Kibernetička sigurnost kao komponenta koncepta korporativne sigurnosti

Jarža, Ivona

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, The Faculty of Political Science / Sveučilište u Zagrebu, Fakultet političkih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:114:235868

Sveučilište u Zagrebu
Fakultet političkih znanosti
Diplomski studij politologije
Smjer nacionalna sigurnost

Ivona Jarža

KIBERNETIČKA SIGURNOST KAO KOMPONENTA KONCEPTA KORPORATIVNE SIGURNOSTI

DIPLOMSKI RAD

Zagreb, 2022

Sveučilište u Zagrebu
Fakultet političkih znanosti
Diplomski studij politologije
Smjer nacionalna sigurnost

KIBERNETIČKA SIGURNOST KAO KOMPONENTA KONCEPTA KORPORATIVNE SIGURNOSTI

DIPLOMSKI RAD

Mentor: doc. dr. sc. Robert Barić
Studentica: Ivona Jarža

Zagreb

Rujan, 2022

Izjavljujem da sam diplomski rad Kibernetička sigurnost kao komponenta koncepta korporativne sigurnosti, koji sam predala na ocjenu mentoru (doc. dr. sc. Robert Barić), napisala samostalno i da je u potpunosti riječ o mojem autorskom radu. Također, izjavljujem da dotični rad nije objavljen ni korišten u svrhe ispunjenja nastavnih obaveza na ovom ili nekom drugom učilištu, te da na temelju njega nisam stekao/la ECTS - bodove. Nadalje, izjavljujem da sam u radu poštivala etička pravila znanstvenog i akademskog rada, a posebno članke 16-19. Etičkoga kodeksa Sveučilišta u Zagrebu.

Ivona Jarža

Sadržaj

1. UVOD

Kibernetička sigurnost danas je postala jedno od najvažnijih kategorija sigurnosti. Rastući broj korisnika računala i interneta poboljšao je modernizaciju i napredak društva, posebice u informacijskom smislu. No korištenje računalnih tehnologija nije bezazleno, jer smo sa svakim odlaskom na internet potencijalno izloženi kibernetičkim rizicima. Problem kibernetičke sigurnosti proteže se mnogo dalje od toga, naime, privatni korisnici nisu jedini izloženi kibernetičkim napadima, već su izložene i same države i korporativni sektor.

Teza ovog rada glasi: Tržište zaštite od kibernetičkih napada konstantno implementira nove načine zaštite svojih subjekata, a najefikasniji način obrane je međusobna suradnja privatnog i javnog sektora. Države su, kako bi poboljšale nacionalnu sigurnost, uz tradicionalan vojni pogled, počele uvoditi i moderniji pogled na sigurnost, a posebice se naglašava kibernetička sigurnost kao jedna od najvažnijih aspekata modernijeg pogleda na sigurnost. No trenutna svjetska situacija (npr. kriza u Ukrajini) itekako je i dalje naglasila potrebitost razvoja vojne komponente nacionalne sigurnosti. Globaliziran svijet iziskuje drugačiji pogled na sigurnost – kombinaciju tradicionalnog (vojnog) pogleda na sigurnost i modernog (sveobuhvatnog) pogleda na sigurnost gdje se treba fokusirati na međunarodnu suradnju i na suradnju privatno – javnog sektora po pitanju nalaženja odgovora na sigurnosne prijetnje i izazove.

Istraživačko pitanje na koje ovaj rad pokušava odgovoriti glasi: Kako je suradnja javnog i privatnog sektora u SAD i EU doprinijela poboljšanju obrane od kibernetičkih prijetnji? Ova problematika razmatra se kroz analizu aktivnosti kibernetičke sigurnosti u djelovanju korporativnog sektora protiv kibernetičkih napada. Korporativni sektor, danas, skoro u potpunosti ovisi o aktivnostima u informacijskom prostoru pa je on tako najizloženiji kibernetičkim napadima. Korporativna sigurnost, stoga, se danas sastoji od informacijske sigurnosti za koju je striktno zadužen IT sektor, ali i od kibernetičke sigurnosti za koju je zadužen apsolutno cijeli korporativni (privatni) sektor. Neznanje i neopreznost pojedinca može ponajviše ugroziti kibernetičku sigurnost cijele kompanije.

Moderni pogled države na nacionalnu sigurnost i usmjerenost korporativnog sektora na kibernetičku sigurnost doveli su do javno - privatnog partnerstva (PPP). Javno – privatno partnerstvo po pitanju kibernetičke sigurnosti najzastupljenije je u SAD-u, dok su EU i ostale države i dalje pomalo skeptične o toj suradnji – prvenstveno zbog prevelikih (za njih možda i nespojivih) razlika između ova dva politička entiteta. U Europskoj Uniji više se fokusira na jednu zajedničku suradnju svih država članica preko krovne institucije ENISA (*European*

Union Agency for Network and Information Security) koja je izričito zadužena za kibernetičku sigurnost. U Republici Hrvatskoj postoji nekoliko organizacija koje su zadužene za kibernetičku sigurnost i sve su u suradnji sa institucijama Europske Unije. Suradnja SAD-a i Europske Unije po pitanju kibernetičke sigurnosti ostvaruje se preko suradnje raznih organizacija vezanih uz kibernetičku sigurnost, a najpoznatiji primjer te suradnje vidljiv je u borbi protiv kibernetičkog kriminala suradnjom FBI-a i EUROPOL-a. NATO također ima ulogu u suradnji ova dva entiteta, no glavni naglasak NATO još uvijek stavlja na vojnu sigurnost. Kibernetička sigurnost u NATO Savezu poprima sporednu ulogu, no nedavni sigurnosni incidenti dokazali su da su vojna i kibernetička sigurnost danas neodvojive.

U konačnici, **cilj** ovog diplomskog rada je prikazati moguće načine zaštite od kibernetičkih prijetnji kroz analizu aktivnosti kibernetičke sigurnosti u djelovanju korporativnog sektora protiv kibernetičkih napada, gdje je jedan od važnijih mehanizama (u demokratskim državama) suradnja javnog i privatnog sektora. S napretkom tehnologije, potrebna je i inovativnost u zaštiti od mogućih tehnoloških napada i krađe podataka.

2. NASTANAK KONCEPTA KIBERNETIČKE I KORPORATIVNE SIGURNOSTI

Ovo poglavlje bavi se povijesnim razvojem koncepta kibernetičke sigurnosti, tj. pozadinom nastanka same kibernetičke sigurnosti. O kibernetičkoj sigurnosti zapravo možemo pričati od trenutka nastanka prvog računala tj. od trenutka međusobnog povezivanja računala preko mreže. Prve vlade koje su financirale istraživanje kibernetičkog sektora su one u Sjedinjenim Američkim Državama i Velikoj Britaniji. Ta istraživanja bila su ključna za vrijeme Drugog svjetskog rata s ciljem predviđanja sljedećeg koraka protivnika. Cilj je bila obrana od zračnih napada i računalno razbijanje tajnih kodova protivnika. ENIGMA je najpoznatiji primjer uređaja sa šifriranim tajnim kodovima koji je stvarao velike probleme Saveznicima u ratu. Upotrebom prvih računala, Alen Turning uspio je razbiti tajne ENIGME i omogućio razumijevanje njemačkih tajnih kodova (Puyvelde, 2019: 6).

Fokus na istraživanje kibernetičkog prostora i vladino financiranje omogućilo je da se razvije suradnja između vlade, znanstvene zajednice i privatnog sektora za jednim zajedničkim ciljem – razvitkom sigurnog i pouzdanog kibernetičkog prostora (Puyvelde, 2019: 6). Kibernetički prostor bio je novi prostor u kojem su se stvarale *online* zajednice, a ljudi su napokon slobodno mogli izraziti svoje mišljenje – što je u konačnici dovelo do današnjih društvenih mreža. Zaključno, kibernetički prostor može se definirati kao „globalna i dinamična domena (podložna

konstantnim promjenama) okarakterizirana kombiniranim korištenjem elektrona i elektromagnetskog spektra, čija je svrha kreiranje, spremanje, modificiranje, razmjena, dijeljenje, izvlačenje, korištenje i/ili eliminacija podataka i informacija i rušenje fizičkih barijera (Mayer (2014): 1).

2.1. Povijest kibernetičke sigurnosti

Otvaranje *online* prostora donosi i prijetnje, pa se tako već 1960-ih godina počeo bilježiti značajan porast kibernetičkog kriminala. Kibernetički problem stoga nije nov, već je to problem koji se razvijao više od pola stoljeća, točnije 60-ak godina. Informacijska revolucija uistinu je promijenila svijet. Prvi uvid u mogućnost kibernetičkog kriminala spominje se već 1960. godine kada dolazi do spoznaje da računala mogu propustiti osjetljive podatke i stoga se moraju zaštiti. Sljedeća spoznaja došla je deset godina kasnije, kada se 1970-ih počelo pričati o digitalnim napadima kojima je cilj bio ukrasti informacije. O moći računala u vojnom sektoru počelo se pričati 1980-ih godina kada je došlo do spoznaje da računala mogu biti alati koji odlučuju o tijeku i sudbini rata. Spoznaja da su apsolutno svi korisnici računala i interneta ranjivi i vjerojatno već izloženi kibernetičkim napadima javlja se krajem 20. stoljeća. Ove spoznaje napravile su prekretnicu u stvaranju politika, standarda i doktrina (Warner, 2012: 3).

Komunikacija između računala javlja se već ranih 1960-ih kada su računala počela koristiti mrežu kao sredstvo komunikacije, a u to doba, točnije 1962. je u svijetu bilo registrirano čak 10 000 računala, a većina njih u SAD-u (Puyvelde, 2019: 8). U to doba su računala bile ogromne mašine kojima je upravljalo nekoliko ljudi te su zahtijevala posebne prostorije koje su korisnici mogli iznajmiti na korištenje. Korištenje računala u to doba mogli su si priuštiti samo oni najbogatiji kao pojedinci ili agencije kao zajednica. Marshalla Cartera (1968), direktor Nacionalne sigurnosne agencije (NSA) ponosno je izjavio NSA posjeduje stotine računala koja okupiraju čak 20.234 m^2 poda kojima upravljaju najinteligentniji ljudi. Već u to doba je NSA shvaćala težinu sigurnosnih problema i kibernetičke ranjivosti. Zastupnički dom Kongresa održao je 1966. trodnevno saslušanje o kibernetičkim opasnostima koje su zaprijetile privatnosti američkih građana. U Europi, prvi ikad zabilježen slučaj kibernetičke špijunaže dogodio se 1968. godine kada je policija Zapadne Njemačke ulovila istočno-njemačkog špijuna u sjedištu IBM-a. Ujedno je to bio i prvi ikad zabilježen slučaj informacijske špijunaže u svijetu (Warner, 2012: 5).

Desetljeće kasnije dolazi do mnogih programerskih inovacija u svrhu poboljšanja kibernetičke sigurnosti, a neke od njih su: administratorska dopuštenja i ograničenja, dopuštenja za otvaranje datoteka i teško probojne lozinke. U to doba javlja se i enkripcija (šifriranje) podataka i datoteka, inovacija koju je osmislila njemačka podružnica IBM-a kako bi se zaštitile bankarske transakcije, a kasnije je taj algoritam prodan i međunarodnim institucijama (Warner, 2012: 6).

Internet je postao relativno javna stavka 1980-ih godina. Početkom 1980-ih godina javlja se i problem virusa i hakiranja koji su ozbiljno naštetili integritetu nacionalne sigurnosti država. Širenje lažnih informacija postalo je jedno od glavnih sredstava dizanja opće panike. Naime, u studenome 1979. godine, netko je u Sjevernoameričkom zračno-obrambenom centru (NORAD) pustio *online* informaciju da je Rusija uputila 2200 raketa prema SAD-u, što je diglo opću uzbunu i paniku. Informacija je došla čak do i Zbigniewa Brzezinskoga (savjetnika za nacionalnu sigurnost) i predsjednika Ronalda Reagana koji se mnogo puta referirao na ovaj lažni scenarij kao upozorenje za budućnost. Sličnih slučajeva je bilo još podosta, ali ono što je najviše uzdrmalo medije i javnost je realizacija da su čak i tinejdžeri (Milwaukee's 414's) [1] jednostavno uspjeli upasti u američku vojnu bazu podataka te ukrasti podatke i moguće uzrokovati ogromnu štetu za cijeli SAD (Warner, 2012: 6 – 8). Ovo je zapravo samo pokazalo značajnu ranjivost sustava nacionalne sigurnosti SAD-a i nepovjerenje građana u javne institucije.

Danas skoro svako kućanstvo na svijetu ima računalo unatoč sigurnosnim rizicima. Podaci iz 2014. godine pokazuju da 80% odraslih u SAD-u posjeduje računalo, 78% u Rusiji, 59% u Kini, 55% u Brazilu, dok samo 11% u Indiji (Puyvelde, 2019: 10).

Razvoj komunikacijskih mreža, s druge strane, počinje čak i ranije, kada se pojavio prvi telegraf i telegrafski pisač 1914. godine – ovi alati ovisili su o protoku komunikacijskog signala. Nakon Drugog svjetskog rata, javila se potreba za istraživanjem bolje povezanosti više računala, pa se tako javljaju i razne agencije za napredak komunikacijskih mreža, a najpoznatija na svijetu, dakako, bila je ARPA (*Advanced Research Project Agency*) koja je 1969. godine osnovala prvu računalnu mrežu – ARPANET. Prvo je ARPANET služio kao platforma za razne istraživače kojima je cilj bio razviti tehnologiju koja bi međusobno povezala nekoliko sveučilišta i istraživačkih centara – prva dva čvora koja su se koristila bila su između University

[1] 414's bila je grupa hakera tinejdžera koji su provalili u desetke viskoko profiliranih računala sa snažnom zaštitom. Ovim postpukom istaknuli su ranjivost informacijskog sektora I uzdrmali nacionalnu sigurnost SAD-a. Oni su prva hakerska grupa koja je dobila snažnu medijsku pokrivenost I interes javnosti.

of California, Los Angeles (UCLA) i Stanforda. Broj čvorišta se 1977. povezao na čak 55 gdje su bili međusobno povezani istraživački centri i sveučilišta (Puyvelde, 2019: 9 – 11). Kada je to bilo postignuto, mreža (internet (WWW koji je nastao 1990-ih)) se dalje lako razvijala te stekla mogućnost povezati cijeli svijet sa samo nekoliko klikova miša. Godine 2016. bilo je čak 3,6 milijarde korisnika interneta, što je nešto više od 40% sveukupnog čovječanstva. Danas se sa računalom može koristiti bilo tko, ono mu je lako dostupno, a pristup internetu je još i rasprostranjeniji. Točnije, danas se informatičkim uslugama i internetom koristi čak 5,3 milijarde ljudi, tj. 63% sveukupne svjetske populacije (*datareportal.com*).

