Kibernetička sigurnost

Szombathelyi, Donata

Sveučilište Josipa Jurja Strossmayera u Osijeku

Filozofski fakultet Osijek

Preddiplomski studij informatologije

Donata Szombathelyi

Kibernetička sigurnost

Završni rad

Mentorica: izv. prof. dr. sc. Anita Papić

Osijek, 2021.

Sveučilište Josipa Jurja Strossmayera u Osijeku

Filozofski fakultet Osijek

Odsjek za informacijske znanosti

Preddiplomski studij informatologije

Donata Szombathelyi

Kibernetička sigurnost

Završni rad

Društvene znanosti, informacijske i komunikacijske znanosti,
informacijski sustavi i informatologija

Mentorica: izv. prof. dr. sc. Anita Papić

Osijek, 2021.

IZJAVA

Izjavljujem s punom materijalnom i moralnom odgovornošću da sam ovaj rad samostalno napravila te da u njemu nema kopiranih ili prepisanih dijelova teksta tuđih radova, a da nisu označeni kao citati s napisanim izvorom odakle su preneseni.
Svojim vlastoručnim potpisom potvrđujem da sam suglasan da Filozofski fakultet Osijek trajno pohrani i javno objavi ovaj moj rad u internetskoj bazi završnih i diplomskih radova knjižnice Filozofskog fakulteta Osijek, knjižnice Sveučilišta Josipa Jurja Strossmayera u Osijeku i Nacionalne i sveučilišne knjižnice u Zagrebu.

U Osijeku, 2. rujna, 2021.

Dvataj., 0122225600

ime i prezime studenta, JMBAG

SAŽETAK

Računalni su sustavi danas postali velika meta napadačima, a dobro je poznato da su informacije imovina koja ima vrijednost poput bilo koje druge imovine. Kibernetička sigurnost zato danas postaje važno područje dok osiguravanje i očuvanje podataka o pojedincu i organizaciji postaju veliki izazovi u današnjem društvu. Cilj ovoga rada je prije svega objasniti važnost kibernetičke sigurnosti i ukazati na probleme s kojima se suočava kibernetička sigurnost. Iako većina korisnika računalnih sustava nije svjesna rizika, razvijanje svijesti o važnosti kibernetičke sigurnosti je od izrazitog značaja kao i pravovremeno reagiranje u trenutku napada. U radu se nastoji objasniti provođenje politike kibernetičke sigurnosti u vidu smjernica za održavanje i upravljanje tehnologijom primjerice putem Nacionalne strategije o kibernetičkoj sigurnosti. Nadalje, navode se i objašnjavaju osnovni koncepti kibernetičke sigurnosti kao što su autorizacija i autentičnost te se naglašava uloga kibernetičke sigurnosti u obrazovnom sustavu. Također, u radu se približavaju glavni izazovi kibernetičke sigurnosti kao što je primjerice kibernetički terorizam, ali i trendovi u razvoju kibernetičke sigurnosti kao npr. razvijanje kibernetičkoga imuniteta.

Ključne riječi:

kibernetička sigurnost, kibernetički terorizam, kibernetički imunitet

SADRŽAJ

1. UVOD

Kibernetika općenito je znanost o teoriji upravljanja, a za njezin razvoj zaslužan je američki matematičar Norbert Wiener. U ovom radu se kibernetička sigurnost stavlja u međuodnos s ostalim vrstama sigurnosti kao što su informacijska sigurnost, mrežna sigurnost, aplikacijska sigurnost te internet sigurnost. S obzirom na današnju umreženost društva svaka država bi trebala provoditi određene strategije u borbi protiv kibernetičkih napada i osvješćivati svoje građane o važnosti kibernetičke sigurnosti. U radu se opisuju dobro uređene politike kibernetičke sigurnosti u Kini i SAD-u i to kroz sljedeće četiri domene upravljanja: zakoni i propisi, politika poduzeća, tehnološke operacije te konfiguracija tehnologije. Nadalje, rad opisuje temeljne koncepte kibernetičke sigurnosti kao što su autentičnost, autorizacija i neprihvaćanje. Također, naglasak u radu stavlja se na povjerljivost podataka, njihovom integritetu i dostupnosti te važnosti kibernetičke sigurnosti u obrazovnom sustavu. Naime, svjedoci smo učestalih hakerskih napada na sveučilišne ili fakultetske mrežne sustave čime intelektualno vlasništvo fakulteta dolazi u opasnost, a samim time i osobni podaci studenata i nastavnog osoblja. S obzirom na tu činjenicu, velik broj znanstvenika predviđa nastanak kibernetičkog ratovanja i kibernetičkog terorizma u budućnosti. Kibernetički napadi koji se dogode u pojedinim državama zahtijevaju određene globalne odgovore koji su zasnovani na regionalnim sporazumima. Nadalje, u radu se podastiru i statistički podaci vezano uz raspodjelu meta i kibernetičkih napada u 2020. godini. Na kraju rada u okviru poglavlja o budućnosti kibernetičke sigurnosti opisuje se The Cyber 2025 Model i otkriva se što će sve donijeti snaga tehnoloških promjena te koga će sve zahvatiti i na što će sve utjecati. Također, opisuje se kibernetički imunitet te njegova funkcija, koja se vrlo dobro može usporediti i s imunološkim sustavom čovjeka, kao i princip rada tzv. Cyber Protect-a, poznatog programa čija je zadaća provjeravanje, odnosno nadziranje bilo kakvih sumnjivih aplikacija i njihovih korisnika.

