objasniti kaznenopravne aspekte kibernetičkog ratovanja na što jednostavniji način, kako bi se čitatelji upoznali sa pojmom i pravnom regulativom te shvatili opasnost koja prijeti u 21. stoljeću. Nakon istraživanja različitih slučajeva i brojnih pravnih tekstova želim upozoriti na ono najbitnije, a to je da su ljudi danas apsolutno nesvjesni opasnosti uređaja i koliko su im podaci, imovina, pa i fizička dobrobit ugroženi. Nerealno je očekivati od svijeta da ozbiljno shvati prijetnju kibernetičkog rata s obzirom na to da ga niti jedna zemlja dosada nije službeno proglasila[125], ali internetsku sigurnost zaista treba shvatiti ozbiljnije, nego što se sada nalazi u svijesti građana. Zbog intenzivnog razvoja međunarodnih odnosa u kibernetičkom prostoru, ovo područje će uvijek biti zanimljivo i izazovno, a taj zaključak proizlazi iz stalne promjene stavova i tehnologije.[126] Većina autora, primjerice Thomas Reed smatraju da zapravo ni nećemo svjedočiti čistom kibernetičkom ratu u bližoj budućnosti te se nadaju da će sve ostati samo na hipotezama i pripremama za potencijalni sukob.[127] Međutim, s druge strane autori i stručnjaci često iznose predviđanja eskalacije sukoba i drugih obavještajnih aktivnosti u kibernetičkom prostoru te navode da su kibernetički napadi među najvećim prijetnjama međunarodnoj sigurnosti. Kibernetički prostor stvara jedinstveno bojno polje s mnogo izazova za ratno pravo i općenito pravnu regulaciju.[128] Nedavno objavljeni Tallinski priručnik je korisni vodič u ovom području, ali važno je naglasiti da nije obvezujući i ne daje iscrpan popis uputa.

Ostale organizacije slijede jedna drugu, bez ozbiljnih pomaka, usuđujem se reći „tapkajući u mraku“, a kada dođe do prijetnje ili sukoba, njihova aktivnost i rad se pokažu nestabilnima, nimalo u kontroli nad velikim silama. Zasada nam preostaje oslanjati se na znanstvena mišljenja, eventualne buduće rezolucije Vijeća sigurnosti i Opće skupštine UN- a, kao i na moguće presude ili savjetodavna mišljenja o tom pitanju od strane Međunarodnog suda pravde. Podsjećam na to da u *cyber* ratu napadači vjerojatno neće nositi uniformu, otvoreno nositi oružje, imati zapovjednika ili biti podvrgnuti unutarnjim disciplinskim postupcima. Ratno pravo treba proširiti tradicionalne kriterije za izravno sudjelovanje u *cyberspaceu*.

[125] Dunlap, C. J., *Perspectives for Cyber Strategists on Law for Cyberwar. Stratigic Studies Quarterly, 5:1*, 2013., str. 81.
[126] Duić, Cvrtila, Ivanjko, *International cyber security challenges*; Republika Hrvatska, 2017.
[127] Reed, Thomas, *Cyber War Will Not Take Place,* Oxford, 2013, str.187.
[128] https://www.thebalancecareers.com/law-of-armed-conflict-loac-3332966, preuzeto 29. travnja 2019.

Koristeći strogu interpretaciju načela, napadnute države nemaju nikakvo pravo da uzvrate protiv većine *cyber* napada, a smatram da je to nepoželjna situacija. Vlade širom svijeta s druge strane, znaju koliko je digitalni prostor važan, te vojnim snagama kontroliraju tu sferu, smanjujući troškove obrane u drugim područjima, brzo stvarajući *cyber* snage kojima bi obranili svoje virtualne teritorije i napali one svojih suparnika. Unatoč tome, ono što je zajedničko civilima i Vladama je to da nitko nije svjestan koliko je kiberprostor važan, barem u sigurnosnim okvirima, pošto ni približno ova nova sfera ratovanja nije dosegla svoj vrhunac. Je li to samo nova periferija ratovanja, kazalište za hladni rat 21. stoljeća koji će se voditi nevidljivo i gotovo bez posljedica u stvarnom svijetu? Ili nastaje kao najvažniji borbeni prostor informacijske dobi, kritična domena u kojoj će se pobijediti i izgubiti budući ratovi?
Zbog porasta kibernetičkog kriminala generalno, a i prijetnje od mogućeg kibernetičkog rata potrebno je bolje organizirati sustavno obrazovanje te ojačati operativne vojne, obavještajne policijske i civilne centre za obranu od kibernetičkih napada[129] ali i pristupiti strukturiranijoj i konkretnijoj pravnoj regulaciji problema. Nadam se da će pravo 21. stoljeća naći odgovor na sva pitanja i biti spremno kada kibernetički rat doživi svoj vrhunac i napadne ono najvrijednije – mir u svijetu.