3. TEORIJSKI OKVIR

Koncept sigurnosti postoji odavno, no tek je u prošlom stoljeću pobudio zanimanje akademske zajednice. Iako je sigurnost u državi oduvijek bila vrlo važan faktor, dominirajuća komponenta bila je vojna sigurnost. Tek su novi izazovi krajem 20. stoljeća, po završetku hladnog rata, pobudili snažnu potrebu za postizanje sveobuhvatne sigurnosti. Hladni rat bio je prekretnica nakon kojeg se počeo sve više davati naglasak s koncepta državne sigurnosti na sigurnost pojedinca odnosno koncept ljudske sigurnosti (Zedner, 2003: 153).

Teroristički napad 11. rujna smanjio je distinkciju između unutarnje i vanjske prijetnje, što je automatski značilo i drugačiji pogled na nacionalnu sigurnost općenito. Zapadne države napokon su shvatile da je dosadašnji sustav nacionalne sigurnosti narušen te da je potrebno implementirati mnoge nove strategije kako bi se zaštitila sama egzistencija, kako građana, tako i države. U tom novom okviru implementiranih promjena napokon se našla i kibernetička sigurnost kao vrlo važan dio nacionalne sigurnosti bez koje država, pa to tome i privatni sektor, ne može nikako funkcionirati.

Kibernetička sigurnost postala je važan i nezaobilazan faktor za korporativno upravljanje.[2] Kibernetičkoj sigurnosti je cilj osigurati siguran kibernetički prostor, zaštititi svoje korisnike i njihovu privatnost provedbom strogih sigurnosnih regulacija i protokola koji će spriječiti potencijalni kibernetički napad. Korporativna sigurnost, osim osnovne sigurnosti, danas mora imati i vrlo kvalitetno razvijenu obranu od kibernetičkih napada. Korištenjem interneta,

[2] Korporativno upravljanje predstavlja skup procesa, običaja, pravila, zakona, odluka, institucija i nadzornih mehanizama kojima se utječe na upravljanje, kontroliranje i administriranje privrednog subjekta tj. tvrtke (Dropulić, Ružić (2011): 5.

korporativni sektor je većinu svojeg poslovanja prebacio *online,* što je dovelo do iznimnog napredovanja kvalitete poslovanja, ali je dovelo i taj sektor u značajan rizik od kibernetičkih napada. Kibernetički napad ima potencijal u potpunosti uništiti reputaciju i financijsko blagostanje neke kompanije. Danas je potreba za kibernetičkom sigurnosti u korporativnom sektoru jedan od najviših aspekata dobrog poslovanja. Korporativni sektor, stoga, najčešće ima i posebni odjel kibernetičke sigurnosti koja je prvenstveno zadužen za obranu od kibernetičkih napada.

3.1. Informacijska (kibernetička) sigurnost kao dio korporativnog upravljanja

Informacijska (kibernetička) sigurnost nekad se smatrala izričito tehnološkim problemom sa tehnološkim rješenjima, za koju je bio striktno zadužen informatički (IT) odjel, koji je bio odvojen od glavnog poslovanja. No danas je informacijska sigurnost puno više od pukog IT problema. Ona danas zahtjeva uključivanje svih sektora i višeg rukovodstva u uspostavu politika, procedura, organizacijskih struktura i svih povezanih za osiguranje informacijske sigurnosti (Arbanas, 2021: 42). Kibernetička sigurnost danas je definitivno dio koncepta korporativne sigurnosti jer postaje važno upravljačko pitanje. Arbanas navodi kako su danas mnogi autori složni oko toga da je kibernetička sigurnost prvenstveno problem upravljanja i poslovanja. Informacijska (kibernetička) sigurnost se stoga treba tretirati kao poslovna (korporativna) sigurnost, a ne kao tehnički problem (Arbanas, 2021: 42).

Bitno je razumjeti da je informacijska sigurnost danas odgovornost korporativnog upravljanja, ona je poslovno, a ne tehničko pitanje i činjenica je da je informacijska sigurnost višedimenzionalna cjelina (Arbanas, 2021: 42). Informacijska sigurnost treba biti integrirana u korporativno upravljanje organizacije kako bi se potaknula odgovornost cijelog privatnog sektora koji će se pridržavati sigurnosnih pravila i propisa koji sprječavaju lake kibernetičke napade. No danas je itekako jasno da se u velikoj većini, opasni i sofisticirani, kibernetički napadi ne mogu spriječiti, već je potrebno pravovremeno i adekvatno ispraviti štetu i umanjiti posljedice napada (Arbanas, 2021: 43).

Informacijsko upravljanje korporativnom sigurnošću obuhvaća provedbu i nadzor sigurnosnog programa, dok je korporativno upravljanje zaduženo za zadavanje smjernica i odlučivanje o važnim aspektima privatne sigurnosti. Postoji nekoliko principa dobrog informacijskog upravljanja kibernetičkom sigurnošću, a to su: „odgovornost izvršnog rukovodstva da osigura

strateški smjer, osigura postizanje ciljeva, nadgleda da se rizicima upravlja na odgovarajući način i da se potvrđuje odgovorno korištenje resursa“ (Arbanas, 2021: 43). Prema Volchkovu, napominje Arbanas, učinkovito korporativno upravljanje ima sljedeće karakteristike: uključena je cijela tvrtka, definirane su odgovornosti, razina zaštite ovisi o apetitu za rizik i sigurnošću se aktivno upravlja (2021: 43).

Korporativni sektor je danas žrtva većine kibernetičkih napada, a takve napade nazivamo kibernetičkim incidentima. Najčešća posljedica ovakvih napada je povreda podataka koju ISO definira kao: „ugrozu sigurnosti koja vodi do nezakonite destrukcije, gubitka, izmjene, neautoriziranog dijeljenja i nezakonitog pristupa zaštićenim i privatnim podacima. Svaki ovakav kibernetički napad može izazvati korporativnu kibernetičku krizu (Knight, 2020: 3). Brzo mijenjajuće prijetnje predstavljaju nove izazove za korporativni sektor, zlonamjerni softveri sofisticiraniji su no ikada, nove vrste kibernetičkih napada događaju se i zbog lošeg ponašanja zaposlenika koji to radi iz neznanja ili nemara. Veće ugroze sigurnosti mogu se dogoditi i zbog lošeg višeg rukovodstva, loše tehničke opreme i/ili nepostojanja standarda i smjernica ili čak i zbog loše financijske situacije kompanije. Nedovoljno pružanje financijskih sredstava informacijskoj sigurnosti posebno je izraženo kod malih i srednjih poduzeća (Arbanas, 2021: 46).

Korporativni sektor se danas vodi sa idejom upravljanja rizicima jer se mora prihvatiti činjenica da će se zbog kibernetičkih napada dogoditi manji ili veći informacijski proboji, krađe podataka i financijski gubici. Kako bi se upravljalo rizicima, prijetnje se moraju prepoznati, klasificirati i procijeniti da bi se mogao izračunati njihov potencijal štete (Arbanas, 2021: 49). Kako bi se upravljalo rizicima, još je potrebno i definirati sam rizik koji Međunarodna organizacija za standardizaciju (ISO) definira kao „mogućnost štetnih posljedica za organizaciju ukoliko prijetnje iskoriste ranjivosti informacijske imovine”, prijetnju kao „potencijalni uzrok neželjenog događaja koji može rezultirati štetom za sustav ili organizaciju”, a ranjivost kao „slabost imovine ili kontrole koju može iskoristiti jedna ili više prijetnji” (Arbanas, 2021: 49). Kako bi se nešto smatralo prijetnjom, ne mora se nužno dogoditi incident ili sigurnosni proboj ili kibernetički napad, već ta prijetnja može biti unaprijed prepoznata.

Kako bi se rizik mogao procijeniti, potrebno je slijediti metodologiju rizika. Metodologija rizika postoji mnogo, no one sve se slažu u tome da je potrebno slijediti određene korake kako bi se mogao uspješno procijeniti rizik. Prvo se počinje sa identifikacijom prijetnji i ranjivosti, pa je onda potrebno procijeniti razinu rizika i taj rizik onda tretirati sa četiri moguće opcije:

prihvaćanje, smanjivanje, prijenos ili izbjegavanje rizika (Arbanas, 2021: 50). Ozbiljnost kibernetičkih napada treba prihvatiti jer je čak 57% organizacija, od 2019. godine do 2021. godine, doživjelo kibernetički napad (Arbanas, 2021: 51). Ne postoji još točna statistika za kibernetičke napade u 2022. godini, no itekako se može vidjeti da je korporativni sektor na udaru kibernetičkih napada više no ikad.

ENISA je objavila statistiku glavnih prijetnji za 2019. godinu, gdje u zadnje tri godine, prvo mjesto uvjerljivo drži zlonamjerni softver. Kako bi se vidio razmjer kibernetičkih prijetnji, Arbanas parafrazira i IBM-ovo istraživanje o kibernetičkim rizicima gdje navodi „kako je je od 2014. godine udio sigurnosnih proboja uzrokovanih zlonamjernim napadima porastao za 21%, rastući s 42% proboja u 2014. godini na 51% proboja u 2019. godini. Iako su zlonamjerni proboji najčešći, nenamjerni proboji zbog ljudskih pogrešaka i propusta na sustavu i dalje su osnovni uzrok gotovo polovice (49%) proboja podataka analiziranih u izvješću. Zlonamjerni ili kriminalni napad uključivalo je 51% incidenata, 25% uključivalo je probleme u sustavu, uključujući IT i poslovne procese, a 24% je bilo zbog ljudske greške uslijed nepažnje“ (Arbanas, 2021: 54).

3.2. Problem definiranja kibernetičke sigurnosti

Iako se i dalje mogu koristiti izrazi kao što su informacijska sigurnost, digitalna sigurnost, računalna sigurnost, IT sigurnost, izraz kibernetička sigurnost uživa sve veću popularnost javnosti. Ovaj izraz popularnost je stekao nakon 2009. godine kada je predsjednik SAD-a Barack Obama izjavio da poziva građane SAD-a da osvijeste važnost kibernetičke sigurnosti. Izraz kibernetička sigurnost onda postaje jedan od najviše korištenih izraza za takvu vrstu sigurnosti. To dokazuje ova tablica gdje se jasno može vidjeti kako popularnost ostalih izraza opada, dok izraz kibernetička sigurnost dobiva na popularnosti (2004 – 2015):

TRENDOVI GOOGLE ISTRAŽIVANJA RIJEČI SIGURNOST

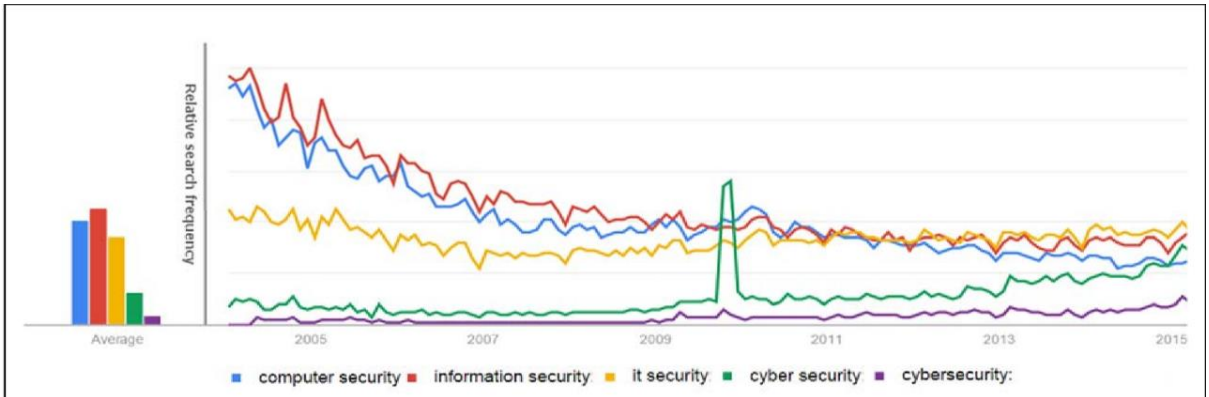

Figure 1. Google search trends for security 2004 – 2015

(preuzeto 3. 6. 2022) Schatz, Wall i Bashroush (2017): 3

Iako su ovi izrazi vrlo slični, oni nisu sinonimi i mogu izazvati konfuziju kod korisnika. Ključna stvar u razlikovanju kibernetičke sigurnosti od ostalih pojmova (npr. računalna sigurnost, informacijska sigurnost, IT sigurnost) zapravo je korištenje interneta (WWW – World Wide Web). Uz kibernetičku se sigurnost uvijek veže taj važan pojam online, dok se kod drugih sličnih riječi ne mora specifično koristit internet kako bi se nanijeli problemi. Iako zapravo ovo razlikovanje pojmova ne predstavlja problem privatnome sektoru, kriva terminologija itekako može napraviti problem u javnom sektoru i u stvaranju javnih politika, uredbi i zakona vezanih uz kibernetičku sigurnost (Schatz, 2017: 3 – 4).

Nedostatak uniformne definicije kibernetičke sigurnosti prepoznat je na nekoliko razina: na profesionalnoj razini (Barzilay, 2013; Stubley, 2013; Walls, Perkins i Weiss, 2013)), na (javnoj) razini vladinih organizacija (Falessi, Gavrila, Klejnstrup Ritter i Moulinos, 2012; Vlada Crne Gore (2013); Wamala (2011) te na akademskoj razini (Baylon, 2014; Giles i Hagestad, 2013). Na profesionalnoj, tj. industrijskoj razini (kako to nazivaju Schatz, Basroush i Wall, 2017), kibernetičku sigurnost gleda se kao profesionalno pružanje usluga gdje je glavni fokus na realnom vodstvu donošenja ispravnih strateških odluka (Walls, 2013). Za njih je terminologija kibernetičke sigurnosti prihvatljiva kada se koristi u kontekstu sigurnosnih praksi napada i obrane koji se direktno postižu korištenjem informacijske tehnologije. Za Stubleyja (2013), kibernetička sigurnost je pojednostavljena informacijska sigurnost gdje se analiziraju ključne kibernetičke komponente. Potpuno drugačiji pristup uzima Barzilay (2013) koji tvrdi da se kibernetička sigurnost može definirati kroz kibernetički rizik – što dovodi do zaključka da je kibernetička sigurnost pod - disciplina informacijske sigurnosti. Isaca (2014) tvrdi da kibernetička sigurnost popunjava prazninu između informacijske i tradicionalne sigurnosti.