2. KIBERNETIČKA SIGURNOST

Kibernetika se definira kao skup znanstvenih disciplina i postupaka koji se implementiraju pri upravljanju i vođenju složenih sustava.[1] Danas se često pridjev kibernetički koristi kao istoznačnica s pridjevom *cyber*, no pridjev ipak nije u potpunosti točan jer *cyber* podrazumijeva svijet koji nastaje uz pomoć računala. Osim toga, korijeni kibernetike sežu iz stare Grčke pa tako riječ κυβερναώ označava upravljati, kormilariti. S obzirom da je kibernetika novija znanost, ona je interdisciplinarne prirode.[2] Danas se temelji na zajedničkim odnosima ljudi i strojeva – koristi se u teoriji upravljanja, teoriji automatizacije i računalnim programima za smanjenje mnogih dugotrajnih izračuna i procesa donošenja odluka koje su prije radili ljudi. Norbert Wiener definira kibernetiku kao znanost o vezi, upravljanju i kontroli nad strojevima i živim bićima, odnosno disciplinu koja proučava strukturu živih i neživih regulacijskih sustava te upravljanje njima. Prema tome, stvorio je opće okvire za jedinstvenu teoriju koja obuhvaća ponašanje ljudskih bića i strojeva.[3] Kasnije je taj sustav prozvan kibernetičkim sustavom. Zamišljeni sustav ima tri cjeline, odnosno podsustave[4]. Prvi je podsustav osjetila koji je zadužen za prikupljaje svih potrebnih informacija o trenutačnom stanju sustava, dok je drugi podsustav u kojem se iz prikupljenih informacija uspoređuje trenutno stanje s ciljanim stanjem i na taj se način jasno utvrđuje razlika. Zadnji, odnosno treći podsustav je taj koji utječe na ponašanje sustava tako što smanjuje određene razlike. Ovime se ostvaruje tzv. povratna veza koju je najbolje objasniti na sljedeći način. Na primjer, u procesu[5] dohvaćanja određenog predmeta postoji povratna veza koja može obuhvaćati vid, misaoni proces u mozgu, ali i poticaj mišićima koji pokreću šaku prema predmetu. Povratna će se veza odmah prekinuti zatvarenjem očiju pa će sam postupak dohvaćanja predmeta biti otežan. Pretvorba i stvaranje informacija temeljni su preduvjet djelovanja takvih sustava, pa se sastavnim dijelom kibernetike smatra i teorija informacija. S vremenom se pokazalo da je ova prvotna zamisao o teoriji upravljanja i vođenja bila previše

[1] Usp. Kibernetika. // Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2020. URL: https://enciklopedija.hr/natuknica.aspx?id=31381 (2020-08-15)
[2] Usp. Vuković, Hrvoje. Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj. National security and the future, vol. 13, br. 3, 2012. Str.15. URL: https://hrcak.srce.hr/100728 (2020-08-15)
[3] Usp. Kibernetika. Nav. dj.
[4] Isto.
[5] Isto.

samouvjerena, no za taj su problem danas zaslužne odgovarajuće znanstvene discipline.[6] Dok se one žele orientirati na primjenu informacijsko komunikacijskih tehnologija (dalje u tekstu: IKT), kibernetika se uglavnom koristi u svrhe komparativnih studija, točnije ljudskoga živčanoga sustava i artefakata IKT-a. Osim ovog povijesnog dijela, potrebno je objasniti i određenu terminologiju vezanu uz sigurnost općenito. Međunarodna Telekomunikacijska Unija (ITU) određuje kibernetičku sigurnost kao zbirku alata, politika, akcija, obuka, najboljih praksi, sigurnosnih koncepata, sigurnosnih zaštitnih mjera, smjernica, pristupa upravljanju rizicima, osiguranja i tehnologija koje se mogu koristiti kako bi zaštitili cyber okruženja, organizacijsku i korisničku imovinu.[7] Ova se sigurnost posebno usredotočuje na podatke u digitalnom obliku, a to su mobilni uređaji, tableti, računala, poslužitelji mreže i slično. ITU također naglašava kako su cyber prijetnje jedan od velikih problema današnjice pa je upravo zbog toga za uspješno provođenje ovakve sigurnosti potrebna dobra međunarodna koordinacija i snalaženje u tzv. *cyberspace-u* tj. kibernetičkom prostoru, odnosno računalnoj simuliranoj stvarnosti koja je zasnovana na IKT-u. Uz kopno, more i zrak, smatra se četvrtom domenom ljudskog djelovanja. Ovaj je prostor u uskoj vezi sa *cyberpunkom* - znanstvenofantastičnim podžanrom kojeg je smislio Bruce Bethke, a karakteriziraju ga protukulturni pojedinci zarobljeni u visokotehnološkoj budućnosti. Prema tome, kako bi provođenje kibernetičke sigurnosti bilo uspješno, usporedno moraju sudjelovati i druge vrste[8] sigurnosti - informacijska sigurnost, aplikacijska sigurnost, mrežna sigurnost te internet sigurnost.

