Stručni članak
Primljeno: 2. prosinca 2022.
https://doi.org/10.46672/zsl.7.8.11

Damir Prskalo*

KIBERNETIČKA SIGURNOST KAO KLJUČNA DETERMINANTA NACIONALNE SIGURNOSTI REPUBLIKE HRVATSKE

Sažetak

U radu se elaborira što je kibernetička sigurnost te zašto ona postaje ključna determinanta nacionalne sigurnosti Republike Hrvatske. Rad je podijeljen u nekoliko cjelina: nakon uvoda, u drugome dijelu objašnjavaju se ključni pojmovi, kao što su nacionalna sigurnost, kibernetički prostor te kibernetička sigurnost. Treći dio rada govori o klasifikaciji prijetnji, odnosno o vrsti prijetnji za kibernetičku sigurnost, o kibernetičkom ratovanju, kibernetičkom terorizmu, kibernetičkoj špijunaži i kibernetičkom kriminalu. Zadnji dio rada govori o kibernetičkim napadima na državne institucije i gospodarske subjekte u Republici Hrvatskoj te se iznosi primjer napada.

Ključne riječi: kibernetička sigurnost, nacionalna sigurnost, Republika Hrvatska, kibernetički prostor

1. Uvod

Danas je kibernetička sigurnost sve značajniji sigurnosni izazov s kojim se države moraju nositi. Republika Hrvatska u zadnjih par godina sve više postaje meta napada iz kibernetičkog prostora. Dakako, u prilog tomu idu i podaci koje objavljuje Sigurnosno-obavještajna agencija. Prema njihovom izvješću iz 2020. zabilježeno je 12 državno sponzoriranih napada na ciljeve u Republici Hrvatskoj. Tu se uglavnom radi o državno sponzoriranim napadima, odnosno APT napadima. Njihova zadaća je penetracija u informacijske sustave Ministarstva obrane, Ministarstva vanjskih poslova Republike Hrvatske te ostale institucije od egzistencijalnog državnog značaja (Sigurnosno-obavještajna agencija, 2020).

Osim kibernetičkih napada na državne institucije, treba spomenuti i napade na kritičnu infrastrukturu. Sami napadi na takvu infrastrukturu za sobom mogu ostaviti

* Damir Prskalo, mag. rel. int. et dip., doktorand na Ekonomskom fakultetu Sveučilišta u Zagrebu, daprskalo1994@gmail.com

ozbiljne posljedice ne samo u financijskom smislu, nego i na ljudskim životima. Zapadne države, kao i Republika Hrvatska, pod kritičnu infrastrukturu ubrajaju: financije, telekomunikacije, energetske sektore (opskrbu strujom, vodom i plinom) te promet (Vuković, 2012). To dovodi do same ideje kibernetičke sigurnosti, što nije otkrivanje kibernetičkih napada nego njihovo predviđanje, odnosno korištenje tehnologije kako bi se napadače moglo odvratiti od takvih namjera. Upravo zbog toga sve više država ne postavlja pitanje što ako se kibernetički napad dogodi, nego kada će se dogoditi i koju će možebitnu štetu taj napad proizvesti na sve dionike u sustavu. Svjedoci smo da više nisu samo države i velike kompanije postale mete napada, nego i mala poduzeća i pojedinci koji se koriste digitalnim tehnologijama. Cilj je rada pokrenuti pitanje postaje li kibernetička sigurnost uistinu važan dio nacionalne sigurnosti (Spremić, 2017). U nastavku ćemo objasniti što je kibernetička sigurnost, koje su moguće prijetnje za kibernetičku sigurnost te dati pregled stanja o kibernetičkoj sigurnosti u Republici Hrvatskoj.

2. Terminološke determinante

Sigurnost se smatra jednim od egzistencijalnih pitanja, bez sigurnosti nema opstanka ni za jednu zajednicu na svijetu. Drugim riječima, sigurnost je *conditio sine qua non* normalnog života i rada ljudi bilo gdje da se nalaze. Najjednostavnija definicija sigurnosti govori da je to odsutnost od štetnih ugrožavanja (Tatalović i Bilandžić, 2005: 4). Ujedno za sigurnost bi se moglo reći da je i socijalno konstruirana, odnosno da za različite dionike ima različito tumačenje, pri čemu se srž sigurnosti mijenja ovisno o okruženju u kojem se dionik nalazi (Djurkin-König i dr. 2020: 16). Upravo iz tog razloga nastaje pojam nacionalne sigurnosti jer je cilj svake države da bude sigurna, odnosno da država opstane. Pojam nacionalne sigurnosti prvi se put spominje u Sjedinjenim Američkim Državama četrdesetih godina 20. stoljeća, ali intenzivnije se počeo koristiti na kraju Drugog svjetskog rata, kada su na međunarodnu pozornicu stupile dvije supersile – SAD i SSSR (Tatalović i Bilandžić, 2005: 30). Definicija nacionalne sigurnosti prema američkom novinaru Walteru Lippmanu glasi „nacija je sigurna u mjeri u kojoj nije u opasnosti da mora žrtvovati ključne vrijednosti da bi izbjegla rat te je sposobna, ako je izazovu, da ih zadrži pobjedom u takvom ratu" (Collins, 2010: 17). Osim Waltera Lippmana definiciju nacionalne sigurnosti dao je i Giacomo Luciani prema kojoj je „nacionalna sigurnost sposobnost odolijevanja agresije izvana" (Collins, 2010: 17). Kako god definirali nacionalnu sigurnost, većina teoretičara slaže se da je cilj nacionalne sigurnosti što bolje iskoristiti nacionalne resurse radi ostvarivanja nacionalnih interesa i sigurnosti države (Tatalović, Grizold i Cvrtila, 2008: 21).