[129] Duić, Cvrtila, Ivanjko, *International cyber security challenges*; Republika Hrvatska, 2017.

4. ZAHVALE

Autorica ovog rada se zahvaljuje...

Mentoru doc. dr. sc. Aleksandru Maršavelskom, koji mi je bio od nemjerljive pomoći, te od samog početka sa velikim entuzijazmom prihvatio mentorstvo. Svojim savjetima, komentarima, podrškom i strpljenjem vodio me je kroz stvaranje ovog rada i obradu ovako kompleksne teme. Njegova pristupačnost i predanost djelovale su ohrabrujuće i motivacijski, što mi je uvelike pomoglo pri stvaranju rada.

Djelatnicima Nacionalne sveučilišne knjižnice u Zagrebu na stručnoj pomoći pri nalaženju literature i ustupu iste.

Djelatnicima knjižnice Pravnog fakulteta u Zagrebu na usmjerenju pri pronalasku studije slučajeva.

Kolegama s fakulteta, posebno Ana-Mariji, Denisu, Juraju, Marku i Petri koji su mi beskrajno pomogli svojim savjetima i prijateljstvom.

Anti, na ljubavi, strpljenju i poticajima da proširim svoje znanje i vidike izvan isključivo pravne sfere.

Na kraju, hvala mojoj obitelji na strpljenju i razumijevanju tokom studiranja.

5. POPIS LITERATURE

1. Adkisson, James, *And others Law of Armed Conflict: Implications for Navy Cyber Strategy*; SAD, 2012.
2. Andress, *What is Cyber Warfare?* ; SAD, 2011.
3. *Atlantic Council, Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures* (Nexus rizika: prijetnja od kibernetičkih rizika? gospodarske koristi i troškovi alternativnih kiberbudučnosti), 10. Rujna 2015.
4. Bailes, Alyson J.K., Dunay, Pal, Guang, Pan, Troitskiy, Mikhail, *The Shanghai Cooperation Organization*; Švedska, Svibanj, 2007.
5. Bijela kuća, *Cybersecurity spending fiscal year 2019* (Potrošnja na kibersigurnost u fiskalnoj godini 2019.)
6. Brangetto, Pascal, Kert-Saint Aubyn, Mari, *Economic Aspects of National Cyber Security Strategies*; Estonija, 2015.
7. CfUS, *international strategy for Cyberspace* (broj 24) str 9.
8. Clarke, Richard A.; *Cyber War*; SAD, 2010.
9. Clarke, Richard, Robert, Knake. *Cyber war: the next threat to national security and what to do about it.* SAD, 2012.
10. Cvitić, Ivan, Peraković, Dragan, Periša, Marko, *An Overview of the Cyber Security Strategic Management in Republic of Croatia,* 2018.
11. *Cyber Attack Trends Analysis, Key insights to gear up for in 2019*.; 2019 *Security report*, SAD, 2019.
12. *Cybersecurity Best Practices Guide, for IIROC Dealer Members*; Kanada 2018.
13. Deibert, Ron, Rohozinski, Rafal, *Tracking Ghostnet: Investigating a cyber espionage network*; Kanada, 2009.
14. Dragičević, Kaspersen, Schwerha, *Article 15: Conditions and Safeguards under the Budapest Convention on Cybercrime*; 2012. Str. 3.