Zaključno, kibernetička sigurnost se razlikuje od informacijske sigurnosti u opsegu, motivu, prilici i metodi napada.

Definicije na državnoj, tj. nacionalnoj razini najbolje može opisati Falessi (2012) koji kroz istraživanje država članica Europske Unije izrađuje terminološko vodstvo gdje opisuje kako, opet, ne postoji univerzalna definicija kibernetičke sigurnosti – za neke je kibernetička sigurnost sinonim za informacijsku sigurnost, dok je za neke to nešto potpuno drugo. To da je kibernetička sigurnost grana informacijske sigurnosti tvrdi i Wamala (2011), no on ipak daje jednu glavnu razliku između te dvije vrste sigurnosti – a to je korištenje interneta. Baylon (2014) se okreće multinacionalnoj suradnji gdje tvrdi da nepostojanje uniformne definicije predstavlja ogromnu prijetnju internacionalnoj sigurnosti, tj. međunarodnim ugovorima i kontroli oružja. Uz to, postoji ogromna razlika u razumijevanju kibernetičke sigurnosti između demokratskih i autoritarnih država. U ruskoj legislativi, tvrdi Baylon, uopće ne postoji termin kibernetička sigurnost, već striktno prevladava koncept informacijske sigurnosti. Giles i Hagestad (2013) zaključuju kako se pogledi između Zapada, Kine i Rusije nikako ne mogu uskladiti, tako da je međunarodna zajednica uskraćena korištenja zajedničke definicije.

Što se tiče same akademske razine, Lujiif, Besseling i de Graaf (2013) provode ekstenzivno istraživanje strategija kibernetičke nacionalne sigurnosti (NCSS) između čak devetnaest različitih država gdje se također može vidjeti razlika u terminologijama kibernetičke sigurnosti. Luiijf, de Graaf i Besseling (2013: 3) nacionalnu strategiju definiraju kao „nacionalni plan akcije koji se bazira na temelju nacionalne vizije da se postigne set ciljeva koji mogu doprinijeti sigurnosti domene kibernetičkog prostora“.

Ne postoji međunarodno prihvaćena definicija kibernetičke sigurnosti, niti sve države koriste naziv kibernetička sigurnost. Od osamnaest država koje se spominju u članku Luiijfa, de Graffa i Besselinga (2013: 2), samo njih osam u svojoj strategiji prihvaćaju termin kibernetička sigurnost i definiraju ga; dvije nacije koriste termin informacijska sigurnost. Dvije nacije definiciju kibernetičke sigurnosti samo deskriptivno opisuju, dok njih šest raspravlja o kibernetičkoj sigurnosti na strateškoj razini bez korištenja neke definicije. S obzirom da ne postoji uniformna definicija kibernetičke sigurnosti, tako i svaka država ima drugačiji pristup obrani od kibernetičkih prijetnji. Različito shvaćanje kibernetičke sigurnosti, također, donosi i probleme na međunarodnoj sceni. Početkom 2011. godine, rusko – američka radna skupina sa East-West instituta (EWI) i Moskovskog sveučilišta izbacila je nacrt međunarodne kibernetičke terminologije. Oni su kibernetičku sigurnost definirali kao „svojstvo

kibernetičkog prostora koje ima sposobnost oduprijeti se namjernim i nenamjernim prijetnjama, odgovoriti na njih i oporaviti se od njih“ (Rauscher i Yaschenko (2011): 31). Ova definicija sliči većini definicija relevantnih država i može se smatrati nekom uniformnom definicijom.

Nadalje, slično kao i o kibernetičkoj sigurnosti, petnaest od osamnaest nacionalnih država raspravlja o kibernetičkom zločinu bez korištenja relevantne definicije najprije. Rumunjska je jedina od tih osamnaest država koja definira sve pojmove vezane uz kibernetičku sigurnost u svojoj strategiji nacionalne sigurnosti (Luiijfa (2013): 5). Austrija, Njemačka, Francuska, Indija, Nizozemska, Novi Zeland, Rumunjska i Južna Afrika koriste svoje definicije nacionalne sigurnosti. Velika Britanija i Kanada samo deskriptivno opisuju kibernetičku sigurnost bez davanja relevantne definicije.

Na ovoj stranici stoji tablica preuzeta od: Eric Luiijf, Patrick de Graaf i Kim Besseling (2013): 5, u kojoj su navedene su sve relevantne definicije / opisi kibernetičke sigurnosti za neke međunarodne faktore (preuzeto 3.6.2022):

DEFINICIJE / OPISI KIBERNETIČKE SIGURNOSTI

AUSTRIJA	Kibernetička sigurnost su mjere koje se odnose na povjerljivost, dostupnost i integritet informacija koje se procesuiraju, spremaju I preko kojih se komunicira preko elektronskih ili sličnih sredstava.
KANADA	Kibernetička sigurnost je prikladna razina odgovora na / izbjegavanje kibernetičkih napada – namjernih, neautoriziranih proboja informacija, sredstava, manipulacija, prekid ili uništavanje elektronskih podataka i infrastrukture koji se koriste za procesuiranje, komunikaciju i spremanje podataka (elektronskim putem).
NJEMAČKA	Kibernetička sigurnost je najpoželjniji objekt IT (informacijske) sigurnosne situacije, u kojem je rizik (globalnog) kibernetičkog prostora reduciran na prihvatljivi minimum. Dodatno: Njemačka civilna i vojna sigurnost definirane su na vrlo sličan način
FRANCUSKA	Kibernetička sigurnost je dopuštanje informacijskom sustavu da se odupre događajima koji bi je mogli pogoditi iz domene kibernetičkog prostora koji bi mogli ugroziti dostupnost, integritet i povjerljivost spremljenih, procesuiranih ili prenesenih podataka i sustava vezanih za informacijski ili komunikacijski kanal informacija (ICT).
VELIKA BRITANIJA	Kibernetička sigurnost prihvaća i zaštitu nacionalnih interesa u kibernetičkom prostoru, također i ostvarenje šireg značenja politike kibernetičke sigurnosti preko eksploatacije mnogih prilika koje kibernetički prostor nudi.
INDIJA	Kibernetička sigurnost je aktivnost zaštitite informatičkih i informacijskih sustava (mreža, računala, baza podataka, centara podataka i primjene podataka) sa prikladnim proceduralnim i tehnološkim sigurnosnim mjerama.
NIZOZEMSKA	Kibernetička sigurnost je biti slobodan od opasnosti ili štete koja bi se mogla dogoditi zbog ometanja ili uništavanja informacijsko komunikacijskih sustava.
NOVI ZELAND	Kibernetička sigurnost je praksa gdje se pokušavaju osigurati kibernetičke mreže na najbolji mogući način protiv neželjenih upada, kako bi se sačuvala povjerljivost, dostupnost, autentičnost i neizmjenjivost elektronskih podataka i očuvanje javnih i privatnih usluga u kibernetičkom prostoru.
RUANDA	Kibernetička sigurnost je standard koji je rezultat primjene seta proaktivnih i reaktivnih mjera koje garantiraju povjerljivost, integritet, dostupnost, autentičnost podataka i sprječavanje povrede elektronskih podataka i javnih ili privatnih resursa i sustava u kibernetičkom prostoru.

Većina od ovih devetnaest država ponajviše je fokusirana na ekonomski prosperitet u kibernetičkom okruženju. Kibernetička sigurnost smatra se kao osnovna i minimalna potreba kako bi se poboljšao prosperitet nacije i ekonomska dobrobit države. No postoji jedan veliki problem, većina ovih država nije sigurna tko treba biti najviše zadužen za kibernetičku sigurnost, a kada se dogodi neki napad, vladine institucije ne žele priznati odgovornost. Neke države, kao dio svoje strategije nacionalne sigurnosti, kibernetičku sigurnost stavljaju u nadležnost vojnog sektora gdje se onda većinom provode vojne kibernetičke operacije, što može dovesti do predominantnog militarističkog pristupa kibernetičkog sigurnosti. Najjasniju ulogu vojnog sektora po pitanju kibernetičke sigurnosti ima definirana Njemačka (Lujiif, 2013: 7 – 11).

Craigen, Diakun - Thibault i Purse (2014) također imaju vrlo sličan zaključak Lujiifu et al. gdje istraživanjem zaključuju kako su prijašnje definicije vrlo često vezane uz određeni kontekst, iznimno varijabilne, subjektivne i neinformativne te ne mogu obuhvatiti multi - dimenzionalnost koncepta.

Cilj ovih autora, stvarajući novu definiciju, je obuhvatiti holistički pristup koji kibernetičku sigurnost opisuje više kao interdisciplinarnu aktivnost koja obuhvaća više perspektiva odjednom, umjesto predominantne tehnološke perspektive. Korištenjem devet, autorima relevantnih, definicija koje pružaju materijalnu definiciju kibernetičke sigurnosti, pokušavaju izvesti novu interdisciplinarnu definiciju. Craigen, Diakun – Thibault i Purse (2014): 3, identificirali su pet dominantnih tema kibernetičke sigurnosti: 1) tehnološka rješenja, 2) događaji, 3) strategije, procesi i metode, 4) ljudski angažman i 5) referenti objekt (sigurnosti). Nadalje, identificirali su da se kibernetička sigurnost razlikuje po: 1) njenom interdisciplinarnom sociološko-tehnološkom karakteru, 2) potpunom otvorenošću mreže, gdje su sposobnosti mrežnih aktera potencijalno slične i 3) visokom stupnju promjene, povezanosti i brzini interakcije.

3.3. Nova terminologija kibernetičke sigurnosti

Na temelju svojih istraživanja, autori daju novu definiciju kibernetičke sigurnosti koja glasi: kibernetička sigurnost je organizacija i sakupljanje resursa, procesa i struktura koji se koriste kako bi se zaštitio kibernetički prostor i sustav od događaja koji bi mogli poremetiti de jure od de facto pravo vlasništva (Craigen et al. (2014): 5).

Definicija kibernetičke sigurnosti, kako je navedena u britanskoj strategiji „UK National Cyber Security Strategy 2016 – 2021“ glasi: kibernetička se sigurnost referira na zaštitu informacijskih sustava (*hardware*, *software* i ostalih povezanih struktura), podataka na njima i usluga koje oni pružaju kako bi se mogli spriječiti neautorizirani upadi, pravljenje štete i pogrešna praksa. To uključuje i namjerno napravljenu štetu od strane operatera ili nenamjerno napravljenu štetu koja je rezultat neuspjelog (ili nepostojećeg) korištenja sigurnosnih procedura (Rashid, 2019: 2). Iako je to jedna od mnogih definicija, ona poprilično kvalitetno odgovara na izazov definiranja same kibernetičke sigurnosti, štoviše, ova definicija derivirana je iz ENISA definicije koja se i najviše koristi. Ova definicija posebno naglašava ljudsko ponašanje kao najvažniji faktor za samu potrebu postojanja kibernetičke sigurnosti (Rashid, 2019: 2). Vrlo je važno dati i sveobuhvatnu definiciju kibernetičkog prostora koja obuhvaća niz područja kako bi se mogao razumjeti kontekst: „kibernetički prostor je mjesto gdje se zaključuje i provodi posao, mjesto gdje se događa ljudska komunikacija, mjesto gdje se izrađuje i uživa umjetnost, mjesto gdje se stvaraju razne veze itd. U tom prostoru također mogu nastati kibernetički zločini, kibernetički terorizam i kibernetički ratovi koji imaju ne samo virtualne posljedice, već i posljedice u stvarnom životu“ (Rashid, 2019: 3).

No kibernetička sigurnost ne bi mogla postojati bez svojeg prethodnika – informacijske sigurnosti. Kibernetička je sigurnost zapravo nastala kao zasebna grana informacijske sigurnosti, a danas je kibernetička sigurnost postala obavezni dio svake strategije nacionalne sigurnosti. Kako bi se razumjela kibernetička sigurnost kao cjelina, potrebno je definirati i informacijsku sigurnost. Informacijska sigurnost je zaštita povjerljivosti, integriteta i dostupnosti informacija, dodatno, važna su i ostala svojstva informacija kao što su autentičnost, sveobuhvatnost, zaštita od povrede i povjerljivosti informacija (Rashid, 2019: 2).

Razvitkom digitalne tehnologije razvijale su se i neke druge vrste sigurnosti osim gore navedenih: računalna sigurnost, mrežna sigurnost, sigurnost protoka informacija i sigurnost sustava – kao dio sustavnog inženjeringa (Rashid, 2019: 3). Sve ove vrste sigurnosti zapravo su dio korporativne sigurnosti i međusobno su neizostavne. Korporativni sektor danas je u potpunosti ovisan o korporativnoj sigurnosti koja se sve više i više bazira na zaštiti od kibernetičkih prijetnji i osnivanju posebnih odjela korporativne sigurnosti sa naglaskom na kibernetičku zaštitu.

4. KORPORATIVNA SIGURNOST

Uz kibernetičku sigurnost, za ovaj je rad vrlo važno definirati i korporativnu sigurnost, s obzirom na fokus zaštite privatnog sektora od kibernetičkih prijetnji. Nikolić i Sinkovski (2013): 1; iz Čemerin (2016) definiraju ključan zadatak korporativne sigurnosti: „zadatak je korporativne sigurnosti da poslovni sustav učini stabilnim (zaštićenim) na putu razvoja i u okolnostima svakodnevnog povećavanja neizvjesnosti i rizika." Po njima, zaštita korporativnog sektora ne odnosi se samo na puku tjelesnu i tehničku zaštitu, već i na zaštitu cjelokupne imovine. To obuhvaća racionalno korištenje resursa, zaštitu tajnosti poslovnih odluka te zaštitu poslovne tajnosti. Uz to, korporativna sigurnost zadužena je i za provedbu međunarodnih standarda unutar kompanije (Nikolić, Sinkovski (2013): 1; iz Čemerin (2016). Za Boškovića (2018: 47), komunikacijska infrastruktura i korištenje adekvatnih informacija danas su glavna obilježja efikasnog vođenja (privatne) kompanije. Kako bi se ta obilježja u potpunosti mogla ostvariti, potrebno je koristiti internet s kojim, naravno, dolaze i mnoge prijetnje za korporativni sektor. Prebacivanjem biznisa na *online* servere, javila se potreba za novom vrstom sigurnosti – kibernetičkom sigurnosti kao dijelom korporativne sigurnosti.