2.1. Kibernetički prostor

Cyberspace, odnosno kibernetički prostor pojam je novijeg datuma i označava sve ono što se odvija u virtualnom prostoru posredstvom globalno umreženih računala. Sam pojam *cyberspace* prvi je put u upotrebu stavio američki pisac William Gibson, koji je u svojoj knjizi izdanoj 1948. pod nazivom *Neuromancer*, opisao što je *cyberspace*. Kibernetički prostor istovjetan je stvarnom prostoru jer se ljudi u njemu mogu družiti i komunicirati putem različitih društvenih mreža (npr. *Facebook, Twitter, YouTube, Instagram, LinkedIn* i ostale mreže koje su namijenjene za to (Hrvatska enciklopedija, mrežno izdanje). Dobar primjer da kibernetički prostor postaje sve važnije sredstvo u suvremenom svijetu je i podatak da je od 2000. do 2010. broj ljudi koji koriste kibernetički prostor, odnosno internet, porastao s 360 milijuna na gotovo dvije milijarde korisnika. Osim za komunikaciju, kibernetički se prostor koristi i za druge aktivnosti. Primjeri takvih aktivnosti su međunarodno poslovanje gdje se na vrlo jednostavan način može trgovati uslugama i robom, zatim znanost, jer se pomoću kibernetičkog prostora mogu okupiti svi znanstvenici na jednom mjestu i razmjenjivati ideje u stvarnom vremenu (Vuković, 2012: 13). Izuzev gospodarskih aktivnosti, kibernetički se prostor može koristiti i u vojne svrhe pa je Združeni stožer oružanih snaga SAD-a u listopadu 2006. dao svoju definiciju kibernetičkog prostora kao „područja koje karakterizira upotreba elektroničkog i elektromagnetskog dijapazona za pohranjivanje, modificiranje i razmjenjivanje podataka, putem mrežnih sustava i povezanih fizičkih infrastruktura" (Vuković, 2012: 16).

Uz sve prednosti koje daje u suvremenom svijetu, kibernetički prostor predstavlja i značajan sigurnosni izazov. Sigurnosne prijetnje u kibernetičkom prostoru možemo podijeliti na četiri razine. Prva razina je kibernetski kriminal, duga razina je kibernetska špijunaža, treća razina je kibernetski terorizam i četvrta razina je kibernetičko ratovanje. Sve te ugroze su maliciozne, odnosno imaju zadatak naštetiti sustavima, npr. kritičnoj infrastrukturi, financijama, prometu, komunikacijama i ostalim osjetljivim sustavima (Vuković, 2012: 17–18).

2.2. Kibernetička sigurnost

Kibernetička sigurnost tema je koja već dugo zaokuplja pažnju mnogobrojnih znanstvenika, istraživača, ali i ljudi iz poslovnog svijeta. Argument koji govori tomu u prilog je taj da se sve više socijalnih interakcija odvija u kibernetičkim prostoru. To pokazuje i podatak da korisnici diljem svijeta pošalju preko 40 trilijuna e-poruka. Uz to, prema određenim procjenama broj uređaja koji su bili spojeni na internet iznosio je oko 8,7 milijardi u 2012., dok će prema nekim projekcijama broj uređaja koji će biti spojeni na internet u 2020. iznositi više od 40 milijardi, što je u konačnici frapantan podatak (Božinović, 2016: 123). Upravo iz tog razloga kibernetička sigurnost dobiva sve više na važnosti u svim segmentima života.

Sama ideja kibernetičke, odnosno *cyber* sigurnosti počiva na ideji holističkog modela, odnosno naučiti kako upravljati i osigurati nesmetano funkcioniranje informatičkog okruženja. Samo informatičko okruženje podrazumijeva tehnološke, organizacijske, društvene i ostale aspekte u odnosnu na klasične postupke informacijske sigurnosti. Naravno, i ovdje treba napraviti pojmovnu distinkciju između informacijske i kibernetičke sigurnosti (Spremić, 2017: 52). Pojam informacijske sigurnosti prema autorima Ivandić Vidović, Karlović i Ostojić (2011: 94) je sljedeći: „informacijska sigurnost podrazumijeva stanje povjerljivosti, cjelovitosti i raspoloživosti informacija, neovisno o tome u kojem obliku informacije egzistiraju, a postiže se primjenom odgovarajućih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere, i dorade tih mjera i standarda." Prema Središnjem državnom uredu za razvoj digitalnog društva (2022) „kibernetička sigurnost obuhvaća skup procesa, mjera i standarda kojima se jamči određena razina pouzdanosti pri korištenju proizvoda i usluga u kibernetičkom prostoru, pri čemu sustavna zaštita računala i računalnih mreža, informatičke i informacijske infrastrukture, mobilnih uređaja i podataka od malicioznih napada." Iz toga je vidljivo da kibernetička sigurnost postaje krucijalna stavka unutar nacionalne sigurnosti. Naime, danas su kibernetičke prijetnje sve više u porastu, a napadi postaju sve napredniji i složeniji te imaju reperkusije na naš svakodnevni život. Sama tipologija napada je različita, ali možemo reći da su to razni maliciozni programi, krađa osobnih i financijskih podataka, računalne prevare te zloupotreba raznih društvenih mreža (Središnji državni ured razvoj digitalnog društva, 2022).

3. Klasifikacija prijetnji za kibernetičku sigurnost

U ovome poglavlju detaljnije ćemo se pozabaviti klasifikacijom prijetnji za kibernetičku sigurnost. Da bismo mogli klasificirati prijetnje za kibernetičku sigurnost, najprije je potrebno napraviti pojmovnu distinkciju što je prijetnja. Definicija prijetnje prema Ahiću i Nađu (2017: 63) kaže da je „prijetnja potencijalni uzrok neželjenog incidenta, koji može dovesti do štete na sistemu ili organizaciji, odnosno projektu." Također, bitno je spomenuti da su prijetnje možebitni generator neizvjesnosti i ako nema prijetnji, nema ni ugroze za bilo koji sustav. Iz tog razloga potrebno je odmah na početku napraviti klasifikaciju prijetnji kako bi se kasnije na jednostavan način mogle identificirati. Drugim riječima, prilikom identifikacije prijetnji bilo bi poželjno da se koriste tri vrste identifikacije prijetnji: izvor prijetnji, lokacija i motivacija (Ahić i Nađ, 2017: 64).