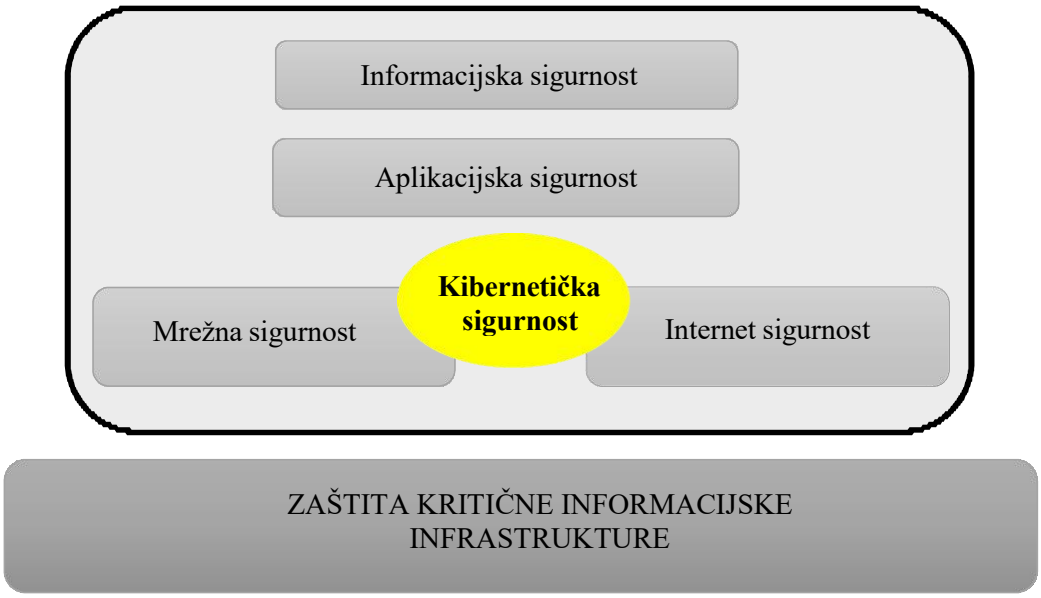
Informacijska sigurnost ima za cilj zaštititi privatnost korisnika te osigurati trajnost i dostupnost informacija. Iako se danas često vode kao sinonimi, informacijsku sigurnost treba razlikovati od kibernetičke (Slika 1.) po tome što je kibernetička sigurnost skup praksi koje se koriste za pružanje sigurnosti od internetskih napada, dok je informacijska sigurnost samo poddisciplina kibernetičke sigurnosti. S druge strane, aplikacijska sigurnost predstavlja proces koji se obavlja kako bi se primijenile

[6] Isto.

[7] Usp. Hamidović, Haris. Mjesto i uloga cyber sigurnosti u razvoju modernih društava. // Sarajevski žurnal za društvena pitanja, vol 4, 1-2(2015). Str. 82. URL: https://www.researchgate.net/publication/302901758_Mjesto_i_uloga_cyber_sigurnosti_u_razvoju_modernih_drustava (2020-08-15)

[8] Usp. Isto. Str. 83.

odgovarajuće kontrole i mjerenja na organizacijske aplikacije.[9] Zadaća mrežne sigurnosti je da dizajnira, implementira i radi na mrežama, a internetske sigurnosti da zaštiti internetski povezane usluge. Ona se sastoji od niza sigurnosnih taktika za zaštitu aktivnosti i transakcija koje se vrše putem interneta te su namijenjene zaštiti korisnika od prijetnji, poput provala u računalne sustave, adrese e-pošte ili mrežne stranice.[10]



Slika 1. Međuodnos kibernetičke sigurnosti i ostalih vrsta sigurnosti

2.1. Važnost kibernetičke sigurnosti

Premda se internet nekima čini sigurnim sučeljem, svakodnevno se događa veliki broj napada, kako na pametnim telefonima, tako i na laptopima i tabletima. Većinu ljudi ne zabrinjava činjenica o tome kako se broj kibernetičkih napada iz dana u dan povećava, a samim time se povećava i važnost kibernetičke sigurnosti. Svijest o kibernetičkoj sigurnosti predstavlja kombinaciju poznavanja i poduzimanja nečega radi zaštite informacijske imovine organizacije ili tvrtke. Međutim, stvaranjem kulture o važnosti kibernetičke sigurnosti ne znači da će se u potpunosti iskorijeniti rizik kibernetičkog

[9] Usp. Isto. Str. 84.
[10] Isto.