Kibernetički prostor je u zadnja dva desetljeća postao glavni prostor provođenja biznisa. Internet je doslovno postao svakodnevica velikom broju ljudi, kako bilo privatno, tako i javno. Što se tiče samog poslovnog sektora, kibernetički je prostor postao široko prihvaćena arena za opsežniju i bržu komunikaciju, ekonomska sfera koja se konstantno prepliće sa socijalnim životom pojedinaca (Kaurin; iz Trivan, 2018: 151). Tvrtka *Microsoft* i neovisne analitičke kuće već godinama sa svojim istraživanjima dokazuju kako su kompanije i privatni korisnici interneta ranjiviji nego ikada prije. Kibernetički su napadi, nažalost, postali normalan dio života svakog korisnika. Ovaj problem zahvaća milijarde ljudi, dok se, uz to, svakih sedam minuta dogodi neka vrsta kibernetičkog napada na privatne kompanije (Kaurin, iz Trivan, 2018: 152).

Važno je napomenuti kako je korištenje informatičke tehnologije (IT) znatno proširilo ljudske sposobnosti procesuiranja, sakupljanja, pohranjivanja, korištenja i prezentiranja informacija (Kaurin (2017); iz Trivan, 2018: 152). Korištenjem interneta, javljaju se i mnogi rizici, a neki od njih su: otkazivanje informatičke opreme, greške u programima i procedurama, ljudske greške, a posebice štetni su: namjerno uništavanje i izmjenjivanje povjerljivih informacija, oštećivanje i onemogućavanje funkcioniranja opreme, korištenje informacija u zlobne svrhe, krađa intelektualnog vlasništva te blokiranje efikasnosti informacijskih sustava. Zbog svega gore navedenoga, kako navodi Kaurin, danas se gotovo nemoguće (tj. ekstremno teško) boriti tradicionalnim sigurnosnim metodama. Može se zaključiti kako su potrebne nove metode

zaštite korporativnog sektora. Za korištenje novih metoda ključno je imati stručnjake za kibernetičku sigurnost koji pravovremeno mogu reagirati na neku i umanjiti posljedice kibernetičkih napada.

Informacijska tehnologija (IT) okarakterizirana je sa nekoliko ključnih značajki: dostupnost, volumen, komunikativnost, ekonomičnost, brzina i preciznost (Kaurin (2017); iz Trivan, (2018): 152). Korištenje informacijskih tehnologija znatno povećava ljudsku efikasnost obavljanja poslova. No ta se efikasnost stalno pokušava omesti sa raznim pokušajima kibernetičkih napada. Postoje razni načini održavanja te efikasnosti, a jedan od najboljih je postojanje adekvatnog sigurnosnog sustava. Za Kaurin, taj sigurnosni sustav mora biti dobro dizajniran, sveobuhvatan, detaljan, sa sigurnosnim i kontrolnim mehanizmima, sa precizno definiranim pravima, odgovornosti i sankcijama za sve kategorije korporativnih tijela (2018: 152). Tom se problematikom posebno bave stručnjaci koji su proizveli ISO / IEC (*International standardization in the field of information technology*) standarde. Ovih standarda bi se trebao držati svatko tko se želi probati adekvatno zaštiti od kibernetičkih napada. Prema web stranici *advisera.com*, ISO 27001 je zapravo najpopularniji i najviše prihvaćeni međunarodni standard koji opisuje kako upravljati informacijskom sigurnošću u tvrtkama. Objavljen je od strane Međunarodne organizacije za Standardizacije (ISO). Prva inačica ovog standarda objavljena je 2005. godine, dok je najnovija inačica objavljena 2013. godine. Postoji nekoliko osnovnih ISO / IEC kategorija koje se odnose na sigurnosne standarde, a to su:

- Procjena rizika
- Sigurnosna politika
- Organizacija informacijske sigurnosti
- Klasifikacija i kontrola imovine
- Sigurnost ljudskih resursa
- Fizička sigurnost i sigurnost okruženja
- Upravljanje komunikacijama i operacijama
- Kontrola pristupa
- Nabava, razvoj i održavanje informacijskih sustava

- Upravljanje incidentima informacijske sigurnosti
- Upravljanje poslovnim kontinuitetom
- Usklađenost

Iako je svaki standard zaseban i kompleksan, oni zajedno čine jednu veliku, usko povezanu cjelinu (Trivan, 2018: 153).

5. SIGURNOSNA PARADIGMA U MODERNOM SVIJETU

Prijetnje na području korporativne sigurnosti vidljive su i u fenomenu kibernetičkog terorizma. Kibernetički terorizam može posebice biti opasan za korporativni sektor jer može narušiti financijsko blagostanje neke kompanije i u potpunosti uništiti njihovu reputaciju krađom povjerljivih podataka. Kibernetički terorizam danas je jedna od najvećih prijetnji nacionalnoj, korporativnoj i općenito sigurnosti pojedinca. Destruktivne metode sve su inovativnije, a mete više nisu samo država i njene institucije, već su ugroženi i pojedinci i korporativni sektor. Zbog toga se smatra da su sigurnosni izazovi, rizici i prijetnje međusobno isprepleteni, uvjetovani, raznovrsni i međusobno se nadopunjavaju. Sigurnosne izazove motiviraju popisi zaštićenih vrijednosti i informacija, kao i dobro razumijevanje same sigurnosti (Trivan, 2012). Moderna tehnologija doprinijela je i razvoju sofisticiranijih alata za masovno narušavanje sigurnosti za koje država i privatni sektor često uopće nemaju odgovor, stoga se ne mogu adekvatno zaštititi od tih prijetnji. Po pitanju odgovora na sigurnosne prijetnje, međunarodna zajednica ima problema. Naime, međunarodna zajednica nikako nije složna u pronalasku zajedničkog rješenja za situaciju koja se događa u svijetu. Ono što može okarakterizirati međunarodnu zajednicu danas je multi polarnost i jedna velika borba za prevlast i moć, no tradicionalni pogled na sigurnost više nije jedini relevantan pogled (Pejanović, iz Trivan, 2018: 238).

Nakon što se u potpunosti redefinirao i sam pojam sigurnosti, danas se sigurnosna paradigma može opisati kao percepcija mogućnosti, potrebe i modaliteta očuvanja sigurnosti na nekoliko različitih razina – očuvanje sigurnosti društva kao cjeline, preko korporacija i drugih entiteta pa sve do očuvanja sigurnosti pojedinca (Pejanović, iz Trivan, 2018: 239). Ovakav pogled na sigurnost se znatno razlikuje od tradicionalnog pogleda na sigurnost gdje su vojska i politika (prvenstveno javni sektor) bili dominantni faktori, bez fokusa na privatni sektor i pojedinca samog. No u zadnjih nekoliko desetljeća itekako je postalo jasno da je i privatni sektor (korporacije i pojedinac) jednako važan faktor sigurnosti. Dok je nekad država i njena sigurnost bila referentni objekt zaštite, danas je referentni objekt zaštite postala ljudska sigurnost

općenito. Pod ljudskom se sigurnošću podrazumijeva sigurnost pojedinca, njegova sfera interesa, te ekonomska, ekološka, društvena i kulturološka sfera (Pejanović, iz Trivan, 2018: 239 - 240). Zaključno, tradicionalni (vojni) pogled na sigurnost države danas se redefinirao na moderniji, više humanistički pogled na sigurnost i zaštitu pojedinca, tj. zaštitu osnovnih ljudskih prava i zaštitu privatnog sektora.

6. KIBERNETIČKE PRIJETNJE

Korporativni sektor sve je više i više izložen kibernetičkim prijetnjama te postoji sve veća potreba za širenjem koncepta sigurnosti, tako da se sigurnost može podijeliti na više područja kako bi se sa svakim problemom moglo zasebno baviti. Prošireni koncept sigurnosti obuhvaća privatni sektor i ljudsku sigurnost, a pod ljudskom sigurnošću se podrazumijeva i zaštita od kibernetičkih prijetnji. Kibernetičke prijetnje mogu se okarakterizirati kao jedne od najgorih prijetnji nacionalnoj sigurnosti danas (Poulsen, 1999; Porteus 2001). Myriam Dunn Cavelty (2010: 197) navodi kako postoje tri vrste kibernetičkih prijetnji: kibernetički zločin (*cyber crime*), kibernetički terorizam (*cyber terrorism*) i kibernetički rat (*cyber war*). Prvi spomen kibernetičke prijetnje javlja se u SAD-u kasnih 80-ih godina, no pravi zamah kibernetičkih prijetnji javlja se sredinom 1990-ih godina, dok se u druge zemlje prošilo kasnih 90-ih godina 20. stoljeća. S obzirom da je SAD pionir u prepoznavanju kibernetičkih prijetnji, oni su oblikovali i percepciju kibernetičke prijetnje (Brunner i Suter, 2008). S jedne strane, navodi Miriam Dunn Cavelty, debata je bila oblikovana fokusirajući se na post – hladnoratovski koncept gdje se spominju asimetrična ranjivost i širenje zlonamjernih aktera (državnih i ne-državnih) čiji su kapaciteti za nanošenjem štete sve veći. S druge strane, navodi M. D. Cavelty, rasprava o kibernetičkim prijetnjama oduvijek je spominjana u kontekstu informacijske revolucije gdje ta revolucija utječe na svaku poru života. Razvijanjem sigurnosno – informacijske paradigme, zaključuje se kako su gore navedene tri vrste kibernetičkih prijetnji međusobno isprepletene, pa tako često dolaze u kombinaciji (Dunn, 2010: 194 – 198).

Prvo, spomen kibernetičkog zločina javlja se integracijom telekomunikacija s računalima, na koje se mogao spojiti svatko tko ima računalo i modem. Kako se korištenje interneta širilo, tako se širio i diskurs o kibernetičkim prijetnjama među političkim akterima – jer je to utjecalo na svakodnevni život građana. No uskoro se percepcija kibernetičke prijetnje pojedincu promijenila na kibernetičku prijetnju nacionalnoj sigurnosti. To se dogodilo kada su krenuli hakerski napadi grupe „414s“ na vladine organizacije s ciljem krađe povjerljivih informacija

(Dunn, 2010: 198). Grupa „414s“ ,u kojoj su djelovali većinom maloljetnici, bila je razlog osvještavanja američke političke elite o kibernetičkim napadima, uskoro nakon toga dolazi do mijenjanja strategije nacionalne sigurnosti. Kibernetički napad „*Cuckoo's egg*“ bio je prvi otkriveni slučaj kibernetičke špijunaže SAD-ovih institucija koji je bio financiran od strane KGB-a. Cifford Stoll je sa svojom upornošću uspio doći do samog izvora hakiranja i svojim metodama utkao je put za bolji nadzor ranjivih računalnih sektora kao što je na primjer pasivno praćenje računala kako bi se spriječile razne vanjske prijetnje (*passive monitoring*). Ovaj slučaj pokazao je američkoj političkoj eliti kako su izloženi kibernetičkim napadima, njihove institucije su vrlo ranjive, a sami građani ne pridaju dovoljno pažnje primjeni sigurnosnih protokola (od najjednostavnijeg mijenjanja originalnih lozinki pa sve do nenamjernog propuštanja hakerskih alata na računalo). Kibernetički zločin može se okarakterizirati kao najbliža poveznica surovoj realnosti modernog svijeta (Dunn, 2010: 199).

Sredinom 1990-ih javlja se problem kibernetičkog terorizma. Od tog trenutka, kibernetičke prijetnje viđene su kao prijetnja osnovnim vrijednostima društva kao cjeline, kao i prijetnja ekonomskom i socijalnom probitku cijelih nacija. Nadalje je uspostavljeno kako se štetni napadi na infrastrukturu mogu izvršiti na ogroman broj načina koje skoro nitko unaprijed ne može predvidjeti, a te napade može izvršiti svatko tko ima pristup računalu i internetu. Postoje mnogi razlozi zašto bi netko izvršio kibernetički napad - od maloljetničkog hakiranja iz zabave, organiziranog kriminala pa sve do političkog aktivizma i strateškog ratovanja (Dunn 2010: 199). Ovaj novi neprijatelj može biti u potpunosti nevidljiv, jer njegov identitet ne mora imati jasne poveznice sa nacijom ili državom. Posljedice čak i najmanjeg kibernetičkog napada mogle su se pretvoriti u veliki unutardržavni ili čak međunarodni incident. Zbog široke i lake dostupnosti hakerskih alata svim korisnicima interneta, njihovih nejasnih ali drastičnih posljedica, termin „kibernetički terorizam“ (*cyber terrorism*) ušao je u svakodnevni javni diskurs (Dunn, 2010: 199).

Do tog trenutka, kibernetski napadi su se shvaćali samo kao krađa povjerljivih informacija, no to se ubrzo promijenilo kada su terorističke organizacije počele koristiti alate hakiranja kao način onesposobljavanja vojne obrane neke države, u tom trenutku, SAD-a. Kibernetički zločin više nije samo zločin, već i terorizam – s obzirom na ugrožavanje nacionalne sigurnosti neke države.

Postoji još jedan vrlo važan termin koji se razlikuje od ova dva gore navedena, (kibernetički zločin; kibernetički terorizam) a to je kibernetički rat. Ovaj pojam razvijao se paralelno sa

pojmom kibernetičkog terorizma, ali važnost dobiva nakon Drugog Zaljevskog rata (1990 – 1991) kada se zaključuje da je američka vojska koristila kibernetičke napade kao sredstvo za postizanje prevlasti u ratu. Sam pojam kibernetičkog rata se, na međunarodnoj sceni, javlja 1999. godine kada je NATO reagirao na rat u bivšoj Jugoslaviji (koji se još popularno naziva „prvi rat vođen u kibernetičkom prostoru; prvi rat na internetu“) gdje se prvi put koristio puni kapacitet informacijskog ratovanja (Dunn, 2010: 200). Korištenjem *DDoS* (*distributed denial of service*) napada na razne *web* stranice i širenjem lažnih informacija o tome kako je američka vojska hakirala privatne račune Slobodana Miloševića doprinijeli su pobjedi NATO-a protiv Jugoslavije. Mediji su također igrali veliku ulogu u tom informacijskom ratovanju zato što su širenje propagande i širenje dezinformacija jedni od važnijih aspekata informacijskog ratovanja. Informacijsko ratovanje znatno je utjecalo i na korporativni sektor koji je oduvijek bio najidealnija meta za postizanje destrukcije nekog privatnog poretka.