Kad je riječ o prijetnjama kibernetičkoj sigurnosti, Vuković (2012: 17) ih dijeli na kibernetički kriminal, kibernetičku špijunažu, kibernetički terorizam i kibernetičko ratovanje. U pogledu metoda, napadi se mogu izvesti u dvjema varijantama: napad na podatke i napad na nadzorne sustave ili operativne tehnologije. Cilj napada na po-

datke je njihova krađa ili šteta i sabotiranje određene usluge, a takvi se napadi izvode putem računala ili interneta. Uzmimo kao primjer da netko provali u bolničku bazu podataka i ondje pacijentu promijeni terapiju lijekova koje treba dobiti. Upravo takav čin za sobom može ostaviti ozbiljne posljedice za pacijenata, ako je pacijent npr. alergičan na taj lijek ili ako ga dobije u većoj dozi od dozvoljene (Vuković, 2012: 17–18).

Nadalje, napad na nadzorne sustave također za sobom ostavlja nesagledive posljedice i takvi napadi se najčešće koriste za ugrožavanje kritične infrastrukture jedne države (npr. voda, plin, električna energija, prometu i sl.). Takvi napadi izvode se putem interneta ili penetracijom u sustave nadzora odnosno operativnih tehnologija, koje su ključne za mnoge industrije danas. Dobar je primjer napad u ožujku 2000. kada je bivši zaposlenik putem interneta ušao u nadzorni sustav otpadnih voda u gradu Queenslandu u Australiji i preko pumpi pustio milijun litara otpadnih voda u sustav za pitku vodu. Upravo je taj slučaj eklatantan primjer kako se može na vrlo jednostavan način ugroziti zdravlje milijuna ljudi koji koriste pitku vodu. U cijelom slučaju je šokantan podatak da je nakon samo 45 pokušaja izvršio penetraciju u sustav i pustio otpadnu vodu u sustav pitke vode, dakle ostala 44 pokušaja nitko na vrijeme nije detektirao (Vuković, 2012: 17–18).

3.1. Kibernetičko ratovanje

Univerzalna definicija kibernetičkog ratovanja odnosno *cyberwarfarea* ne postoji. Stoga ćemo, za bolje razumijevanje pojma i njegovih obilježja navesti nekoliko definicija. *Encyclopedia Britannica* kibernetičko ratovanje definira kao „rat koji se provodi pomoću računala i mreža koje ih povezuju, a sam rat provode države ili njihovi opunomoćenici protiv drugih država." Nadalje, glavni cilj kibernetičkog rata je poremetiti, uništiti ili uskratiti upotrebu vladinih i vojnih mreža (Sheldon, 2022). Da je takva vrsta rata zastrašujuća govore nam i dva primjera kibernetičkih napada. Prvi se napad dogodio na Estoniju 2007., nakon što je Estonija odlučila premjestiti spomenik sovjetskog vojnika iz parka u Talinu. Upravo je taj čin izazvao niz kibernetičkih napada na tu zemlju. Mete koje su napadači, u ovom slučaju hakeri, odabrali su sve važnije institucije za funkcioniranje države pa su tako pod napadom bile stranice vlade, medijske kuće, bankarski sustavi (Božinović, 2016: 126). Nedugo nakon tih napada, 8. kolovoza 2008. dogodio se napad i na Gruziju. Radilo se o DDos napadima, engl. *distributed denial-of-service attack*. Kao i kod Estonije, glavni cilj napada bile su vladine stranice, odnosno onemogućiti građanima pristup bilo kakvim uslugama. Bio je to prvi napad koji je bio koordiniran s kopnenom invazijom na Gruziju (Kovačević, 2013: 93). Upravo ti napadi potaknuli su NATO savez da kibernetičko ratovanje apostrofira kao ozbiljnu prijetnju za kritičnu infrastrukturu i druge segmente života te zbog toga može ubuduće aktivirati članak 5. Washintonskog sporazuma o obrani svojih članica (Božinović, 2016: 127).

Kada govorimo o obilježjima kibernetičkog rata govorimo o nekoliko ključnih determinanti koje ih razlikuju od klasičnih načina ratovanja, odnosno ratovanja na kopnu, moru i u zraku. U tom pogledu imamo četiri osnovna obilježja kibernetičkog rata: niski operativni troškovi, brisanje tradicionalnih granica, nepripisivost odgovornosti i utjecaj na široku publiku (Brzica, 2020: 20). Prvo obilježje govori o tome da je kibernetičko ratovanje znatno jeftinije od konvencionalnog napada koji za sobom nosi enormne troškove u pogledu angažmana ljudstva i vojne tehnike jer samo kibernetičko ratovanje ne zahtijeva veliki angažman ljudi i opreme, a njegovi učinci mogu imati ozbiljne posljedice za metu koja je pod napadom. Drugo obilježje kibernetičkog ratovanja je izostanak tradicionalnih granica jer se odvija u kibernetičkom prostoru gdje nema granica. Stoga postoji opasnost da napad može doći iz bilo kojeg dijela svijeta, a napadač se može vrlo lako prikriti, dok je treće obilježje nepripisivanje odgovornosti za izvedeni napad. Glavni problem je u tome što je identifikacija počinitelja vrlo otežana ako do napada dođe. Zato je vrlo teško raspoznati o kakvoj se vrsti prijetnji radi, je li to unutarnja ili vanjska prijetnja, radi li se o državnim ili nedržavnim akterima. Kada je riječ o kibernetičkom ratu, odnosno napadu, potrebno je ustanoviti od kuda je napad došao s visokom izglednošću, kako bi se moglo uzvratiti protumjerom. Zadnji obilježje kibernetičkog ratovanja je sposobnost utjecaja na široku publiku, odnosno da svaki takav napad koji je izveden može imati veliki odjek na percepciju sigurnosti. Tu posebno treba dodati društvene mreže koje postaju sve važnija sastavnica sukoba, kako na državnoj tako i na nedržavnoj razini (Brzica, 2020: 20–22).