15. Duić, Cvrtila, Ivanjko, *International cyber security challenges*; Republika Hrvatska, 2017.
16. Dunlap, C. J., *Perspectives for Cyber Strategists on Law for Cyberwar. Stratigic Studies Quarterly,* 2013.
17. Dunlap, C. J., *Perspectives for Cyber Strategists on Law for Cyberwar. Stratigic Studies Quarterly, 5:1*, 2013.
18. *Dutch national cyber security agenda* - https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-1, preuzeto 15. Lipnja 2109.
19. Erbschloe, Michael, Vacca, John, *Information warfare: How to survive cyber attacks*; SAD, 2001.
20. *European Network and Information Security Agency* ili skraćeno ENISA agencija je Europske unije koja se bavi pitanjima sigurnosti informacija i informacijskih mreža
21. Europska komisija, Radni dokument službi komisije: Procjena učinka priložena Prijedlogu uredbe Europskog parlamenta i Vijeća o uspostavi programa Digitalna Europa za razdoblje 2021-2027, SWD (2018) 305 FINAL, 6. Lipnja 2018.
22. Franjić, Siniša; Kaznena djela računalnog kriminliteta iz glave XXV. kaznenog zakona u RH; Pravne teme 10:105-114.; 2017.
23. Gervais, M.. *Cyber Attacks and the Laws of War*, 30 BJIL, 2012.
24. Gladyshev, P., Marrington, A., Baggili, I., *Digital Forensics and Cyber Crime,* Fifth International Conference, Revised Selected Papers, Moskva, 2014.
25. Hathaway, A. Oona, Crootof, Rebecca, Levitz, Phillip, Nix Haley, Nowlan, Aileen, Perdue, William, Spiegel, Julia. *The Law of Cyber – Attack,* SAD, 2012.
26. Healey, Jason, Leendert van Bochoven, *Atlantic Council, NATO's Cyber Capabilities*, Yesterday, Today, and Tomorrow, at 2, 2012.
27. Henkin, Louis, *How Nations Behave*; SAD, 1978.
28. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.477.2090&rep=rep1&type=pdf
29. http://ipacso.eu/downloads/public-deliverables.html http://oas.org/juridico/english/cyb_VIrec_en.pdf
30. http://www.cert.hr/en/start
31. http://www.eca.europa.eu, http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914- policy-cyberdefence.pdf

32. http://www.oas.org/en/media_center/press_release.asp?sCodigo=AVI-129/17 http://www.oas.org/juridico/english/ga04/agres_2040.htm. *http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-reportlamc.pdf*
33. https://ccdcoe.org/
34. https://en.wikipedia.org/wiki/Tallinn_Manual
35. https://enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/croatian-cyber-security-trategy/view
36. https://narodne-novine.nn.hr/clanci/medunarodni/2002_07_9_119.html
37. https://sigurnost.carnet.hr
38. https://www.cert.hr/onama/
39. https://www.morh.hr/hr/vijesti-najave-i-priopcenja/vijesti/14506-provedena-vojna-vje%C5%BEba-paukova-mre%C5%BEa-2017.html
40. https://www.nato.int/cps/en/natolive/news_85161.html
41. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf
42. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf
43. https://www.soa.hr/hr/vijesti/
44. https://www.thebalancecareers.com/law-of-armed-conflict-loac-3332966
45. Izazovi u pogledu djelotvornosti kibersigurnosne politike EU-a; http://www.eca.europa.eu, preuzeto 16. Lipnja 2019.
46. Izvješće o provedbi strategije nacionalne sigurnosti Republike Hrvatske, Vlada Republike Hrvatske; Siječanj 2019.
47. Keane Woods, Andrew, *The Tallinn Manual review,* USA, 2017.
48. Kezerić, Ana – Maria, Analiza prijetnji i rizika *cyber* sigurnosti Republike Hrvatske: Ranjivost informacijske sigurnosti; Zagreb 2017.
49. Killerby, Margaret, *The Convention on Cybercrime*, USA, 2006.
50. Klaić, Aleksandar, *A Method for the Development of Cyber Security Strategies,* Hrvatska, 2015.