kriminala.[11] Primjerice, kada su zaposlenici poduzeća svjesni kibernetičke sigurnosti to znači da razumiju što su kibernetičke prijetnje, potencijalni utjecaj kibernetičkih napada na njihovo poslovanje, ali i koraci koji su potrebni za smanjenje rizika i sprječavanje kibernetičkog kriminala koji predstavlja rizik u njihovom mrežnom radnom prostoru.[12]

Današnje moderno društvo ovisi o tehnologijama i svi problemi koji se dogode u kibernetičkom prostoru, utječe na sve segmente društva, a društvo mora biti svjesno toga. Kibernetički ratovi (engl. *cyber wars*) traju već niz godina, a interes za probleme koji oni donose često je usredotočen samo na incidente koje oni mogu prouzrokovati i na to kako se s njima boriti, dok se zabrinutost, prevencija i ulaganje u bolju kibernetičku sigurnost zapravo zapostavlja, stoga se u ovom radu pokušava dati odgovor na pitanje zašto je tako malo razvijena svijest o važnosti kibernetičke sigurnosti i zašto se ne poduzimaju određene mjere. Postoje određeni paradoksi[13] koji najbolje objašnjavaju razvijanju svijesti o važnosti kibernetičke sigurnosti. Oni su uglavnom u uskom dodiru s politikom. Naime, vlada je ta koja treba pratiti korisničke potrebe, no problem je taj što ona zahtjeva da se sav postupak provođenja kibernetičke sigurnosti provodi u svrhu nadzora, pritom još zahtijevajući pristup korisničkim podacima, bilo da su u pitanju pojedinci ili organizacije. Drugi paradoks objašnjava kako vlada želi pomoć i zaštitu od vodećih tvrtki, no isto tako ne želi nikakve postupke enkripcije podataka, niti bilo što drugo vezano uz kriptografiju.[14] Osim toga, ova problematika zahtjeva suradnju i drugih država, najčešće susjednih, kako bi se riješile prijetnje i sukobi u kibernetičkom prostoru.

2.2. Politike i nacionalne strategije kibernetičke sigurnosti

Riječ *politika* općenito se primjenjuje u raznim situacijama koje se tiču kibernetičke sigurnosti. Inače podrazumijeva korištenje smjernica koje su namijenjene održavanju same kibernetičke sigurnosti - ona poziva na zakone i propise koji se odnose na distribuciju informacija, kao i za zaštitu informacija te računalne metode upravljanja

[11] Usp. The Importance Of Cyber Security Awareness. URL: https://www.ogl.co.uk/the-importance-of-cyber-security-awareness (2020-08-25)
[12] Usp. Isto.
[13] Usp. Bruijn de Hans; Janssen, Marijn. Building Cybersecurity Awareness: The need for evidence-based framing strategies. Government Information Quarterly, 2017. Str. 2. URL: https://www.sciencedirect.com/science/article/pii/S0740624X17300540 (2020-08-25)
[14] Usp. Isto.

tehnologijom.[15] Nadalje, politika kibernetičke sigurnosti država trenutno se smatra podskupom politike nacionalne sigurnosti. Premda se politika kibernetičke sigurnosti država i vanjska politika znaju nalaziti u "istoj ravnini", te politike nikako nemaju jednaku snagu kao zakon. Ovakva vrsta politike sadrži četiri tzv. domene upravljanja - *zakone i propise*, *politiku poduzeća*, *tehnološke operacije* te *konfiguracije tehnologije*. Svaka od ovih domena je sigurnosna politika koja se posebno primjenjuje na određenu domenu ili skup računala u danom sustavu. Zakoni i propisi moraju biti u skladu s odgovarajućim opsegom, kao i sve ostale domene i njihova je misija da mudro i promišljeno odražavaju koncipiranu kibernetičku politiku. Ovakvi su propisi primjerice jasno vidljivi u Kini i u SAD-u[16]. Kina je s jedne strane, zorno prikazala i uspostavila svoju kibernetičku politiku tako što je odlučila kontrolirati svaku aktivnost u kibernetičkom prostoru koja predstavlja rizik za državu, a samim time je i stvorila utisak kako internet služi samo interesima države. U SAD-u, s druge strane, politiku kibernetičke sigurnosti uključuju strategije, politike i standardi koji su u vezi sa sigurnošću i operacijama u kibernetičkom prostoru. Ona kao takva pokriva cijeli niz prijetnji, međunarodni angažman, računalnu mrežu, osiguravanje informacija te obavještavanje koje se odnose na sigurnost te stabilnost globalne informacijske i komunikacijske infrastrukture. Politika poduzeća, kao druga domena, nema toliko jaku politiku u sebi kao što je politika primjerice neke više institucije. Ona se može odnositi na procjenu informacijskog rizika u određenoj tvrtki u kojoj svaki pojedinac višeg stupnja zaposlenja ima mogućnost utvrđivanja sankcija onima nižeg stupnja zaposlenja. Nadalje, kao treća domena izdvajaju se tehnološke operacije koje su ključne u radu pravnih i računovodstvenih znanosti koje na bilo koji način imaju doticaj sa zaštitom podataka, informacijama i telekomunikacijama. Povrh toga, koriste se i standardi (primjerice NIST - National Institute of Standards and Technology). Zadnja, četvrta domena, opisuje tehnološku konfiguraciju.[17] Konfiguracije se odnose na tehničko uređivanje sustava kojeg provode administratori uz odgovarajuće softvere. Glavni aspekt ove domene jest obostrano udovoljavanje, kako korisnicima, tako i davateljima usluga. Strategija poput *Nacionalna strategija kibernetičke sigurnosti* ima primarni cilj uspostaviti ispravnu, odnosno racionalnu koordinaciju različitih