Uz kibernetički rat bi također trebalo dodati i pojam hibridni rat. Tako NATO hibridni rat definira „kao ne klasičan vojni pristup koji uključuje specijalne snage, informacijske tehnologije u svrhu provedbe psiholoških operacija i zastrašivanja te upotrebu ne vojnih elemenata s ciljem širenja nesigurnosti i stvaranja unilateralne prednosti okupacijom ili aneksijom određenog područja" (Brzica, 2022: 122). Drugim riječima, ideja hibridnog rata počiva na činjenici da se napravi odmak od klasičnog načina uništavanja neprijatelja primjenom vojne sile do primjene kombinacija nevojnih metoda s ciljem dezintegracije protivnika, eksploatacije njegovih slabosti te širenje vlastitog narativa. Proces hibridnog rata odvija se u osam faza. Prva faza je nevojno asimetrično ratovanje, druga faza su specijalne vojne operacije, treća faza je zavaravanje i podmićivanje vladinih dužnosnika i vojnog vodstva, četvrta faza destabilizirajuća propaganda, a njezin cilj je izazvati nemir i nezadovoljstvo među građanstvom, peta faza je uspostava tzv. *no-fly* zone iznad zemlje koju se napada, šesta faza su vojne akcije, a njima prethode izviđačke i zadaće subverzije, sedma faza uključuje informacijske operacije, kibernetičko ratovanje i slično, a zadnja faza je uništenje preostalog otpora upotrebom specijalnih vojnih operacija (Brzica, 2022: 129–130).

3.2. Kibernetički terorizam

Kibernetički terorizam relativno je nova pojava i odnosi se na upotrebu terorističkih metoda u kibernetskom prostoru. Definicija kibernetičkog terorizma prema Vukoviću (2012: 18) je sljedeća: „kibernetički terorizam označava promišljene, političke motivirane napade izvršene od strane nacionalnih skupina ili prikrivanih čimbenika, odnosno pojedinaca, usmjerenih protiv informacijskih ili računalnih sustava, računalnih programa te podataka, a rezultat im je nasilje nad neborbenim metama." Kako je već rečeno, kibernetički terorizam se odvija u kibernetičkom prostoru, a cilj mu je fizičko uništenje određenih uređaja, sustava uređaja ili nekog poslovnog procesa gdje postoje računalni sustavi. Uzmimo kao primjer napad terorističke skupine Oslobodilački tigrovi tamilske domovine, odnosno njezine frakcije Internet Black Tigers, koja je u kolovozu 1997. napala sustav komunikacije veleposlanstava Šri Lanke diljem svijeta. Napad se odvijao tako da je frakcija napadala službenu komunikaciju, dolazilo je oko 800 spam e-mailova na dan što je rezultiralo onesposobljenom komunikacijom veleposlanstva. Upravo taj napad smatra se jednim od prvih terorističkih napada izvedenih u kibernetičkom prostoru (Vuković, 2012: 18).

Osim napada na vladine mrežne stranice, ostali sustavi koji mogu biti mete kibernetičkog terorizma su bolnice, nuklearna postrojenja, elektrane, sustavi za kontrolu leta i slični objekti od egzistencijalne upotrebe. Argument zašto su takvi napadi postali učestaliji je u tome što su znatno jeftiniji od klasičnih napada i ne zahtijevaju puno ljudi i opreme. Takav razvoj događaja, odnosno selidba terorističkih napada u kibernetički prostor postaje ozbiljna prijetnja svim državama. Samo zbog ilustracije uzmimo da ISIL ili Al-Kaida izvedu teroristički napad pomoću računalnih sustava na kritičnu infrastrukturu jedne zemlje. Takav možebitni napad bi za sobom ostavio ozbiljne posljedice s mogućim smrtnim ishodima. Nažalost, svjedoci smo da kritična infrastruktura u mnogim državama nije na dovoljnoj razini sigurnosti, odnosno da je više ulaganja bilo u fizičko-tehničku zaštitu nego u kibernetičku zaštitu. Zbog toga i ne iznenađuje činjenica da je Velika Britanija u svojoj strategiji nacionalne sigurnosti kibernetički terorizam uvrstila kao ozbiljnu sigurnosnu prijetnju. Osim strategije nacionalne sigurnosti i prema strateškom pregledu obrane Velike Britanije, za borbu protiv kibernetičkog terorizma izdvojili su gotovo 650 milijuna funti na razdoblje od četiri godine. Iz svega proizlazi da je kibernetički terorizam postao stvarnost, ali i budućnost, i samo suradnja država može pomoći u borbi protiv te nove sigurnosne ugroze. Evolucija informacijske tehnologije jedan je od glavnih generatora gospodarstva svih država, ali i odgovornost da se spriječi možebitno zloupotrebljavanje (Božinović, 2016: 128).

3.3. Kibernetička špijunaža

Kibernetički prostor danas predstavlja bitno područje svjetskog gospodarstva, ali istodobno sa sobom nosi i sve veće ugroze za kibernetičku sigurnost. Jedna od većih

ugroza je kibernetička špijunaža čiji je cilj neovlašteno prikupljanje podataka u kibernetičkom prostoru (Vuković, 2012: 13). Definicija kibernetičke špijunaže prema Buchanu (2019: 13) obuhvaća četiri ključna elementa: „(1) kopiranje povjerljivih informacija bez pristanka, (2) povjerljivih informacija, (3) koje imaju boravište u kibernetičkom prostoru ili (4) prolaze kroz kibernetički prostor." Kada govorimo o akterima kibernetičke špijunaže to nisu samo kriminalne skupine ili pojedinci, nego to mogu biti države ili neke strane kompanije koje prikupljaju informacije. Razlozi prikupljanja takvih informacija su mnogobrojni, ali u većini slučajeva odnosi se na nekoliko ključnih segmenata. Tako kibernetičkom špijunažom možemo doći do visoko tehnoloških podataka koji bi mogli pomoći u razvoju kompanije ili države, možebitna trgovina takvim informacijama trećim stranama ili kako bi te iste informacije iskoristile za političku ili vojnu premoć. Problem je ako kibernetičku špijunažu koriste države kako bi određene informacije iskoristile protiv neprijatelja. Tada možemo reći da je ugrožena sama nacionalna sigurnost te države (Mihaljević i Nađ, 2018: 96).