51. Košutić, Dejan, Primjena normi informacijske sigurnosti na primjeru HEP-a. U: Krajcar, Slavko (ur) Energetska sigurnost i kritična infrastruktura (161-171). Zagreb: Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva. , 2009.
52. *Latin American and Caribbean Cybersecurity Trends*, Report, Washington, DC: Organization of American States Secretariat for Multidimensional Security, 2014.
53. Libicki, Martin, *Conquest in Cyberspace: National security and information warfare*; Ujedinjeno Kraljevstvo, 2007.
54. Libicki, Martin, *Cyberdeterrence and cyberwar*; SAD, 2009.
55. Mačak, Kubo, *Is the international law of cyber security in crisis?;* Ujedinjeno Kraljevstvo, 2016, str. 132.
56. McGhee, E., J., *The Schmitt Analaysis, Tallinn Manual and US Cyber Policy*, Journal of Law & Cyber Warfare, vol. 2, izd. 1, 2013.
57. Minović, Adriana, Adel, Abusara, Eranda, Begaj, Erceg, Vladimir, Tasevski, Predrag, Radunović, Vladimir, Klopfer, Franciska, *Cybersecurity in The Western Balkans: Policy Gaps and Cooperation Opportunities*, Švicarska, 2016.
58. NATO, *Defending the Networks*, The NATO Policy on Cyber Defence, 2011.
59. NATO; Centar izvrsnosti za suradnju u obrani od kibernetičkih napada. *Tallinnski priručnik o međunarodnom pravu primjenjivom na kibernetičko ratovanje*.
60. NATO. *Policy on Cyber Defence*
61. NNATO, *Lisbon Summit Declaration* para. 2, 2010. http://www.nato.int/nato_static/assets/pdf/pdf_2010_11/2010_11_11DE1DB9B73C4F9BBFB52B2C94722EAC_PR_CP_2010_0155_ENGSummit_LISBON.pdf.
62. Organizacija Američkih Država IV(8), AG/RES. 2040 (XXXIV-O/04), 2004.
63. Organizacija Američkih Država*; A comprehensive Inter – American Cybersecurity Strategy: A multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity*; Dodatak A, 2004.
64. Owen, Bowcott, *The Guardian,* https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4
65. Ozturk, Ozgur; *Digital Dark Side: Cyber warfare*; SAD, 2014.
66. Perrit, Henry H., *The internet as a threat to sovereignty? Thoughts on internet role in strenghtening national and global governance*, Sjedinjene Američke Države, 1998.
67. Pleskonjić, Dragan, *Cyberwar: Pearl Harbor*, Tallinn Manual, Srbija, 2009.
68. Protrka, Nikola, Marić, Kristijan, Plecas, Mihael, *Challenges and Aspects of Cyber Security of the Republic of Croatia,* Acta Economica et Turistica, broj 3. 2017.

69. Prpić, Ratimir, *Osvrt na Tallinnski Priručnik u Međunarodnom pravu primjenjivom na kibernetičko ratovanje,* Zagreb, 2017.
70. Reed, Thomas, *Cyber War Will Not Take Place,* Oxford, 2013.
71. Republika Hrvatska, Ministarstvo unutarnjih poslova, Policijski nacionalni ured za suzbijanje korupcije i organiziranog kriminaliteta, Nadležnost i postupanje Ministarstva unutarnjih poslova u području zaštite prava intelektualnog vlasništva; Zagreb, studeni 2014.
72. Reed, Thomas, *Cyber War Will Not Take Place,* Oxford, 2013.
73. Schreif, Fred; *On Cyberwarfare*; SAD, 2015.
74. Služba Europskog parlamenta za istraživanje, transatlantic cyber-insecurity and cyber crime. Economic impact and future prospects (transatlantska kibernetička nesigurnost i kiberkriminal. Gospodarski učinak i budući izgledi), PE 603.948, prosinac 2017.
75. Službeni glasnik Republike Hrvatske, Odluka Vlade o usvajanju Nacionalne strategije kibernetičke sigurnosne zaštite i Akcijskog plana za provedbu Strategije, NN 108/2015 (14. Prosinca 2015.) www.uvns.hr
76. Šangajska Organizacija za suradnju, Ekaterinburg, Deklaracija šefova država članica Šangajske organizacije za suradnju, Generalni konzulat Uzbekistana u New Yorku; 2009. Godine; dostupno na www.uzbekconsulny.org/news/572/
77. Šangajski sporazum o suradnji između država članica u suradnji na području osiguravanja međunarodne informacijske sigurnosti; članak 2, stavak 5, ; Rusija, 2008.
78. Šesti sastanak Radne skupine za Kibernetički kriminal, SAD, 2010.
79. Škrtić, Dražen, *Implementacija odredbi Konvencije o kibernetičkom kriminalu u hrvatsko Kazneno i Kazneno procesno pravo,* Karlovac, 2014.
80. Theohary, Catherine A., Rollins, John W., *Cyberwarfare and Cyberterrorism: In brief*; SAD, 2012.
81. Trezza, Carlo, *A Negotiation on Cyber Warfare*; Italija, 2013.
82. Vuković, Hrvoje; *Kibernetska Sigurnost i Sustav Borbe Protiv Kibernetskih Prijetnji u Republici Hrvatskoj,* Svezak 13, br. 3, 2012.
83. Waxman, Matthew, *Cyber Attacks as Force*, SAD, 2011.
84. Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu (NN broj 09/02) i Zakon o potvrđivanju dodatnog protokola uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava (NN broj 04/08)