[15] Usp. Bayuk, L. Jennifer et al. Cyber Security Policy Guidebook. Wiley, 2012. Str. 4. URL: https://www.programmer-books.com/wp-content/uploads/2018/07/Cyber-Security-Policy-Guidebook-1st-Edition-2012.pdf (2020-08-27)
[16] Isto. Str. 8.
[17] Isto. Str. 10.

institucija kako bi uspješno odgovorile na prijetnje u kibernetičkom prostoru. Naime, treba imati na umu da stvaranjem bilo kakvih strategija ne mogu najedanput nestati svi problemi koji se odnose na računalne sustave i komunikaciju u kibernetičkom prostoru. Ona je samo prvotna zamisao kako bi se poboljšalo trenutno stanje komunikacije i kibernetičke sigurnosti općenito. Osim toga, svrha je takve strategije i zaštititi sve korisnike modernih elektroničkih usluga, kako u javnom, tako i u gospodarskom sektoru.[18] Na taj bi se način više razvijala svijest o važnosti kibernetičke sigurnosti te mehanizam razmjene i pristupa podataka. Poticao bi se razvoj usklađenih obrazovnih programa u školama, visokim učilištima povezivanjem akademskog, javnog i gospodarskog sektora.[19] Nadalje, svaki kibernetički prostor da bi bio jasno prikazan, osmišljen i siguran za korištenje, trebao bi imati prije svega odlučne i zainteresirane sudionike. Svi sudionici moraju zauzeti određene stavove poduzimanja mjera iz svoje nadležnosti, surađivati s drugima, ali se i prilagoditi kad situacija to zahtjeva. Integracijom svih segmenata društva (različiti sektori) i koordinacijom različitih institucija moguće je ostvarivanje procesa kibernetičke sigurnosti u određenoj situaciji.

2.3. Osnovni koncepti kibernetičke sigurnosti

Koncepti kao što su *autentičnost*, *autorizacija* i *odbijanje* nužni su cyber stručnjacima za implementaciju, dizajn i sigurnost određenih sustava. Uz njih, postoje još tri dodatna koncepta, koja su poznata kao CIA-ina trijada - *confidentiallity* (povjerljivost), *integrity* (integritet) i *availabilty* (dostupnost). Ovoga se svi stručnjaci moraju pridržavati kako bi se uspješno provodila koordinacija kibernetičke sigurnosti zato što svaki od ovih koncepata djeluje poput stupa koji drži sigurnost sustava.[20] Ako napadač prekrši bilo koji stup, sigurnost sustava će pasti. *Autentičnost*, prije svega, predstavlja ključ svakog sigurnosnog sustava kod procesa primanja informacija. Ona govori o vjerodostojnosti informacija, a National Information Assurance Glossary (NIAG) ju definira kao sigurnosnu mjeru koja je namijenjena utvrđivanju

[18] Usp. Nacionalna strategija kibernetičke sigurnosti. Zagreb, 2015. Str. 20. URL: https://www.uvns.hr/UserDocsImages/dokumenti/Nacionalna%20strategija%20kibernetic ke%20sigurnosti%20(2015.).pdf (2020-08-30)
[19] Isto.
[20] Usp. Graham, James et al. Cyber Security Essentials. New York: Auerbach Publications. Str. 1.URL: http://www.bandido.ch/programming/Cyber_Security_Essentials.pdf (2020-08-30)