Metode koje se koriste u kibernetičkoj špijunaži slične su industrijskoj špijunaži. Primjer jedne tehnike je ubacivanje *malwara* u računalnu infrastrukturu kompanija ili državnih institucija. Nakon što je taj *malware* ubačen u ICT sustav, on ondje prikuplja podatke o kompaniji ili državnoj instituciji. Osim metoda, tu su i akteri koji mogu sudjelovati u kibernetičkoj špijunaži. Tako možemo uzeti primjer da neki visoko pozicionirani menadžer koji raspolaže informacijama kompanije ubaci *malware* kako bi vršio kibernetičku špijunažu (Mihaljević i Nađ, 2018). Kada govorimo o kibernetičkoj špijunaži bilo bi dobro spomenuti i *spyware*, odnosno softver čija je namjena da prikuplja podatke o korisniku te da bez njegovog znanja preuzme kontrolu nad računalnim sustavom (CERT, 2022). Jedan od najpoznatijih *spywarea* je Pegasus. Njega je razvila izraelska tvrtka s ciljem prikupljanja podataka o meti napada. Pegasus može snimati pozive i slike te prikupljati poruke i lozinke. Zanimljiva činjenica vezana za taj *spyware* jest da ga je razvila izraelska tvrtka NSO, grupa za borbu protiv terorizma i kriminala, ali nažalost, zabilježeni su i određeni slučajevi zloupotrebe tog softvera (CERT, 2022).

3.4. Kibernetički kriminal

Kibernetički kriminal najčešća je sigurnosna ugroza u kibernetičkom prostoru. Kibernetički kriminal pojavljuje se sredinom sedamdesetih godina prošlog stoljeća kada dolazi do značajnijeg razvoja računala. Naime, prva računala koja su bila razvijena bila su za upotrebu u vojne, znanstvene i tek nešto kasnije gospodarske svrhe. Upravo ta činjenica je onemogućavala da se bilo tko izvan tih organizacija može baviti kibernetičkim kriminalom (Bača, 2004). Sama definicija kibernetičkog kriminala prema Bači (2004: 22) kaže da je to „vrsta kriminalnog ponašanja kod kojeg računalna tehnologija predstavlja način izvršenja kaznenog dijela, ili se računalo upotrebljava kao

sredstvo izvršenja, a čime se ostvaruje neka kaznenopravna posljedica." Drugim riječima, za kibernetički kriminal bismo mogli reći da obuhvaća prevare u kibernetičkom prostoru. Najučestaliji način kibernetičkog kriminala je prevara na internetskom bankarstvu, odnosno krađa s kreditnih kartica, a određene procjene govore da takav oblik kriminala godišnje raste i do 40 %. Sama zarada od takve vrste kibernetičkog kriminala penje se na 100 milijuna dolara godišnje (Vuković, 2012: 20). Osim prevare putem internet bankarstva, postoje i drugi oblici kibernetičkog kriminala. To su *phishing* napadi, socijalni inženjering, zlonamjerni računalni programi, *keyloggersi* i *ransomware* (Spremić, 2017: 48).

4. Kibernetička sigurnost u Republici Hrvatskoj

Kao i druge zemlje u svijetu, i Republika Hrvatska suočava se sa sve većim kibernetičkim napadima. Razlog takvih napada je sve veća međuovisnost države, društva i gospodarskih subjekata o kibernetičkoj tehnologiji. Iz toga razloga kibernetička sigurnost sve više dobiva na važnosti u sklopu nacionalne sigurnost. Tako Sigurnosno-obavještajna agencija kroz svoja javna izvješća informira javnost o stanju kibernetičke sigurnosti u Republici Hrvatskoj (Sigurnosno-obavještajna agencija, 2019). Prvo javno izvješće Sigurnosno-obavještajne agencije datira iz 2014. u kojem SOA prvi put ukazuje na to da postoji mogućnost *cyber* napada na Republiku Hrvatsku. Razlog toga upozorenja leži u činjenici da se evolucijom tehnologije podatci koji su bitni za nacionalnu sigurnost pohranjuju te razmjenjuju putem ICT kanala te iz toga razloga postaju značajnije ranjivi (Sigurnosno-obavještajna agencija, 2014).

Poslije toga Sigurnosno-obavještajna agencija u svim svojim izvještajima od 2016. do 2020. kibernetičku sigurnost označava kao odlučujući izazov za nacionalnu sigurnost Republike Hrvatske. Detaljnijim uvidom u javno izvješće Sigurnosno-obavještajne agencije iz 2017. vidljiv je podatak da je tijekom 2016. zamijećeno čak sedam pokušaja državno sponzoriranih kibernetičkih napada na informacijsko-komunikacijske sustave državnih tijela u RH (Sigurnosno-obavještajna agencija, 2017). Samo četiri godine kasnije, SOA je detektirala čak 12 državno sponzoriranih napada na Republiku Hrvatsku. Glavni cilj takvih napada bio je proboj u informacijske i komunikacijske sustave ministarstava i drugih državnih tijela. Uz to, Republika Hrvatska je početkom 2020. predsjedala Vijećem EU-a, što je bila dodatna motivacija da se izvrše takvi napadi. Osim hrvatskog predsjedanja Vijećem EU-a, u svijetu je bila ozbiljna zdravstvena ugroza, odnosno pandemija COVID-19 koja je ubrzala digitalizaciju kako javne uprave tako i poslovanja, ali s tim je i povećan rizik od kibernetičkih napada na te sustave (Sigurnosno-obavještajna agencija, 2020).

Glavna motivacija takvih napada bio je proboj u informacijske sustave državnih institucija i gospodarskih subjekata u Republici Hrvatskoj. U većini slučajeva radi se

o državno sponzoriranim napadima, a njihova izvedba iziskuje visoki stupanj tajnosti te korištenje naprednih tehnologija, odnosno softvera. Kada promatramo namjeru napadača, ona uvijek ide u dvama smjerovima. Prvi smjer je prikupljanje određenih podataka hrvatskim političkim, gospodarskim i sigurnosnim procesima. Drugi smjer je prikupiti podatke o euroatlantskim organizacijama, gdje je Republika Hrvatska članica, prije svega o NATO-u i EU. Ukoliko bi takav napad prošao nezamijećen, za sobom može ostaviti ozbiljne reperkusije u fizičkom svijetu gdje čak mogu biti i ugroženi ljudski životi. Primjeri takvih napada su napad u Ukrajini gdje je napadnut elektrodistribucijski sustav, nadalje napadi u Velikoj Britaniji gdje su napadači napali britanski energetski i zdravstveni sektor (Sigurnosno-obavještajna agencija, 2017).