6.1. Vrste kibernetičkih napada

Korporativni sektor danas ima cilj postići čim veću kibernetičku sigurnost. Što se tiče same kibernetičke sigurnosti, ona je postala jedan vrlo važan i nezaobilazan koncept 21. stoljeća. Brzi protok podataka (preko interneta) stvorio je potrebu za stvaranjem novog sigurnosnog okruženja. Modernizacijom tehnologije, privatni i javni sektor dijele sve svoje podatke preko interneta, pohranjujući ih na informacijskim oblacima (*Cloud Storage*). No to može značiti i proboj sigurnosti, s obzirom da to može biti (nenamjerno) dostupno široj javnosti. Kibernetički su napadi stoga postali svakodnevnica. Zloćudne aktivnosti na internetu (*Malware activity*) mogu zahvatiti ogroman dio populacije, točnije, kako javan, tako i privatan sektor. Neke od tih zloćudnih aktivnosti na internetu su: hakiranje, *DDOS* napadi (uskraćivanje usluge), razne prijevare koje najčešće rezultiraju krađom identiteta (*Phising*) te krađom zaporki i korisničkih imena (*Pharming*). Vrlo se često koriste i tzv. crvi (*Worms*) kako bi raširili virus do krajnjeg korisnika i tako bili u mogućnosti kontrolirati žrtvin operativni sustav te to najčešće završava krađom vrlo važnih i povjerljivih podataka koje onda ugrožavaju cijelo poslovanje neke osobe, kompanije ili države. Stoga je vidljivo da se zapravo zloćudne aktivnosti odnose na sve korisnike interneta, nevažno je li to privatnog ili javnog svojstva.

Zlonamjerni softver (*Malware*) predstavlja softver koji, bez vlasnikova znanja i pristanka, ulazi u računalo i radi štetu. Svojstvo zlonamjernih softvera je neprimjetni ulazak u računalo gdje pruža zarazu računala i skriva svoju prisutnost. „U globalnom istraživanju o informacijskoj

sigurnosti iz 2019. godine koju je proveo EY, zlonamjerni softver predstavlja drugu po redu najveću sigurnosnu prijetnju organizacijama dok ga ENISA već treću godinu zaredom svrstava na prvo mjesto“ (Arbanas, 2021: 55).

Neželjena pošta (*Spam*) jedna je od najčešće zastupljenih pokušaja „lakih“ kibernetičkih napada gdje se u prostor elektroničke pošte guraju e-mailovi sa neželjenim sadržajem koji sadrže podvale i poveznice do web stranica kojima je cilj krađa povjerljivih podataka kao što su najčešće lozinka od email adrese koja ih je i preusmjerila na tu web stranicu. Za spam ne postoje učinkoviti načini obrane, tj. učinkovite protumjere te ono stvara ozbiljan problem u online zajednici jer ono zakrčuje informacijske sustave neželjenim porukama, što troši propusnost i resurse e mail sustava (Campbell; iz Arbanas, 2021: 55).

Špijunski softver (*Spyware*) je svaki softver koji narušava privatnost korisnika i koji je implementiran na način da narušava korisnikovu kontrolu nad računalom. Uz to, ovakav softver prikuplja, distribuira i koristi osobne i osjetljive podatke kako bi utjecao na korisnikovo iskustvo korištenja sustava. Najčešće je cilj tom prikupljanju podataka upijanje korisnikovih navika kako bi onda preusmjerio npr. web preglednik na (ne)željeno mjesto. Uz to, ovaj softver može i usporiti uređaj i prikazivati skočne oglase. Najpoznatiji spyware su tako oni koje koriste Internet trgovine kako bi reklamirali svoje proizvode i u konačnici natjerali korisnike da kupe neki njihov proizvod. Ovaj softver se prilagođava korisnikovim pretraživanjima i zapravo ih špijunira (Arbanas, 2021: 56).

Oglašivački softver (*Adware*) vrlo je sličan špijunskom softveru, no za razliku od njega, ovaj softver ne krade privatne podatke niti ih distribuira, već se koristi samo u svrhu zarade preko interneta. Ovaj softver prikazuje neželjene oglase koji ometaju korisnike i čine ih nezadovoljnima. Ovo je vrsta neželjenog marketinga jer ometa korisničko iskustvo na internetu, a u konačnici i korisnikovu produktivnost (Arbanas, 2021: 57).

Ucjenjivački softver (*Ransomware*) je zlonamjerni softver koji je namijenjen za prepoznavanje i enkripciju vrijednih (tajnih) podataka kako bi onda iznudio novčanu naknadu za te informacije. Najčešće to bude klasično ucjenjivanje gdje se prijeti da će se podaci ili izbrisati ili javno objaviti. Ovakav softver se najčešće instalira nakon što korisnik otvori spam e-poštu ili klikne na neželjenu poveznicu te se onda zlonamjerni kod prenese na korisnikovo računalo gdje ima apsolutni pristup svim podacima (Arbanas, 2021: 57).

Virus je vrsta zlonamjernog softvera koji se priključuje na neke druge programe. Svojom aktivacijom, on namjerno reproducira i širi u ostale sustave/računala. Ovaj virus djeluje na

sličan način kao i biološki virus koji uvijek ima „*patient zero*“ tj. domaćina koji taj virus širi dalje. Ovi domaćini su najčešće originalne sistemske datoteke. Cilj ovog virusa, osim krađe podataka, je onesposobljavanje funkcionalnosti računala brisanjem ili izmjenom datoteka, potrošiti sav slobodan prostor na tvrdom disku, formatirati (izbrisati) ga ili jednostavno olakšati prisup svim drugim virusima (Arbanas, 2021: 58).

Crv (*Worm*) je vrsta zlonamjernog softvera koji se samostalno razmnožava i širi internetom, e-poštom, zaraženim web stranicama i instant porukama – za razliku od virusa, njemu nije potrebna ljudska aktivnost da bi se širio (Arbanas, 2021: 59).

Trojanski konj (*Trojan Horse*) je zlonamjerni softver koji sebe prikazuje kao legitimni program i korisni program koji ljudi svojevoljno instaliraju na računalo, no on u tom istom trenutku obavlja i zlonamjernu aktivnost – pretraživanje sustava zbog broja kreditnih kartica i lozinka gdje se onda povezuje sa nekim udaljenim sustavom i šalje te povjerljive informacije dalje (Arbanas, 2021: 59)

7. SURADNJA PRIVATNOG I JAVNOG SEKTORA PO PITANJU KIBERNETIČKE SIGURNOSTI

Postalo je normalno da danas većina javnog i privatnog sektora ovisi o informacijskoj tehnologiji. No korištenje informacijske tehnologije sa sobom donosi i rizike koji nisu limitirani na neku fizičku lokaciju, već se mogu pojaviti neočekivano i sva svih mogućih lokacija. Dapače, većina kibernetičkih napada ima sakrivenu lokaciju i teško je otkriti od kud oni dolaze. „Kibernetička sigurnost okarakterizirana je sa fundamentalnom nesigurnošću“ (Kjaersgaard, 2017: 2). S obzirom na ogromnu dozu nesigurnosti, moguće rješenje pokušaja obrane od kibernetičkih napada je sklapanje javno-privatnih partnerstava (PPP)[3]. Javno - privatna partnerstva imaju takvu vrstu organizacije u kojoj je povećana fleksibilnost i otpornost u odnosu na samo javni ili samo privatni sektor zato što uključuju širi spektar aktera: civilnih i privatnih (Kjaergaard, 2017: 2).

Javno – privatno partnerstvo slijedi čistu logiku tržišta prema kibernetičkoj sigurnosti, tvrdi Carr (2016: 1). Myriam Dunn Cavelty i Sutter javno - privatna partnerstva vide kao prebacivanje sigurnosne odgovornosti (javnog sektora) na tržišno orijentiran privatni sektor.

[3] Javno-privatno partnerstvo podrazumijeva suradnju tijela javne vlasti s privatnim sektorom, bilo na razini središnje ili lokalne zajednice, s ciljem zadovoljavanja neke javne potrebe (Persoli (2007): 111).

Javno - privatna sigurnosna partnerstva ne baziraju se samo na strateškom sebičnom interesu, već se baziraju i na praksi lojalnosti (patriotskoj, profesionalnoj ili osobnoj) koja se zapravo može smatrati društvenim ljepilom. Lojalnost drži partnerstva zajedno te otvara prostor za vodstvo i usmjerivanje (Kjaergaard, 2017: 3).

Po tradicionalnom pogledu, država – nacija je oduvijek bila zadužena za nacionalnu sigurnost – zaštitu granica i ostvarivanje unutrašnje sigurnosti države. No tradicionalni pogled na nacionalnu sigurnost više nije relevantan, prvenstveno zbog prirode novih prijetnji kao što su terorizam, klimatske promjene i kibernetičke prijetnje. Novi pogled na sigurnost je taj da je potrebna suradnja između privatnog i javnog sektora. Privatni sektor je zapravo dobio ulogu suučesnika ostvarivanja sveopće sigurnosti. Američki predsjednik Barack Obama prvi je naglasio potrebu javno - privatnih partnerstava i izjavio da se protiv kibernetičkih prijetnji može boriti jedino suradnjom privatnog i javnog sektora. Europska unija u svojim strateškim dokumentima ističe javno - privatna partnerstva kao adekvatan način borbe protiv kibernetičkih prijetnji. U SAD-u se broj ovakvih javno - privatnih partnerstava drastično povećao, više od njih stotinu koji su povezani ili sa sustavom Domovinske sigurnosti (*Homeland Security*) ili sa radom FBI. Iako u Europi ne postoji toliko velik broj PPP-a kao u SAD-u, ona su i dalje vrlo značajna – ali nemaju nikakav aspekt institucionalizacije kao što to imaju u SAD-u. Privatne kompanije u Danskoj, Velikoj Britaniji i Švedskoj u kontaktu su sa nacionalnim sigurnosnim agencijama, ali nemaju neko stvarno institucionalno partnerstvo sa njima (Kjaergaard, 2017: 4).

Mnogi akademski autori, uključujući i javnost u Europi smatraju kako su razlike između privatnog i javnog sektora jednostavno prevelike i iziskuju ogromnu dozu truda i vremena kako bi se moglo ostvariti partnerstvo između njih, no to je opet tradicionalan pogled na sigurnost. U današnje vrijeme, čak su se i interesi promijenili, kako za državu, tako i za korporativni sektor, svima je u cilju minimizirati troškove, a to se može napraviti zajedničkom obranom od kibernetičkih prijetnji – procjena rizika mnogo je važnija od pukih troškova sigurnosti. Iako je za Europsku uniju pojam suradnje između privatnog i javnog sektora po pitanju sigurnosti još uvijek dosta nespojiv, SAD je dokazao kako PPP može funkcionirati na određeni način.

8. PRIKAZ PRAKSE ORGANIZACIJA KIBERNETIČKE SIGURNOSTI

8.1. DEMOKRATSKE DRŽAVE

Demokratske države imaju jedan veliki izazov u obrani od kibernetičkih prijetnji. Ne samo da se moraju fokusirati na kibernetičku sigurnost kao takvu, već se ove države moraju držati i nekih vrlo važnih odrednica kako se ne bi povrijedila osnovna ljudska i građanska prava pri obrani od kibernetičkih prijetnji. Postoji snažna potreba za suradnjom demokratskih vlada i privatnog sektora kako bi se uvela najbolja moguća praksa obrane od kibernetičkih prijetnji, a da se uz to očuvaju i sloboda demokratskih izbora i sva osnovna ljudska prava.

8.1.1. NATO i EU

Kibernetička sigurnost je za NATO i EU strateški problem koji utječe na obranu zemalja članica ovih organizacija. Zemlje članice ovih organizacija često su prepuštene same sebi po pitanju kibernetičke sigurnosti jer se ove organizacije fokusiraju na cjelokupnu njihovu sigurnost. NATO se prvenstveno fokusira na sigurnosni i obrambeni aspekt kibernetičke sigurnosti, a EU se više fokusira na širi, većinski ne-vojni aspekt kibernetičke sigurnosti i kibernetičkih problema (sloboda interneta i vladavine, online prava i zaštita podataka) i na unutrašnji sigurnosni aspekt država članica (Pernik, 2014: 3).

NATO i EU dijele zajedničke strateške interese i vrijednosti. NATO, koji je prvenstveno vojni i politički savez se brine o samoobrani, čuva zajedničke vrijednosti koje su nastale razvojem liberalne demokracije (sloboda, ljudska prava, individualna sloboda, demokracija i vladavina zakona) koje dijele sve države članice. Očuvanje sigurnosti glavna je misija NATO saveza – pa tako i očuvanje kibernetičke sigurnosti, no nije u glavnom fokusu. NATO vidi kibernetičke prijetnje kao prijetnje koje ostavljaju negativnu konotaciju za transatlantsku i nacionalnu sigurnost. U Strateškom konceptu (*The Strategic Concept of 2010 NATO Allies*) priznaje se značajnost kibernetičkih napada: „Kibernetički napadi postaju sve učestaliji, organiziraniji i sve skuplji… mogu doseći prag koji prijeti sveukupnom nacionalnom i euroatlantskom prosperitetu, sigurnosti i stabilnosti“ (Pernik, 2014: 3). U deklaraciji donesenoj na sastanku NATO-a u Walesu 2014. godine, odlučeno je kako će NATO braniti sve svoje članice od ugroza sigurnosti – a to se tiče i kibernetičke sigurnosti. Dakle, kibernetička sigurnost je onda prvi puta službeno uvrštena u obrambeni plan NATO saveza.

Zaključno, Europska unija, kao političko – ekonomski savez, fokusira se na unutarnju kooperaciju država članica po pitanju kibernetičke sigurnosti, najčešće provodeći kriminalnu i

policijsku pravdu. Svijest o kibernetičkoj sigurnosti u Europskoj uniji podigla se tek 2010. godine kada se u sigurnosnu strategiju uveo pojam kibernetičkih prijetnja, fokusirajući se na kibernetički kriminal, javno - privatno partnerstvo i izgradnju boljih kapaciteta za obranu od kibernetičkih prijetnja (Pernik, 2014: 3 – 4).