valjanosti prijenosa poruka.[21] Prema tome, da bi sustav proveo ispravnu autentičnost osobe, potrebno je postaviti osobi određena pitanja, na koju samo ta osoba zna odgovor - primjerice, zaporka bankovnog računa. Drugim riječima isto se naziva faktor autentičnosti[22]. Međutim, kad sustav provjere autentičnosti zahtijeva više od jednog od ovih čimbenika, zajednica sigurnosti ga klasificira kao sustav koji zahtijeva višefaznu provjeru autentičnosti. Nadalje, autentičnost se može odnositi i na provjeru izvora poruke. S obzirom da se sustavi za provjeru autentičnosti poruka uglavnom oslanjaju na kriptografske potpise, takvi se sastoje od skupa poruka generirane tajnim ključem. U tom slučaju samo jedna osoba ima pristup i primatelj može potvrditi identitet pošiljatelja. *Autorizacija* se za razliku od autentičnosti nastoji usredotočiti na dopuštenja, odnosno sve privilegije koje može imati korisnik. Sigurnosni sustav uvijek nakon procesa autentičnosti mora odrediti i privilegije korisnika - primjerice online bankarstvo. Sustav će uvijek identificirati korisnika te na temelju njegovih vjerodajnica (npr. OIB-a) omogućiti mu pristup, npr. uvid u stanje računa.[23] Nadalje, treći koncept bilo bi *odbacivanje* ili *neprihvaćanje* **-** jamstvo da korisnik ne može poreći valjanost, podrijetlo ili cjelovitost nečega, bio to običan podatak ili mnoštvo informacija. Opisuje se kao pravni pojam koji se opsežno koristi u kibernetičkoj i informacijskoj sigurnosti. Što se tiče *povjerljivosti* podataka, ona jasno ukazuje na to da se informacije nipošto ne bi trebale objavljivati nepoznatim i neovlaštenim autorima, procesima i uređajima. Njezin je fokus na zaštiti i prikrivanju informacija, stoga uvijek moraju postojati ograničenja čiji je cilj smanjivati pristup informacijama, osim onima kojima je dopušten pregled.[24] Primjer za to može biti povjerljiva e-poruka koju je poslao korisnik A korisniku B, ali kojem korisnik C pristupa bez odobrenja ili znanja korisnika A i B. Kako bi podaci bili na što sigurnijem mjestu, postoje određene privatne mreže (npr. VPN - Virtual Private Network) i lokacije koje štite podatke. Na taj način sustav šalje podatke putem javnih mreža, gdje organizacije koriste ključ kojeg odobravaju samo određene skupine kako bi se uspostavila *enkripcija* (šifriranje) podataka. Što se tiče *integriteta* podataka, on predstavlja logičku cjelovitost hardvera i softvera koji implementiraju mehanizme zaštite, tj. dosljednost strukture podataka. Štoviše, ovakvo djelovanje može dovesti do raznih kvarova softvera što može prouzrokovati gubitak cjelovitosti podataka, pa samim time

[21] Isto.
[22] Isto. Str. 2.
[23] Isto. Str. 3.
[24] Isto. Str. 4.

sustav može lako postati meta neovlaštenog korištenja od strane cyber napadača. Prema tome, dovoljna je samo mala "ranjivost" ili "rupa", da bi se uspostavila izmjena u sustavu - primjerice pisanje ili brisanje koda u bazama podataka.[25] U konačnici, važna je i *dostupnost* sustava, što označava da je nešto pouzdano i pravovremeno. Bez dostupnosti nema usluga koje korisnicima trebaju, što znači da sustav neće biti od nikakve koristi. Samim time se olakšava napadačima da iskoriste sustav i onemoguće pristup. Najpoznatiji napad na dostupnost je upravo uskraćivanje usluge (DoS - Denial of Service Attack). DoS može imati više oblika, ali najčešći je *flooding* (poplava). Događa se kada napadnuti sustav preplavi velika količina prometa s kojim se poslužitelj ne može nositi pa se sustav s vremenom zaustavlja. Drugi oblik je primjerice napad koji rezultira *rušenjem sustava*. Oni se događaju rjeđe, kada cyber kriminalci prenose bugove koji iskorištavaju nedostatke ciljanog sustava. Ovakvi napadi sprječavaju legitimne korisnike da pristupe mrežnim uslugama poput web stranica, e-pošte ili npr. uslugama bankovnih računa.

2.4. Uloga kibernetičke sigurnosti u obrazovnom sustavu

Razvoj informacijskih tehnologija donio je za sobom određene promjene, a te su promjene vidljive na obrazovnim sustavima. Kibernetički napadi koji se dogode na softverima obrazovnih sustava ne ugrožavaju samo sigurnost intelektualnog vlasništva škola/fakulteta, već i osobnih podataka njezinih učenika/studenata. Budući da sveučilišta moraju imati otvorenu mrežu za pristup svojim studentima i osoblju, hakeri tada imaju više prostora, tj. mogućnosti za ulazak u sustav. Upravo zbog toga, sveučilišta moraju poduzeti određene mjere kako bi spriječili napade, korištenjem softvera za otkrivanje prijetnji i drugih nadogradnji sustava.[26] Podaci koji se nalaze u računalima, kao što su popisi studenata mogu postati savršena meta napadačima, a kompleksnije mreže sustava mogu se hakirati putem neželjenih pošta. Naime, općepoznata je činjenica kako fakulteti i visoka učilišta imaju vrlo složenu, ali nažalost nedovoljno zaštićenu mrežu.