Kibernetičke napade možemo podijeliti u nekoliko kategorija koje su bitne za opstojnost države i njezine nacionalne sigurnosti. Prva kategorija su napadi na računalne sustave u vlasništvu državnih institucija (npr. vlada, zakonodavna tijela, ministarstva financija, obrane, policije, zdravstva itd.) Druga kategorija jesu napadi na računalne sustave u vlasništvu velikih gospodarskih subjekata (npr. međunarodne tvrtke). Treća kategorija su napadi na računalne sustave u vlasništvu financijskih institucija (npr. banke, HNB, burze i dr.). Zadnja kategorija su napadi na računalne sustave u državnim institucijama ili organizacijama (npr. elektroenergetika, telekomunikacije, opskrba vodom, opskrba plinom, odnosno sustavi kritične infrastrukture). Navedeni napadi na ključne sustave ozbiljno ugrožavaju nacionalnu sigurnost države (Bača, 2004). Najčešći oblici kibernetičkog napada prema Javnom izvješću SOA-e su APT napadi, odnosno *Advanced Persistent Threat*. Same APT napade obilježava nekoliko ključnih determinanti po kojima su poznati. Prva je svakako visoka stručnost napadača i nemogućnost detekcije na duže vremensko razdoblje. Takvi napadi su vrlo složeni te najčešće biraju mete od nacionalnog značaja za određenu državu. Uz to, većina tih napada dolazi iz trećih država jer je tako napadače teže detektirati, ali kasnije i procesuirati. Sam *modus operandi* APT napada je korištenje zlonamjernog softvera kojeg se nastoji unijeti preko nepostojećih internetskih poveznica, malicioznim USB-ovima ili putem lažnih, odnosno *phishing mailova*. Konačan cilj napada je krađa povjerljivih informacija ili onemogućavanje poslovanja te izazivanje financijske štete (Sigurnosno-obavještajna agencija, 2018).

4.1. Primjeri kibernetičkih napada u Republici Hrvatskoj

Kibernetički napadi svake su godine sve više u porastu, pa tako i u Republici Hrvatskoj. Prvi ozbiljniji kibernetički napad koji se trebao dogoditi na Republiku Hrvatsku bio je napad pod kodnim imenom *#OpCroBlackout*. Napad je simbolično trebao započeti s 1. srpnja 2013. kada je RH ušla u EU. Glavne mete toga napada bile su internetske stranice medijskih, financijskih i državnih institucija u RH. Na svu sreću, SOA je u sklopu operativne akcije Europa na vrijeme detektirala napadače

te im je oduzela računalnu opremu. Također, utvrđeno je da su napadači mogli napraviti znatnu štetu da su uspjeli izvesti napad (Sigurnosno-obavještajna agencija, 2014). Nakon toga pokušaja kibernetičkog napada na RH dogodili su se i drugi napadi na državne institucije i gospodarske subjekte. Sljedeći primjer kibernetičkog napada iste godine napad je na Agenciju za komercijalnu djelatnost, odnosno AKD. Ta agencija je bila izložena kibernetičkom napadu 2013. kada je skupina hakera iz Republike Srpske uz pomagača iz Slavonskog Broda oštetila AKD za 1,8 milijuna kuna. Da je AKD izložen napadu utvrdili su njezini djelatnici 5. rujna 2013. kada su opazili smetanje na stranicama za internetsko bankarstvo, gdje je utvrđeno da im s računa u banci nedostaje 1,8 milijuna kuna (Dešković, 2013). Uz taj kibernetički napad, zabilježen je još jedan koji se nije dogodio u Hrvatskoj, nego u Italiji, ali posljedice napada bile su vidljive i u Hrvatskoj. Riječ je o napadu na talijansku kompaniju Hacking Team, koja proizvodi softvere za prisluškivanje komunikacije. U tom hakerskom napadu ukradeno je 400 GB elektroničke pošte koja je kasnije izašla u javnost te se u njoj spominju neke hrvatske tvrtke i SOA (Izvješće o aktivnostima nacionalnog CERT-a, 2015).

Nakon toga kibernetički napadi na državne institucije i agencije ne prestaju. Tako je u 2016. izvršen kibernetički napad haktivističke grupe Anonymousi na Ministarstvo vanjskih i europskih poslova. Motivacija tog napada je odbacivanje antipiratskog sporazuma ACTA (Index, 2016). Nadalje, u 2018. jedan državni službenik je na službeni e-mail dobio poruku o održavanju konferencije koja je povezana s njegovim djelokrugom rada. U tom e-mailu je osim poruke stajao i obrazac prijave na konferenciju. Frapantan je podatak da su napadači iskoristili stvarnu konferenciju kako bi kreirali lažni e-mail i poslali ga državnom službeniku. Nakon što je provedena forenzična analiza e-maila utvrđeno je da je privitak iz e-maila bio zaražen malicioznim kodom te da je obrazac bio otvoren, u sustav bi bio pušten taj maliciozni kod koji je mogao imati ozbiljne reperkusije na rad same institucije, ali je mogao i omogućiti napadaču da prikuplja povjerljive informacije. Kasnijom analizom također je utvrđeno da se radi o APT napadima, odnosno *Advanced Persistent Threat* (Sigurnosno-obavještajna agencija, 2018).

Osim ministarstva i državnih agencija kibernetičkom kriminalu izloženi su i pojedini gradovi, a primjer toga dolazi iz grada Đakova. Cijeli slučaj se odvijao 9. srpnja 2018. kada je pročelnik za financije grada Đakova od gradonačelnika dobio lažni e-mail s nalogom da izvrši uplatu od 50 000 eura na račun osobe. U ovom slučaju ne radi se o hakerskom napadu na grad Đakovo, nego se radi o računalnom kriminalu. Također, u tom je slučaju zakazao i sustav provjere isplate velikih svota novaca, jer je pročelnik prije takve isplate trebao kontaktirati gradonačelnika kako bi obavio provjeru istoimene uplate (Poslovni.hr, 2018). U 2019. kibernetički napadi na državne institucije ne prestaju, zabilježeno je pet državno sponzoriranih APT napada. Mete

napada su Ministarstvo vanjskih i europskih poslova te Ministarstvo obrane (Sigurnosno-obavještajna agencija, 2019).