8.1.2. Sjedinjene Američke Države (SAD)

SAD je jedna od mrežno najnaprednijih i najpovezanijih država svijeta. Američka ekonomija, privatni i javni sektor snažno ovise o korištenju kibernetičkog prostora. Za razliku od Kine i Rusije, SAD aktivno promiče slobodu medija i korištenja interneta – a posebice slobodu govora u kibernetičkom prostoru (Puyvelde, 2019: 86). No zbog iznimne otvorenosti kibernetičkog prostora, SAD predstavlja stalnu metu kibernetičke sigurnosti, a sustavi koji su vezani uz kibernetički prostor iznimno ranjivi na ovakve napade.

Kako bi se poboljšala kibernetička sigurnost, SAD je osnovao velik broj organizacija i politika dizajniranih tako da se najefektivnije obrane od kibernetičkih prijetnji. Suradnja privatnog i javnog sektora još je jedan aspekt efektivne obrane od kibernetičkih napada. Američka vlada objavila je i na desetke strateških dokumenata koji se bave kibernetičkim prostorom, njegovom moći, ali i ugrozama. Američki pristup, uz to, potiče i međunarodnu kibernetičku suradnju (prvenstveno kroz NATO) jer smatra da to vodi do efektivnije obrane kibernetičkog prostora (Puyvelde, 2019: 86 – 89).

8.2. AUTORITARNE DRŽAVE

8.2.1. Kina

Kina je poznata po svojem do sada izuzetnom ekonomskom napretku, koji sve više ovisi o postizanju kibernetičke sigurnosti. To je vidljivo u četrnaestogodišnjem planu ekonomskog napretka objavljenom 2000. godine. U tom planu, kinesko društvo oslovljava se kao i informacijsko (napredno) društvo. S obzirom da je u Kini nedostajalo visokoobrazovanih i kvalificiranih ljudi u informacijskom sektoru, država se, naravno, posvetila otvaranju edukacijskih centara i promicala uzimanje informacijske karijere kao ispravne. Ovo je dakako rezultiralo iznimnom tehnološkom naprednošću četrnaest godina kasnije. Kina trenutno dominira svjetskom informacijskom scenom, pogotovo u izgradnji umjetne inteligencije - AI (*Artifical intelligence*). No autoritarni režim je taj koji oblikuje i kibernetičku sigurnost i korištenje kibernetičke moći.

Vanjske kibernetičke prijetnje u Kini su apsolutno minimizirane zato što režim blokira neželjeni vanjski internetski sadržaj sa svojim projektom „Zlatni štit“ (*The Golden Shield*).[4] Za kinesko komunističko vodstvo, kibernetička sigurnost je jedno od sredstava političke kontrole. Zbog apsolutne državne kontrole, koncept javno – privatnog partnerstva ne postoji, Komunistička Partija Kine odlučuje o svemu. Za ovakav režim, osiguravanje od vanjskih prijetnji je ključno, a pod tim se podrazumijeva i kibernetička sigurnost.

Kina svoje kibernetičko znanje koristi i za špijunažu zapadnjačkih država kako bi stekla apsolutnu prevlast u vojnom, tehnološkom i znanstvenom napretku (Puyvelde, 2019: 79 – 82). Zaključno, Kina se ne mora boriti protiv vanjskih kibernetičkih prijetnji, dapače, kibernetičke napade i špijunažu koristi u svoju korist kako bi stekla prevlast u svjetskoj utrci za moć.

8.2.2. Rusija

Rusija je poznata po svojem holističkom pristupu kibernetičkoj sigurnosti koji razmatra strateške interakcije kroz sve elemente moći (Puyvelde, 2019: 82). Ruske vlasti, također kao i Kina, kontroliraju priljev informacija izvana, tako da je i internet u Rusiji izričito kontroliran. Ovo se najbolje može vidjeti sa trenutnim ratom u Ukrajini, gdje su ruskim građanima uskraćene one prave informacije o ratu kako ne bi došlo do pobune zbog agresorske politike Rusije prema Ukrajini. Apsolutnu kontrolu nad mrežama danas ima ruska obavještajna agencija FSB koja je to naslijedila još od sovjetskog KGB-a. Iako Rusija nema izrađeni „veliki vatrozid“, navedena obavještajna agencija strogo nadzire sve medije i potiče ih na širenje patriotizma, nacionalizma i tradicije.

Rusija ima dobro razvijene kibernetičke sposobnosti koje koristi za kibernetičke napade upućene prema Zapadu, a najčešći primjeri su rusko kibernetičko upletanje u demokratske izbore nekih država (dokazano u SAD-u i u Francuskoj). Uz to, Rusija koristi i kibernetičko ratovanje što je vidljivo na primjeru Ukrajine, gdje npr. konstantno koristi DDoS (*Distributed Denial of Service*) kako bi nanijela štetu ukrajinskim institucijama. S ovakvom vrstom djelovanja protiv ukrajinskih državnih i vojnih sustava, Rusija kupuje sebi vrijeme kako bi dobila stratešku prednost (Puyvelde, 2019: 83). Rusija kibernetičku sigurnost koristi kao sredstvo unutrašnje kontrole društva gdje ne postoji suradnja između države i društva pa tako

[4] Projekt cenzure i nadzora informacija i medija kojem je cilj zaštita građana od pritoka informacija koje kineska vlada smatra neprimjerenima. Izvan Kine, u međunarodnoj zajednici, ovaj projekt još ima i naziv*„The Great Firewall“* (veliki vatrozid).

ne postoj ni koncept javno – privatnog partnerstva. Kao i Kina, Rusija koristi kibernetičke napade i špijunažu kao instrument za prikupljanje podataka o protivniku izvan zemlje.

Zaključno, javno - privatno partnerstvo u autoritarnim državama kao što su Kina i Rusija ne može postojati – jer u tim zemljama cilj kibernetičke sigurnosti nije zaštita stanovništva, već zaštita režima, a svi ostali subjekti (uključujući i privredne subjekte i područje korporativne sigurnosti) moraju izvršavati naloge koje dobivaju.

9. KIBERNETIČKA I KORPORATIVNA SIGURNOST U REPUBLICI HRVATSKOJ

Kibernetički prostor danas je ključno područje svjetskog gospodarstva (Vuković, 2012: 1). Pa tako je i u Hrvatskoj svaki ključni aspekt javnog i privatnog poslovanja ovisan o kibernetičkom prostoru. Kibernetičke prijetnje danas su svakodnevnica, ne samo za privatan, već i za javni sektor. Međunarodne institucije i međunarodna suradnja također je izložena kibernetičkim napadima, pa je tako i Ministarstvo vanjskih i europskih poslova zabilježilo pojačane kibernetičke prijetnje prema međunarodnim institucijama kao što su UN, NATO, OESS (Vuković, 2012: 2 – 4). Ako su i međunarodne institucije toliko ugrožene, naravno da još veća prijetnja leži na državnim i lokalnim institucijama, ponešto zbog manjka ljudskih resursa, a ponešto zbog manjka financijskih resursa, a u konačnici i organizaciji same države.

U zakonodavstvu Republike Hrvatske ne nalazi se poseban prostor za kibernetičku sigurnost, već svoju aktivnost provodi kroz, prvenstveno, sustav informacijske sigurnosti, a onda i kroz sustav nacionalne sigurnosti. U Hrvatskoj postoji još jedan veliki problem što se tiče izraza i same definicije kibernetičke sigurnosti. Naime, kao što je prije navedeno, na međunarodnoj razini još uvijek postoji ogromna zbrka oko same definicije kibernetičke sigurnosti, a u Hrvatskoj, osim nejasne definicije postoji i problem sa terminologijom. Naime, mnogi autori se ne slažu oko toga treba li se kibernetička (*cyber*) sigurnost na hrvatski prevoditi kibernetska sigurnost ili kibernetička sigurnost, tako da to dodatno stvara konfuziju. Prvi pokušaj prevođenja pojma *Cyber* bio je kada se prevodila konvencija (*Convention on Cybercrime*) gdje se to prevelo kao Konvencija o kibernetičkom kriminalu.

Neki autori smatraju da je kibernetika krivi prijevod zato što to nije istoznačnica sa riječi Cyber, već je to istoznačnica za riječ *Cybernetics*. Hrvoje Vuković (2012: 5) smatra kako je ispravno

koristiti riječ kibernetska (sigurnost), dok se kroz ovaj rad proteže riječ kibernetička te se smatra da je to ispravna terminologija. No u konačnici, problem oko nazivlja još uvijek postoji, pa je stoga teško uopće stvoriti ispravnu politiku prema tom pojmu.

U Hrvatskoj nije zastupljen neki previše ekstenzivan način borbe protiv kibernetičkog kriminala, već postoje razni sigurnosni sustavi u kojima se spominje i obrana od kibernetičkih prijetnji kao važan dio sigurnosti. Sustav borbe protiv kibernetičkih prijetnji u javnom sektoru često se samo svodi se samo na regulatorni okvir koji predstavlja skup propisa pod kojima kibernetička sigurnost nije ništa drugo no informacijska sigurnost (Vuković, 2012;10), što ne pridaje dovoljno veliku distinkciju kibernetičkim opasnostima, pa je stoga može zaključiti da je i sustav obrane od kibernetičkih prijetnji podosta loš. Zakoni i propisi kibernetičke fenomene uopće ne spominju niti prepoznaju kao kibernetičke/kibernetske.

Ono što u Hrvatskoj ipak pridaje značaj djelovanju protiv kibernetičkih prijetnji su međunarodne konvencije i multilateralni/bilateralni u kojima je RH supotpisnik. Ugovor koji prvi priznaje, 2001. godine, kibernetičke prijetnje i kibernetički kriminal je Konvencija o kibernetičkom kriminalitetu Vijeća Europe. Ova konvencija bavi se svim ključnim pitanjima vezanim za kibernetički (online) prostor i sadrži niz ovlasti koje mogu nužno povećati razinu informacijske/kibernetičke sigurnosti (Vuković, 2012: 11).

Republika Hrvatska ratificirala je Konvenciju o kibernetičkom kriminalitetu Vijeća Europe te promijenila kazneni zakon u korist te konvencije. Novi kazneni zakon nastupio je na snagu 1.listopada 2004. godine gdje se uvrštava (Vuković, 2012: 11):

- Zakon o sigurnosno-obavještajnom sustavu (NN 79/06 i 105/06)
- Zakon o tajnosti podataka (NN 79/07)
- Zakon o informacijskoj sigurnosti (NN 79/07)
- Zakon o zaštiti osobnih podataka (NN 41/08)
- Zakon o elektroničkoj trgovini (NN 173/03)
- Zakon o elektroničkim komunikacijama (NN 73/08)
- Zakon o kaznenom postupku

Mjere kibernetičke sigurnosti u Republici Hrvatskoj propisuju se Uredbom o mjerama informacijske sigurnosti (NN 46/08). Uz to, Ured Vijeća za nacionalnu sigurnost (UVNS)

postavio je nekoliko pravilnika koji imaju obvezu primjene na nacionalnoj razini (Vuković, 2012: 11):

- Pravilnik o standardima sigurnosti podataka
- Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava
- Pravilnik o standardima sigurnosti poslovne suradnje

Uz to, postoje i pravilnici koji propisuju standarde provedbe tehničkih područja sigurnosti informacijskih sustava za koje je zadužen Zavod za sigurnost informacijskih sustava (ZSIS) koji glase (Vuković, 2012: 11 – 12):

- Pravilnik o standardima sigurnosti informacijskih sustava
- Pravilnik o postupanju s kriptografskim dokumentima i kriptografskom opremom za zaštitu klasificiranih podataka
- Pravilnik o prevenciji i odgovoru na računalno-sigurnosne ugroze
- Pravilnik o sigurnosnoj akreditaciji

9.1. Zakon o informacijskoj sigurnosti

U Zakonu o informacijskoj sigurnosti stoji definicija informacijske sigurnosti koja glasi: „informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podataka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda“ (Vuković, 2012: 12). Mjere informacijske sigurnosti su „opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini“ (Vuković, 2012: 12). Informacijska sigurnost je širi pojam koji u sebi sadrži i posebni sektor informatičke sigurnosti koje je zaduženo za računalnu kontrolu stanja, tj. postavljanja vatrozidova (firewall), antivirusa i kriptiranje. Sustav borbi protiv kibernetičkih prijetnji se, stoga, sastoji i od informacijske i od informatičke sigurnosti. Uz to, Vuković navodi i područja informacijske sigurnosti koja su osnova sigurnosnog funkcioniranja modernog informacijskog društva:

- Sigurnosne provjere
- Sigurnost podataka
- Fizička sigurnost

- Sigurnost informacijskih sustava
- Sigurnost poslovne suradnje

Djelokrug informacijske (kibernetičke) sigurnosti u Republici Hrvatskoj spada u djelokrug Ureda Vijeća za nacionalnu sigurnost (UVNS), Zavoda za sigurnost informacijskih sustava (ZSIS), Nacionalni CERT (nCERT), Odjela za visokotehnološki kriminalitet Ministarstva unutarnjih poslova i regionalno Središte za kibernetsku sigurnost unutar Centra za sigurnosnu suradnju RACVIAC (Vuković, 2012: 13).

9.2. Sigurnosne institucije Republike Hrvatske na području kibernetičke sigurnosti

Ured Vijeća za nacionalnu sigurnost (UVNS)

Ured Vijeća za nacionalnu sigurnost je središnje sigurnosno tijelo za informacijsku sigurnost u Republici Hrvatskoj koja, stoga, ima obveze i nadležnosti u međunarodnom i nacionalnom sektoru informacijske (kibernetičke) sigurnosti. Ovo tijelo propisuje, koordinira i usklađuje mjere i standarde koje se donose i primjenjuju kako bi se poboljšala informacijska, tj. kibernetička sigurnost. Ovaj dio odnosi se na gore već spomenuta područja informacijske sigurnosti. Ured Vijeća za nacionalnu sigurnost (UVNS) je zapravo nadležan za organizaciju i upravljanje područjem sigurnosti informacijskih sustava, dok je Zavod za sigurnost informacijskih sustava (ZSIS) nadležan za tehničku implementaciju tehničkih standarda koji se odnose na informacijsku sigurnost, sigurnost akreditacija klasificiranih informacijskih sustava, upravljanje kripto materijalima te za prevenciju i obranu od kibernetičkih napada u državnim tijelima, točnije Vladin CERT (Vuković, 2012: 13).