[25] Isto. Str. 5.
[26] Usp. Why Is Higher Education the Target for Cyber Attacks? URL: https://www.blackstratus.com/why-is-higher-education-the-target-for-cyber-attacks/ (2020-08-30)

U sustave je moguće prijaviti se i preko mobilnih telefona, pa su one ujedno i najmanje siguran pristup, no i da se svi korisnici prijave na računala koja su sigurna, i dalje bi se njihova mreža suočavala s prijetnjama kibernetičke sigurnosti.[27] Nadalje, za informacijske je stručnjake oduvijek bilo dosta teško provođenje kontrole i ažuriranje softvera, isto kao i očuvanje i zaštita osobnih podataka. Zbog toga je bitno pratiti i reagirati na sve kibernetičke napade te osigurati prevenciju koliko god je to moguće. Osim nedovoljno zaštićenih mreža, drugi problem predstavljaju vrlo slabe lozinke, ali i previše korisnika s istovremenom prijavom. Iz tog se razloga zahtjeva od korisnika (studenti, nastavnici i ostalo osoblje) da imaju jače lozinke, da ažuriraju postojeće e-mail adrese te da se više educiraju o zaštiti sustava kako ne bi bili napadnuti.[28]

2.5. Izazovi kibernetičke sigurnosti

Broj kibernetičkih napada neprestano raste i mnogi znanstvenici predviđaju vjerojatnost katastrofalnog kibernetičkog ratovanja (eng. *cyber warfare*) u bliskoj budućnosti. Neprestano se pokušavaju riješiti dva najveća problema u mrežnom prostoru, a to su ogromna količina mrežnih kretanja te poteškoće u otkrivanju obrazaca o mrežnom prometu.[29] Kao jedan od najvećih izazova koji ne poznaje granice manifestira se kibernetički terorizam (eng. *cyber terorrism*). Odvija se u kibernetičkom prostoru te pripada podvrsti terorizma koji koristi informatiku kao svoje oružje u svrhu postizanja terorističkog cilja. Između ostalog, ovakav tip terorizma uključuje fizičko uništavanje nekog uređaja, sustava uređaja ili određenog procesa u kojoj sudjeluje informatička komponenta s ciljem remećenja i uništavanja.
Ovakvi zločini sve više privlače teroriste zato što zahtijevaju puno manje resursa i zbog toga što se omogućuje ljudska odsutnost od lokacije napada, a osim toga nudi mogućnost da napadači ostanu anonimni, odnosno nepoznati.[30]

---

[27] Isto.
28 Isto.
[29] Usp. Wlodarczak, Peter. Cyber Immunity - A Bio-Inspired Cyber Defense System. University of Southern Queensland: Australia, 2017. Str. 206. URL: https://www.researchgate.net/publication/315861769_Cyber_Immunity_-_A_Bio-Inspired_Cyber_Defense_System (2020-08-30)
[30] Usp. Vuković, Hrvoje. Nav. dj. Str. 19.

Što se tiče definicija kibernetičkog terorizma, postoji ih mnogo, ali u ovom radu istaknut će se definicija profesorice Dorothy Denning koja definira kibernetički terorizam kao konvergenciju terorizma i kibernetičkog prostora, uzimajući u obzir vrstu motivacije, svrhu te objekte napada. S druge strane, profesor Mark Pollit opisuje kibernetički terorizam kao politički unaprijed osmišljen i motivirani napad na informacije, računalne sustave i podatke koji rezultiraju nasiljem nad neborbenim ciljevima podnacionalnim skupinama i tajnim agentima.[31] Kibernetički napadi na države i njihove informacijske infrastrukture zahtijevaju globalne odgovore na temelju regionalnih sporazuma. Ovakvi se napadi provode u više država pa je zbog toga sam postupak kaznenog progona izrazito kompleksan. Kompleksnost podrazumijeva da se napadnuta država poziva na međunarodno pravo tražeći potpunu pravdu za počinjen zločin.[32] Kako bi države ovo postigle, nužno je koristiti samoregulativne pravne mehanizme, koji moraju biti potpomognuti međunarodnim sporazumima. Zadnjih nekoliko godina statistički podaci ukazuju na to da je za odgovor na transnacionalni kibernetički terorizam neophodna upravo višestruka odnosno multilateralna suradnja. Information Security Timelines and Statistics[33] navodi kako su mete kibernetičkih napada iz 2020. godine u najvećem broju pojedinačne industrije, odnosno proizvodnje (18.9%), dok se zlonamjerni softveri manifestiraju kao najčešće tehnike (37.8%), nakon njih slijede krađe identiteta (17.6%) i ciljani napadi (10.8%). Izvješće također navodi kako ransomeware-i i DOS napadi dalje prevladavaju, osobito u Španjolskoj gdje se često događaju napadi na istraživačke COVID-19 pogone te u Velikoj Britaniji na Ministarstvo vanjskih poslova.[34]

[31] Isto. Str. 208.
[32] Usp. Tehrani, Pardis et al. Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. Computer Law & Security Review 29(3). Faculty of Law, The National University of Malaysia (UKM) Bangi: Malaysia, 2013.Str. 207-208. URL: https://www.researchgate.net/publication/257101606_Cyber_terrorism_challenges_The_need_for_a_global_response_to_a_multi-jurisdictional_crime (2020-08-30)

[33] Usp. Q1 2020 Cyber Attacks Statistics – HACKMAGEDDON. URL: https://www.hackmageddon.com/2020/04/14/q1-2020-cyber-attacks-statistics/
[34] Usp. 16-30 September 2020 Cyber Attacks Timeline – HACKMAGEDDON URL: https://www.hackmageddon.com/2020/11/09/16-30-september-2020-cyber-attacks-timeline/ (2020-11-10)