Osim državnih institucija, i gospodarski subjekti također su izloženi kibernetičkim napadima i raznim oblicima kibernetičkog kriminala. Tako je nacionalna naftna kompanija Ina bila izložena kibernetičkom napadu. Cijeli kibernetički napad započinje 14. veljače 2020. oko 22 sata kada su radnici INE imali problema s izdavanjem bonova za mobitel i elektroničkih vinjeta te naplatom komunalnih računa. Napadači su napad izveli s CLOP *ransomwareom* gdje su tražili otkupninu u iznosu od 100 milijuna kuna, u protuvrijednosti 1500 Bitcoina (Ivezić, 2020). Uz Inu, i druge hrvatske kompanije su bile na meti hakera. Jedna od tih kompanija koju su hakeri napali bila je i kutinska Petrokemija. Ta kompanija je kibernetički napad doživjela 2021., a hakeri pokušali neautorizirano doći do službene elektroničke komunikacije Petrokemije (Prerad, 2021). Treći slučaj kibernetičkog napada na kompaniju bio je hakerski napad na telekomunikacijskog operatera A1. Kompanija A1 se našla na udaru hakera u veljači 2022. kada su hakeri napali središnji korisnički sustav. Cilj napada je kompromitacija korisničkih podataka (ime i prezime, OIB, broj mobitela, adresa stanovanja, broj kreditne kartice i sl.) od korisnika usluga A1, ali ne samo od njih nego i korisnika usluga Tomata i B-neta. Sam napad izvršen je izvan radnog vremena te su tim postupkom hakeri pokrenuli alarme u sigurnosnoj službi A1 te su oni pravovremeno onemogućili daljnji pristup korisničkom sustavu. Nažalost, napadači su uspjeli ukrasti nešto manje od 200 tisuća korisničkih podataka (Ivezić, 2022). Upravo ti napadi su podsjetnik da kibernetička sigurnost nije nešto što se može zapostavljati, jer kada dođe do kibernetičkog napada on za sobom ostavlja ozbiljne financijske gubitke.

5. Zaključak

U radu je prikazano da kibernetička sigurnost postaje sve značajnije pitanje nacionalne sigurnosti. Argumentacija za takvo stajalište leži u činjenici da se sve više društvenih, poslovnih i ostalih interakcija odvija u kibernetičkom prostoru. Zbog toga, tu je i latentna opasnost jer uz sve veću ovisnost suvremenog društva o kibernetičkoj tehnologiji pojavljuju se i značajnije sigurnosne ugroze. Drugim riječima, više nije pitanje ako se kibernetički napad dogodi, nego kada će se dogoditi i kako ćemo se od njega obraniti. Sigurnosne ugroze koje značajnije mogu narušiti kibernetičku sigurnost, a samim time i nacionalnu sigurnost jedne države su kibernetički kriminal, kibernetička špijunaža, kibernetičko ratovanje i kibernetički terorizam. U radu smo postavili pitanje postaje li kibernetička sigurnost ključna determinanta nacionalne sigurnosti. Odgovor je jednostavan i glasi da, postaje. To znači da kibernetičku sigurnost moramo promatrati kao holistički model, odnosno znati na koji način upravljati te osigurati nesmetano funkcioniranje svih sudionika, bilo da se radi o državnim institucija-

ma ili privatnim kompanijama. Također, treba dodati da na kibernetičku sigurnost ne možemo više gledati kao na tehnološki aspekt, nego kao neizostavni dio nacionalne sigurnosti. Republika Hrvatska, kao i ostale države u svijetu, sve više bilježe državno sponzorirane napade na svoje informacijsko-komunikacijske sustave. Glavni cilj takvih napada je prikupljanje podataka o hrvatskim političkim, gospodarskim i sigurnosnim procesima, ali i obavještajnih i drugih podataka o euroatlantskih integracijama.

U tom okruženju Republika Hrvatska kao članica Europske unije i NATO saveza morala je poduzeti odgovarajuće korake kako bi podigla kibernetičku sigurnost na višu razinu. Naime, uzmimo samo primjer da netko napadne opskrbu električnom energijom. Takav napad bi za sobom imao devastirajući učinak, ne samo financijski, nego bi neposredno bili ugroženi i ljudski životi. Upravo zbog toga kibernetička sigurnost mora biti integralni dio nacionalne sigurnosti, a ne samo usputna stavka koju se nastoji zadovoljiti. Za kraj, misao Eugena Spafforda, direktora tvrtke *Computer Operations, Audit and Security Technology* (COAST), „jedini informacijski sustav koji je zaista siguran je onaj koji je ugašen, isključen iz napajanja, zaključan u sefu od titana, zakopan u betonskom bunkeru, okružen nervnim plinom i dobro plaćenim naoružanim čuvarima. Čak ni tada, ne bih se baš kladio na njega."