Nadalje, CARNet ((Hrvatska akademska i istraživačka mreža) - nacionalni CERT) je zadužen za prevenciju i obranu od kibernetičkih napada u javnim (privatnim) informacijskim sustavima (Vuković, 2012: 13). Ured Vijeća za nacionalnu sigurnost još ima i obvezu određivanja klasifikacije podataka pod „povjerljivo“, „tajno“ i „vrlo tajno“ i u skladu s time odrediti stupanj zaštite kako bi se postigla maksimalna sigurnost. Uz to, UVNS konstantno mora usklađivati hrvatske propise sa onima na međunarodnoj zajednici, posebice sa onima u Europskoj Uniji (Vuković, 2012: 13 - 14).

Zavod za sigurnost informacijskih sustava (ZSIS)

Zavod za sigurnost informacijskih sustava je središnje državno tijelo koje je zaduženo za tehnička područja sigurnosti informacijskih sustava, prvenstveno u državnim tijelima, pa u

tijelima jedinica lokalne i regionalne samouprave te pravnim osobama s javnim ovlastima koji koriste klasificirane podatke, navodi Vuković. Zavod za sigurnost informacijskih sustava redovito usklađuje standarde tehničkih područja sa standardima i pravima onih na međunarodnoj sceni te sudjeluje u nacionalnoj normizaciji (ujednačavanju norma) područja informacijskih sustava.

CERT (*Computer emergency response team*) ZSIS-a ima nadležnost nad svim institucijama i pravima kojima zapravo i upravlja sam ZSIS. Stoga se može zaključiti kako u CERT ZSIS-a spada pružanje pomoći tijelima državne vlasti u Republici Hrvatskoj u primjeni mjera (proaktivno djelovanje) kako bi se smanjio rizik od kibernetičkih napada, no ako se napad i dogodi, zadaća je CERTa uspješno ukloniti (reaktivno djelovanje), tj. posredovati u rješavanju posljedica kibernetičkog napada (Vuković, 2012: 14). CERT ZSIS-a također surađuje i sa međunarodnim tijelima koja su zadužena za iste ovlasti, priznat je i od međunarodne udruge CERT-ova i kontinuirano surađuje sa abuse (zloupotreba) međunarodnim službama kako bi dobio pravovaljane informacije, uz to, surađuje i sa hrvatskom policijom i pravosuđem (Vuković, 2012: 14).

Nacionalni CERT

Osnivanju nacionalnog CERT-a prethodio je Zakon o informacijskoj sigurnosti Republike Hrvatske gdje se nalaže da je potrebno osnovati posebno tijelo koje se može boriti protiv kibernetičkih ugroza, a upravo je to CERT. NCERT je tijelo koje se bavi zaštitom javnih informacijskih sustava u Republici Hrvatskoj. Njegova zadaća je bavljenje tzv. incidentom koji se dogodio u hrvatskoj domeni (hr.) ili u hrvatskom IP prostoru, stoji u Pravilniku o radu Nacionalnog CERT-a. Ovo tijelo provodi proaktivne mjere koje se postavljaju prije samog incidenta i drugih mogućih ugroza sigurnosti, točnije, ove mjere nastoje spriječiti da se incident uopće dogodi (obrana od kibernetičkih napada). Uz to, ovo tijelo (nCERT) provodi i reaktivne mjere, točnije, mjere koje se moraju provesti nakon sigurnosnog incidenta koji je najčešće kibernetički napad s ciljem ometanja rada računala ili još gore, s ciljem krađe i manipuliranja osobnim podacima/ tajnim informacijama.

Nacionalni CERT je i u suradnji s ZSIS CERT-om, Uredom Vijeća za nacionalnu sigurnost i Ministarstvom unutarnjih poslova RH. Uz to, naravno, ovaj CERT surađuje i sa drugim međunarodnim CERT-ovima prema kojima prilagođava svoj način djelovanja kako bi bilo efektivnije (Vuković, 2012: 15). Suradnju sa međunarodnim CERT-ovima ostvaruje preko članstva u *Forum of Incident Response and Security Teams* (*FIRST*) i radnoj skupini *Task*

Force – Computer Security Incident Response Teams (TF – CSIRT). Oboje nCERT i ZSIS međusobno surađuju kako bi dali/izradili preporuke i norme iz područja informacijskih sustava u Republici Hrvatskoj (Vuković, 2012: 15).

Odjel za visokotehnološki kriminalitet

Ovaj odjel postoji kao dio Službe gospodarskog kriminaliteta i korupcije Uprave kriminalističke policije Ministarstva unutarnjih poslova Republike Hrvatske, navodi Vuković. Odjel za visokotehnološki kriminalitet „sustavno analizira, prati i izučava fenomenološki i etiološki aspekt kaznenih djela kibernetičkog (računalnog) kriminaliteta, te predlaže rješenja na planu podizanja razine učinkovitosti rada u suzbijanju kibernetičkog kriminaliteta; neposredno provodi složena kriminalistička istraživanja u području kaznenih djela počinjenih na štetu i pomoću računalnih sustava i mreža; obavlja forenzičku analizu i nadzor interneta; pruža specijaliziranu potporu drugim ustrojstvenim jedinicama policije; surađuje s drugim ustrojstvenim jedinicama Ministarstva, tijelima državne uprave i pravnim osobama, policijama drugih zemalja i međunarodnim institucijama u svom djelokrugu rada; sudjeluje u planiranju i izradi programa obuke policijskih službenika u čijem je djelokrugu rada problematika kibernetičkog kriminaliteta; sudjeluje u izradi normativnih akata, izvješća i drugih stručnih materijala iz područja kibernetičkog kriminaliteta te obavlja i druge poslove iz svoga djelokruga rada“ (Uredba o unutarnjem ustrojstvu Ministarstva unutarnjih poslova (NN 070/2012). Ovaj odjel zapravo je zadužen za postupanje sa kaznenim djelima koje je navela Konvencija o kibernetičkom kriminalu, ta Konvencija odredila je i Protokol postupanja kojeg Odjel za visokotehnološki kriminalitet mora slijediti (Vuković, 2012: 16).

Regionalno središte za kibernetsku sigurnost

„*Cyber security project*“ je Radni stol koji je održan u Centru za sigurnosnu suradnju RACVIAC od 12. do 14. prosinca 2011. godine. Ovaj projekt okupio je oko 50-ak stručnjaka iz područja informacijske/kibernetičke sigurnosti, a uz njih su bili i predstavnici zemalja Jugoistočne Europe. Na ovom projektu je dogovoreno kako će RACVIAC služiti kao regionalno središte za kibernetičku sigurnost regija Jugoistočne Europe (Vuković, 2012: 17). Zaključci ovog projekta su kako ova, jugoistočno europska regija, nije dovoljno spremna obraniti se od kibernetičkih prijetnji, a kibernetičke prijetnje na tom prostoru svakog dana rastu. Stoga je bilo potrebno osnovati regionalni centar za kibernetičku sigurnost koji će moći koordinirati sve države regije i nametnuti im protokole i norme kako bi zaštita od kibernetičkih prijetnji bila adekvatnija. Prva faza ovog projekta uključivala bi provođenje edukacijskih i

akademskih aktivnosti u RACVIAC-u, dok bi druga faza uključivala edukativne i istraživalačke aktivnosti (Vuković, 2012: 17).

Sigurnosna suradnja između država Jugoistočne Europe od ključne je važnosti, prvenstveno zato što ni jedna država te regije nije sama sposobna boriti se protiv svih vrsta ugroza modernog doba, a pogotovo ne protiv kibernetičkih prijetnji – ovo je samo zapravo čisto pitanje resursa, tj. manjka istih. Stoga je, da bi se poradilo na suradnji između država Jugoistočne Europe, održana prva takva aktivnost (2012. godine) pod pokroviteljstvom NATO-vog Programa znanost za mir – kao radni stol gdje se prvenstveno raspravljalo o obrani od kibernetičkih prijetnji, pod nazivom „Cyber defence strategies and policies“ (Vuković, 2012: 17).

Zaključno, Republika Hrvatska ne prepoznaje kibernetičku sigurnost kao zasebnu vrstu sigurnosti niti ima najbolju obranu protiv kibernetičkih prijetnji. U hrvatskom zakonodavstvu, kibernetička sigurnost smatra se kao nekom potkategorijom informacijske sigurnosti. Sve važne aktivnosti kibernetičke aktivnosti provode se kroz informacijsku sigurnost, a ono što bi se možda moglo smatrati srodnom pojmu koje hrvatsko zakonodavstvo prepoznaje je pojam informatička sigurnost. No opet postoji ogromna distinkcija između ta dva pojma i stoga se ne može provoditi adekvatna obrana od kibernetičkih prijetnji. Uz to, ogromnu zbrku čini i terminologija riječi cyber. Točnije, u hrvatskoj ne postoji točan prijevod za ovu riječ, pa se akademska zajednica konstantno prepire oko ispravne riječi – je li to kibernetski ili kibernetički. Zbog neslaganja oko tog pojma, mnogo literature i savjeta možda bude i previđeno, pa se zakonodavstvo ni ne koristi savjetima stručnjaka. Još jedan problem je taj da je regija Jugoistočne Europe (pod koju spada i Republika Hrvatska) još uvijek nespremna u potpunosti međusobno surađivati, pa tako nije ni do 2012. bile nekog adekvatnog regionalnog okvira borbe protiv kibernetičkih prijetnji. Osnivanjem RACVAC-a, suradnja se poboljšala, no to i dalje nije dovoljno jer su kibernetičke prijetnje postale sofisticiranije i opasnije. Svijet, pa tako i Republika Hrvatska se još uvijek ponajviše fokusira na onaj tradicionalni pogled na sigurnost, tako da drugi oblici sigurnosti (pogotovo kibernetička) često budu zanemareni.

9.3. Korporativna sigurnost u Republici Hrvatskoj (javno – privatno partnerstvo)

Javno privatno partnerstvo u Republici Hrvatskoj, po pitanju korporativne (i kibernetičke) sigurnosti postoji na određen način, ali nije uspjelo dostići razinu razvoja kao u SAD-u ili u okviru EU. Privatni je sektor, po pitanju sigurnosti, najčešće osuđen sam osmisliti mehanizme obrane, jer država nema dovoljne resurse kako bi se ostvarila sigurnosna suradnja. Uspješnije

hrvatske kompanije prepoznale su potrebu za osnivanjem zasebnog korporativno – sigurnosnog sektora, a u tom su sektoru najčešće zaposleni „bivši policajci, vojnici i sigurnjaci, koji dobrim dijelom znaju opusa sigurnosnih poslova kojima bi se trebala baviti osoba zadužena za poslovnu sigurnost“ (Cvrtila, 2018: 2). No osim tih ljudi, često se javlja i problem nekompetentnosti tog sektora zbog manjka sposobnog i obrazovanog sigurnosnog kadra u Republici Hrvatskoj, s obzirom da se donedavno nije pridavala pažnja ovakvim problemima.

Uz to, pojam poslovne (korporativne) sigurnosti u Hrvatskoj poprilično je nepoznat i nije niti zakonski definiran, osim davanja definicije od strane akademske zajednice gdje (Cvrtila, 2018: 3) poslovnu sigurnost definira kao „skup mjera i radnji koje su poduzete kako bi se osigurale sve vrijednosti pojedinog poslovnog subjekta od uništenja, oštećenja ili otuđenja, eliminacije svih rizika (ili njihovo svođenje na minimalnu razinu) i ugrožavanja koji mogu utjecati na poslovanje tvrtke, te ostvarivanje funkcioniranja tvrtke u uvjetima krize, njezino prevladavanje i ponovna uspostava redovnog poslovanja, a u cilju zadržavanja postojećih i stvaranja novih vrijednosti poslovnog subjekta“.

Zaključno, u hrvatskom pristupu kibernetičkoj sigurnosti kao komponenti korporativne sigurnosti postoji mnogo nedostataka. Prvenstveno, ne pridaje se dosta važnosti opasnostima na internetu, tako da kibernetička sigurnost često sporedna forma sigurnosti. Drugo, što se tiče same korporativne sigurnosti, postoji vrlo malo iskusnog kadra (ljudskih resursa) u ovom sektoru, iako je pozitivno to da su ipak u tom sektoru većinom visokoobrazovani ljudi koji imaju teoretskog znanja o očuvanju sigurnosti. Suradnje privatnog i javnom sektora kao takvoga nema, s obzirom da su i kompanije koje su prepoznale potrebu za ovakvom zaštitom od kibernetičkih napada osnovale svoje sektore korporativne sigurnosti sa svojim kadrovima ljudi. Država u ovom sektoru i dalje dosta malo sudjeluje, tako da je privatni sektor zapravo prepušten samo svojim resursima. Jedina suradnja privatnog i javnog sektora po pitanju korporativne sigurnosti u Hrvatskoj ostvaruje se po pitanju „posuđivanja“ policijskih i vojnih kadrova privatnom sektoru po potrebi.

10. ZAKLJUČAK

Ovim radom prikazuje se važnost postojanja kibernetičke sigurnosti u korporativnom sektoru, tj. korporativnoj sigurnosti. Kibernetičke prijetnje su sveprisutne, a korporativni sektor može zbog toga imati ogromne gubitke – financijske i reputacijske. Kako bi se postigla maksimalna kibernetička sigurnost kao dio korporativne sigurnosti, potrebno je ostvariti suradnju više

aktera, prvenstveno suradnju javnog i privatnog sektora (javno – privatna partnerstva). Rad se kroz poglavlja bavi problematikom kibernetičke sigurnosti i kibernetičkih prijetnji gdje se stavlja naglasak na kibernetičku sigurnost u korporativnom sektoru. Javno – privatna partnerstva po pitanju kibernetičke sigurnosti mogu se vidjeti u demokratskim državama, a najvažnije su Sjedinjene Američke Države i Europska Unija. No ove države imaju drugačiji pristup javno – privatnim partnerstvima i obrani korporativnog sektora od kibernetičkih prijetnji.

Analizom aktivnosti kibernetičke sigurnosti u djelovanju korporativnog sektora protiv kibernetičkih napada može se zaključiti kako su ove dvije vrste sigurnosti – kibernetička sigurnost i korporativna sigurnost međusobno neodvojive. Korporativni sektor danas ovisi o efikasnoj obrani od kibernetičkih napada, a najčešće to može postići postojanjem posebnog sigurnosnog odjela koji se bavi izričito kibernetičkom sigurnosti. Tradicionalna sigurnosna paradigma više ne može u potpunosti odgovoriti na moderna sigurnosna pitanja, već postoji potreba za sigurnosno – informacijskom paradigmom. Tradicionalna (vojna) sigurnost i dalje je snažno prisutna na području međunarodne sigurnosti, posebno sada kada se intenzivira geopolitički sukob Zapada sa Kinom i Rusijom, koji je ponovno potaknuo utrku u konvencionalnom i nuklearnom naoružanju. No danas nije vojna moć jedino što prijeti svjetskoj sigurnosti, već su to i kibernetičke prijetnje.