85. Ziolkowski, Katharina, *'Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force'* , *2012 4th International Conference on Cyber Conflict;* 2016.

6. SAŽETAK

Isabella Rakonić napisala je rad pod nazivom „Kaznenopravni aspekti kibernetičkog ratovanja". Struktura rada sastoji od uvoda, razrade pojma kibernetičkog rata i kibernetičkog napada te zatim pojma kibernetičke sigurnosti i njezine zakonodavne i financijske pozadine. Pravnoj regulaciji kibernetičkog ratovanja rad je posvetio važno poglavlje gdje su istraženi razni internacionalni regulatorni režimi. U predzadnjem poglavlju rad se fokusira na stanje u Republici Hrvatskoj te iscrpno objašnjava strategije, tijela i kazneno zakonodavstvo primjenjivo u Republici Hrvatskoj na područje kibernetičkog ratovanja. Autorica ovog rada smatra da je tema kibernetičkog ratovanja od velike važnosti i aktualna u 21. stoljeću, a istovremeno premalo obrađena u radovima pravnika mlađih generacija, te apsolutno nedovoljno prisutna u svijesti građana Republike Hrvatske.

U uvodu autorica uvodi čitatelje u pojam kibernetičkog ratovanja i samu hipotezu rada. Nakon uvoda u temu, u drugom poglavlju iscrpno se pojašnjavaju pojmovi kibernetičkog rata i kibernetičkog napada, te potom slijedi obrada zakonske regulative gdje se na samom početku pojašnjava pojam i važnost pojma kibernetičke sigurnosti. Autorica je posvetila pažnju samoj pozadini donošenja zakona, kako s legislativne tako i sa financijske strane. Nakon analize brojnih internacionalnih instrumenata regulative, odabrana su ona međunarodno najznačajnija za svrhu ovog rada. Najvažniji pravni dokument je Tallinnski priručnik, koji je detaljno analiziran, počevši od razloga donošenja, posebnosti grupe stručnjaka koja ga je donijela, potom sama struktura Priručnika i njegov utjecaj i značenje na današnju regulaciju kibernetičkog ratovanja. Također obrađeni su i drugi pravni režimi internacionalnog karaktera koji direktno reguliraju kibernetičke napade kao što su Ujedinjeni narodi, NATO, Vijeće Europe i Organizacija Američkih Država. Posebna pažnja posvećena je problematici kibernetičkog ratovanja u Republici Hrvatskoj, gdje autorica rada upozorava na to da RH ima strukturu obrane, ali joj nedostaju resursi za bolju provedbu. Na samom kraju rada, u četvrtom poglavlju nalaze se završne riječi i zaključak. U zaključku je naglašeno kako,

iako dosada niti jedan sukob nije posljedica isključivo kibernetičkog napada, ne znači da u skorijoj budućnosti do toga neće doći, te jednako tako upućena je kritika na (ne)spremnost svjetskih organizacija na takav razvoj događaja. Također, autorica i na samome kraju izražava zabrinutost zbog posljedica koje može izazvati i najmanji sukob potaknut kibernetičkim napadom, unatoč tome što je takva mogućnost zasada samo hipoteza.

Ključne riječi: *računalna kaznena djela, kibernetičko ratovanje, Tallinn priručnik, kibernetička sigurnost, kibernetički napad, Kazneni zakon*