Literatura

1. Ahić, Jasmin i Nađ, Ivan (2017). *Upravljanje rizikom u privatnoj sigurnosti*. Sarajevo: Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu.
2. Index (2016). *Anonymousi hakirali Ministarstvo vanjskih poslova: ali mi nismo nadležni za ACTA-u*. https://www.index.hr/vijesti/clanak/Anonymousi-hakirali-Ministarstvo-vanjskih-poslova-Ali-mi-nismo-nadlezni-za-ACTA-u/599445.aspx. 14. siječnja 2023.
3. Božinović, Davor (2016). *Globalna sigurnost*. Zagreb: Narodne novine.
4. Bača, Miroslav (2004). *Uvod u računalnu sigurnost*. Zagreb: Narodne novine.
5. Brzica, Nikola (2020). Informacijska nadmoć: na sjecištu informacijskog i kibernetičkog ratovanja. *Polemos*, XXIII (47): 13–31.
6. Buchan, Russell (2019). *Cyber Espionage and International Law*. HART.
7. Collins, Alan (2010). *Suvremene sigurnosne studije*. Zagreb: Politička kultura: Centar za međunarodne i sigurnosne studije Fakulteta političkih znanosti.
8. CERT (2022). *O adware/spyware softveru*. https://www.cert.hr/adware/. 14. siječnja 2023.
9. Dešković, Marin (2013). Opljačkan AKD – Hakeri provalili u najčuvaniju hrvatsku agenciju i ukrali 1,8 milijuna. *Jutarnji list*. https://www.jutarnji.hr/vijesti/crna-kronika/opljackan-akd-hakeri-provalili-u-najcuvaniju-hrvatsku-agenciju-i-ukrali-18-milijuna-1070873. 14. siječnja 2023.
10. Djurkin-König, Lana; Ostojić, Alen; Delić, Alen i Mihaljević, Branko (2020). *Korporativna sigurnost u okruženju pandemije COVID-19.* Zagreb: Poslovno učilište integralna sigurnost i razvoj.
11. Ivandić Vidović, Darija; Karlović, Lidija i Ostojić, Alen (2011). *Korporativna sigurnost*. Zagreb: Udruga hrvatskih menadžera sigurnosti.

12. Izvješće o aktivnostima nacionalnog CERT-a (2015). https://www.cert.hr/wp-content/uploads/2018/01/2015-HR-CERT-izvjestaj_0.pdf. 14. siječnja 2023.
13. Ivezić, Bernard (2020). Love ih policija i stručnjaci iz SAD-a: kibernetički kriminalci ucijenili Inu za 100 milijuna kuna? *Poslovni.hr.* https://www.poslovni.hr/kolumne/velike-kompanije-u-strahu-zbog-ucjena-kibernetickih-kriminalaca-4215239. 14. siječnja 2023.
14. Ivezić, Bernard (2022). Doznajemo detalje cyber napada na A1: Hakeri su rovarili bazom, no ostavili su 'glupe tragove'. *Jutarnji.hr.* https://novac.jutarnji.hr/novac/aktualno/doznajemo-detalje-cyber-napada-na-a1-hakeri-su-rovarili-bazom-no-ostavili-su-glupe-tragove-15156146. 14. siječnja 2023.
15. Hrvatska enciklopedija, mrežno izdanje (2021). *Kibernetički prostor*. http://www.enciklopedija.hr/Natuknica.aspx?ID=68098. 22. siječnja 2023.
16. Kovačević, Božo (2013). Cyberwar – američka izlika za novi hladni rat? *Polemos,* XVI (32): 91–110.
17. Središnji državni ured razvoj digitalnog društva (2022). *Kibernetička sigurnost*. https://rdd.gov.hr/kiberneticka-sigurnost-1436/1436. 14. siječnja 2023.
18. Mihaljević, Branko i Nađ, Ivan (2018). *Osnove korporativne sigurnosti*. Zagreb: Hrvatska udruga menadžera sigurnosti.
19. Pegasus CERT.hr. file:///C:/Users/Korisnik/Downloads/Pegasus%20(4).pdf. 14. siječnja 2023.
20. Prerad, Danijel (2021). Hakeri napali kutinsku Petrokemiju, otežana elektronička komunikacija. *Večernji.hr.* https://www.vecernji.hr/vijesti/hakeri-napali-kutinsku-petrokemiju-otezana-elektronicka-komunikacija-1524004. 14. siječnja 2023.
21. Poslovni.hr (2018). *Iz grada Đakova prevarantu uplatili 50.000 eura, nije im palo na pamet da provjere vrlo sumnjivo ime*. https://www.poslovni.hr/hrvatska/iz-grada-akova-prevarantu-uplatili-50000-eura-nije-im-palo-na-pamet-da-provjere-vrlo-sumnjivo-ime-344950. 14. siječnja 2023.
22. Spremić, Mario (2017). *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*. Zagreb: Sveučilište u Zagrebu, Ekonomski fakultet.
23. Sheldon, J. B. (2022). *Cyberwar.* Encyclopedia Britannica. https://www.britannica.com/topic/cyberwar. 14. siječnja 2023.
24. Sigurnosno-obavještajna agencija (2014). *Javno izvješće 2014.* https://www.soa.hr/files/file/JAVNI-DOKUMENT_web.pdf. 14. siječnja 2023.
25. Sigurnosno-obavještajna agencija (2016). *Javno izvješće 2017.* https://www.soa.hr/files/file/Javno-izvjesce-2017.pdf. 14. siječnja 2023.
26. Sigurnosno-obavještajna agencija (2018). *Javno izvješće 2018*. https://www.soa.hr/files/file/Javno-izvjesce-2018.pdf. 14. siječnja 2023.
27. Sigurnosno-obavještajna agencija (2019). *Javno izvješće 2019.* https://www.soa.hr/files/file/Javno-izvjesce-2019.pdf. 14. siječnja 2023.
28. Sigurnosno-obavještajna agencija (2020). *Javno izvješće 2020.* https://www.soa.hr/files/file/Javno-izvjesce-2020.pdf. 14. siječnja 2023.
29. Tatalović, Siniša i Bilandžić, Mirko (2005). *Osnove nacionalne sigurnosti*. Zagreb: Policijska akademija.
30. Tatalović, Siniša; Grizold, Anton i Cvrtila, Vlatko (2008). *Suvremene sigurnosne politike*. Zagreb: Golden-marketing – Tehnička knjiga.
31. Vuković, Hrvoje (2012). Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj. *National security and the future*, 13 (3): 12–31.

Cybersecurity as key determinant of national security of the Republic of Croatia

Abstract

This paper elaborates on what cybersecurity is and why it is becoming a key determinant of national security of the Republic of Croatia. The paper is divided into several units; after the introduction, the second part explains the key concepts, namely national security, cyberspace, and cybersecurity. The third part of the paper deals with the classification of threats, i.e. the types of threats to cybersecurity; cyberwarfare, cyberterrorism, cyberespionage, and cybercrime. The last part of the paper deals with cyber-attacks on state institutions and economic entities in the Republic of Croatia, with an example of attacks that occurred.

Keywords: cybersecurity, national security, Republic of Croatia, cyberspace