Kibernetičke prijetnje potražuju nova sigurnosna rješenja kako bi se zaštitili i javni (država) i privatni (u ovom slučaju, korporativni) sektor. Korporativni sektor mora imati visokoobrazovane i iskusne ljude koji se mogu efektivno boriti protiv kibernetičkih prijetnji. Kibernetičke prijetnje danas su postale toliko sofisticirane da postoji snažna potreba za sigurnosnom suradnjom više aktera kako bi se postigla zajednička obrana. Najpouzdaniji primjer borbe protiv kibernetičkih prijetnji udruženjem više aktera je suradnja javnog i privatnog sektora (PPP – *Public private partnership*). Javno – privatno partnerstvo ima veću moć otpora kibernetičkim prijetnjama, a svoju suradnju baziraju na međusobnom povjerenju i praksi lojalnosti. Demokratske države (u ovom slučaju SAD i EU) ističu stratešku korisnost javno – privatnog partnerstva i u tome vide snažan potencijal obrane od kibernetičkih prijetnji. Autoritarne države (Rusija i Kina) nemaju ovakvu vrste suradnje – prvenstveno zbog državne kontrole nad cijelom sferom društva.

Republika Hrvatska još uvijek nema posebno razvijeni sektor kibernetičke sigurnosti, već se kibernetička sigurnost smatra potkategorijom informacijske sigurnosti što nije dovoljno za

adekvatnu obranu od kibernetičkih prijetnji. Postoji snažna potreba za osnivanjem posebnog sektora koji bi se mogao baviti isključivo obranom od kibernetičkih prijetnji. Kibernetičke prijetnje danas snažno zahvaćaju i sektor korporativne sigurnosti u RH, no ni taj sektor se nije u potpunosti spreman boriti protiv njih. Nerazvijenost i kibernetičke i korporativne sigurnosti u Republici Hrvatskoj donosi mnogo problema, a najveći je ugroženost i privatnog i javnog sektora. Postoji potencijal za snažan razvoj oba područja, a upravo to bi se moglo postići suradnjom javnog i privatnog sektora, tj. javno – privatnim partnerstvom.

Korporativna sigurnost danas je u potpunosti ovisna o obrani od kibernetičkih prijetnji. Kibernetička sigurnost kao dio korporativnog sektora neizostavan je dio svake privatne kompanije, a maksimalna sigurnost može se postići suradnjom države i privatnih kompanija. U SAD-u je ovakva vrsta suradnje, javno – privatna partnerstva, široko rasprostranjena i svaka važna kompanija ima odjel korporativne sigurnosti koji je zadužen za obranu od kibernetičkih prijetnji koji surađuje sa državnim institucijama. Zajedničkim snagama državne i korporativne sigurnosti, postiže se bolja kibernetička sigurnost. Europska Unija također vjeruje u ovakvu vrstu suradnje u borbi protiv kibernetičkih prijetnji, ali razlike između privatne i državne sigurnosti su prevelike kako bi se postiglo pravo javno – privatno partnerstvo, iako se i dalje naglašava snažna potreba za tim, čak i u strateškim dokumentima Europske unije.

Kibernetička sigurnost kao komponentna koncepta korporativne sigurnosti danas je jedno od glavnih pitanja kojima se potrebno snažno baviti. Korporativni sigurnosni sektor danas ima ogroman posao obrane od kibernetičkih prijetnji koje su svakim danom sve sofisticiranije. Može se zaključiti da, kako bi se olakšao posao obrane od kibernetičkih prijetnji u korporativnom sektoru, SAD implementira dobru praksu suradnje javnog i privatnog sektora. Javno – privatnim partnerstvom znatno se olakšalo i korporativnom i javnom sektoru u borbi protiv kibernetičkih prijetnji. Zajedničkom inteligencijom oba sektora može se postići efektivna kibernetička sigurnost kao komponenta koncepta korporativne sigurnosti.

11. POPIS LITERATURE

Arbanas, Krunoslav (2021) Radni okvir za procjenu i unapređenje kulture informacijske znanosti. *Distertacija. University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike*, 1 – 316.

Barzilay, M. (2013, 2013-08-05). A simple definition of cybersecurity. Preuzeto sa: http://www.isaca.org/KnowledgeCenter/Blog/Lists/Posts/Post.aspx?ID=29 6

Baylon, C. (2014). Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives. Retrieved from London: http://www.chathamhouse.org/publication /challenges-intersection-cyber-security-andspace-security-country-and-international

Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change*, *67*(3), 265-288.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62.

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor?. *JCMS: Journal of Common Market Studies*, *55*(6), 1254-1272.

Christensen, K. K., & Liebetrau, T. (2019). A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry. *Intelligence and National Security*, *34*(3), 395-408.

Christensen, K. K., & Petersen, K. L. (2017). Public–private partnerships on cyber security: a practice of loyalty. *International Affairs*, Vol. 93; N.6., str. 1435-1452.

Craigen, Dan.; Diakun–Thiabalt, Nadia.; Purse, Randy. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, Vol. 10, No. 4; str. 13 – 21.

Cvrtila, Željko i Stanko, Zoran (2018). Poslovna (korporativna) sigurnost. *Zaštita*, Vol. 7 – 8, str. 14 – 17. Zagreb

Čemerin, V., & Rubić, I. NAZIVLJE PRIVATNE SIGURNOSTI: PROBLEMATIKA DEFINIRANJA POJMA KORPORATIVNE SIGURNOSTI. *Dani kriznog upravljanja Crisis Management Days*, 61.

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5-32.

Dunn, Myriam, C. (2014) Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Sci Eng Ethics,* Vol. 20; str. 701 – 715.

Dunn, Myriam, C. (2015) Cyber-security. *Contemporary Security Studies, 4e*; chapter 27; str. 401 – 415.

Dunn, Myriam C., Mauer, V., & Balzacq, T. (Eds.). (2010). The Routledge handbook of security studies (No. s 56). London: Routledge, 24 – 90.

Dropulić Ružić, M. (2011). KORPORATIVNO UPRAVLJANJE U HOTELSKIM PODUZEĆIMA - SLUČAJ HRVATSKE. *Ekonomska misao i praksa,* 20 (1), 171-201. Preuzeto s https://hrcak.srce.hr/69710

Eichensehr, K. E. (2016). Public-private cybersecurity. *Tex. L. Rev.*, *95*, 467.

Giles, K., & Hagestad, W. (2013, 4-7 June 2013). Divided by a common language: Cyber definitions in Chinese, Russian and English. Paper presented at the Cyber Conflict (CyCon), 2013 5th International Conference on.

Government of Montenegro. (2013). National Cyber Security Strategy for Montenegro 2013-2017. Podgorica Retrieved from http://www.mid.gov.me/ResourceManager /FileDownload.aspx?rid=165416&rType=2 &file=Cyber%20Security%20Strategy%20for%20Montenegro.pdf

Hansen, Lene.; Nissenbaum, Helen. (2009) Digital disaster, cyber security, and the Copenhagen school. *Internation studies quarterly*. Vol. 53, str. 1155 – 1175.

Harknett, R. J., & Stever, J. A. (2009). The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. *Journal of Homeland Security and Emergency Management*, *6*(1).

https://urn.nsk.hr/urn:nbn:hr:211:439511 pristupljeno 4. svibnja 2022

ISACA. (2014). European Cybersecurity Implementation: Overview. Retrieved from Rolling Meadows: http://www.isaca.org/KnowledgeCenter/Research/ResearchDeliverables/Pages/European-CybersecurityImplementation-Series.aspx

J. Kwon, J. R. Ulmer, i T. Wang (2013) "The Association between Top Management Involvement and Compensation and Information Security Breaches," J. Inf. Syst., vol. 27, no. 1, pp. 219–236.

Karlsen, G. H. (2019). Divide and rule: ten lessons about Russian political influence activities in Europe. *Palgrave Communications*, *5*(1), 1-14.

Kelly, B. B. (2012). Investing in a centralized cybersecurity infrastructure: Why hacktivism can and should influence cybersecurity reform. *BUL Rev.*, *92*, 1663.

Knight, Richard.; Nurse, Jason, R.C. (2020) A Framework for Effective Corporate Communication after Cyber Security Incidents. *Computers and security journal.*

Luiijf, E., Besseling, K., & de Graaf, P. (2013). Nineteen national cyber security strategies. International Journal of Critical Infrastructures, 9(1), 3-31. doi:10.1504/IJCIS.2013.051608

Mayer, M., Martino, L., Mazurier, P., & Tzvetkova, G. (2014). How would you define Cyberspace. *First Draft Pisa*, *19*, 2014.

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, *35*(6), 105336.

Min, K. S., Chai, S. W., & Han, M. (2015). An international comparative study on cyber security strategy. *International Journal of Security and Its Applications*, *9*(2), 13-20.

Muhirwe, Jackson.; White, Nathan. (2016) Cybersecurity awareness and practice of next generation corporate technology users. *Issues in Information Systems*, Vol. 17. No. 2; str. 183 – 192.

Nye, J. S. (2011). Nuclear lessons for cyber security?. *Strategic Studies Quarterly*, *5*(4), 18-38.

Panagopoulos, A. (2020). USA, EU and China as the Leading Actor in the World Trade and Cybersecurity, Divergences and Convergences.

Pernik, P. (2014). Improving cyber security: NATO and the EU. *International Centre for Defense Studies*.

Piggin, Richard (2016) Cyber security trends: What should keep CEOs awake at night. *International Journal of Critical Infrastructure Protection.* Vol. February (002).

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the cyber security body of knowledge. *IEEE Security & Privacy, pristupljeno 15.02.2022* https://www.cybok.org/

Rauscher i Yaschenko (2011): 31). – 19 cyber tech strategies… Rauscher, K.F. and Yashenko, V. (Eds.) (2011) Critical Technology Foundations, EastWest Institute, London, available at http://www.ewi.info/system/files/reports/RussiaU%20S%20%20bilateral%20on%20terminology%20v76%20%282%29.pdf (pristupljeno 5. svibnja, 2022).

Schatz, Daniel.; Bashroush, Rabih.; Wall, Julie. (2017) Toward a more representative definition of cyber security. *The journal of digital forenscics, security and law.* Vol. 12, No. 2.

Shafquat, Narmeen.; Masood, Ashraf. (2016). Comparative Analysis of Various National Cyber Security Strategies. *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 14, No. 1, str. 129 – 136.

Štitilis, D., Pakutinskas, P., & Malinauskaitė, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security Journal*, *30*(4), 1151-1168.

Stubley, D. (2013, 2013-06-07). What is Cyber Security? Retrieved from https://www.7elements.co.uk/resources/blo g/what-is-cyber-security/

Trivan, Dragan (2018) Contemporaty concept of corporate security. *Faculty of Business Studies and Law, University „Union-Nikola Tesla" of Belgrade Austrian Institute for European and Security Policy/AIES Wien Institute for Corporative Security Studies, ICS, Ljubljana*. Beograd, 1 – 348.

Van Puyvelde, Damien & Brantly, Aaron F. (2019) Politics, governance and conflict in cyberspace. *Polity Press,* Cambridge (1 – 212).

Von Solms B. i Von Solms R. (2004) "The 10 deadly sins of information security management," Comput. Secur., vol. 23, no. 5, pp. 371–376.

Walls, A., Perkins, E., & Weiss, J. (2013). Definition: Cybersecurity, 5. Retrieved from Gartner.com website: https://www.gartner.com/doc/2510116/def inition-cybersecurity

Warner, M. (2012). Cybersecurity: A pre-history. *Intelligence and National Security*, *27*(5), 781-799.

Weiss, S., Indurkhya, N., Zhang, T., & Damerau, F. (2004). Text Mining: Predictive Methods for Analyzing Unstructured Information: SpringerVerlag.

POPIS ILUSTRACIJA:

12. SAŽETAK I KLJUČNE RIJEČI

SAŽETAK

Korporativna sigurnost mora se konstantno boriti protiv kibernetičkih prijetnji. Kibernetičke prijetnje izazvale su potrebu za osnivanjem posebnog odjela korporativne sigurnosti koji se izričito bavi kibernetičkom sigurnosti. Poslovanje nekog poduzeća može biti narušeno ili čak i u potpunosti uništeno zbog kibernetičkih napada. Često su ti kibernetički napadi toliko sofisticirani i inovativni da se nemoguće samostalno boriti protiv njih. Potrebna je suradnja odjela korporativne sigurnosti sa državnim institucijama kako bi se moglo efikasnije boriti protiv kibernetičkih prijetnji. Javno – privatna partnerstva po pitanju kibernetičke sigurnosti jedan su od najefikasnijih načina borbe protiv kibernetičkih zločina. Korporativna sigurnost danas u potpunosti ovisi dobroj implementaciji kibernetičke sigurnosti, visokoobrazovanom kadru koji može pravovremeno prepoznati kibernetičku prijetnju i o dobroj sigurnosnoj praksi svojih zaposlenika. Krajnji cilj kibernetičkoj sigurnosti kao komponenti korporativne sigurnosti jest osigurati efikasnu sigurnosnu praksu u borbi protiv kibernetičkih prijetnji.

Ključne riječi: **kibernetička sigurnost, korporativna sigurnost, javno – privatno partnerstvo, kibernetičke prijetnje, hakiranje, kibernetički rat**

RESUME

Corporate security is forced to constantly fight against cyber threats. Cyber threats called for a need to establish a special department of corporate security which would deal with cyber threats only. Business activity can be partly compromised or even fully destroyed because of cyber-attacks. Those cyber-attacks are often so sophisticated and innovative that it's almost impossible to fight against them. So, there is a need for a cooperation between corporate

security department and public institutions for a better and more effective fight against cyber threats. Public – private partnerships considering cyber security are one of the most effective ways of fighting against cybercrimes. Corporate security, today, is fully dependent on good implementation of cyber security, highly educated people who can recognize cyber threats in time and of a good practice of its employees. Final goal of cyber security as a component of corporate security is to ensure that there is a good and effective security practice in fighting against cyber threats.

Key words: **cyber security, corporate security, public – private partnership, cyber threats, hacking, cyber war**