3. BUDUĆNOST KIBERNETIČKE SIGURNOSTI

Digitalne transformacije trajno su promijenile i povezale svijet na bezbroj načina i to brže nego ikad. Tako povezani svijet pruža razne mogućnosti, ali isto tako stvara određene prijetnje. Snaga tehnoloških promjena tijekom sljedećeg desetljeća predstavljat će izazove za pojedince, društvene organizacije, tvrtke i vlade. Kao najveći izazov u budućnosti predviđa se balansiranje masovnih tehnoloških promjena i upravljanje novim rizicima. Nužno će biti iskoristiti informacijsku i komunikacijsku tehnologiju (IKT) i omogućiti svim dionicima da promišljeno razmotre današnji izbor politike kako bi mogao utjecati na buduće ishode, uz što manje neželjenih posljedica.[35] Budućnost kibernetičke sigurnosti opisana je i kroz *The Cyber 2025 Model,*[36] koji procjenjuje da će sljedećih deset godina biti ekspanzivni tehnološki rast, značajni demografski pomaci i sve veće potrebe za obrazovanjem.[37] Također, razmatra se pitanje rada globalnog tržišta, jer pojavom novih proizvoda regulira se potražnja, količina, a i kombinacija proizvodnje istih. Osim što se može otvoriti i ograničiti trgovina, dopušteno je i zabraniti strana ulaganja, isto kao i uključivanje ili isključivanje sudionika u odlučivanju. Također se mogu razvijati i podržavati međunarodni standardi, ali i stvarati nacionalno specifični standardi.[38] Ukupni razvoj tehnologije dovest će do toga da će se podaci pohranjivati u oblaku, pa će to postati uvjet ka sudjelovanju u globalnoj ekonomiji. Pohranjivanje u oblaku (eng. *cloud computing*) je prilično poznata tema posljednjih godina, a oblačni sustavi poput Microsoft Azure, Amazon Web Services i Google Cloud postaju sve popularniji u organizacijama. Ovakav način pohranjivanja predstavlja ogroman plus za svjetski poznate IT tvrtke koje već mogu iskoristiti nevjerojatnu snagu pohrane, povezanost i dostupnost oblaka. Organizacije svih veličina mogu koristiti ove moćne poslužitelje bez da plaćaju novu opremu te mogu pristupiti svojim podacima s bilo kojeg internetskog uređaja. Na ovaj bi se način poboljšala automatizacija rada sustava, a

[35] Usp. Burt, David et al. Cyberspace 2025 Today's decisions, tomorrow's terrain - navigating the future of cybersecurity policy. Microsoft Corporation, 2014. Str. 2. URL: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/Events/netconference_march2015_submissions/C/reference_from_microsoft_cyberspace2025.pdf (2020-09-20)
[36] Usp. Helmbrecht, Udo et al. Cybersecurity: future challenges and opportunities. Greece, 2011. Str. 6. URL: https://www.btg.org/wp-content/uploads/2012/01/ENISA-Cyber-Security-Report-2011.pdf (2020-09-20)
[37] Usp. Burt, David et al. Nav. dj. Str. 9.
[38] Isto. Str. 2.

uvođenje umjetne inteligencije može značajno promijeniti način na koji organizacije rade. Pohranjivanje u oblaku omogućuje veću dostupnost podataka tvrtke s bilo kojeg mjesta, a osim toga, povećava i kapacitet za rad na daljinu.[39] Društvene organizacije bi zato mogle pripremiti radnu snagu, digitalno opismeniti one kojima je potrebno, s ciljem razvoja tržišta rada i osposobljavanja drugih sudionika u globalnoj ekonomiji. Korisnici tih tehnologija trebali bi usvojiti određeno znanje, a tvrtke ostati i dalje konkurentne, uz praćenje trendova.[40] Nadalje, o budućnosti ove sigurnosti i računalnim sustavima progovara i Eugene Kaspersky, ruski znanstvenik, naglašavajući kako budućnost nikako nije daleko. Budućnost je već ovdje, a na korisnicima je da ju osnaže. Kako su se hakeri s vremenom naučili prilagođavati promjenama sigurnosnih metoda, kibernetički se napadi više neće odvijati na isti način u budućnosti, stoga će svi računalni sustavi za otprilike trideset godina prijeći na jednu potpuno novu razinu i postati polazna točka civilizacije.[41] Iz filozofske perspektive, Kaspersky vjeruje kako će koncept kibernetičke sigurnosti sigurno kad tad zastarjeti i da će umjesto nje prevladati tzv. *cyber immunity* (kibernetički imunitet). Koristeći se metaforom, dobar kibernetički imunitet treba biti odlika svake organizacije, poduzeća, tvrtke pa i pojedinca, iako uvijek postoje načini da kibernetički imunitet oslabi, baš kao što oslabi imunitet čovjeka. Kad god ljudski imunološki sustav ne radi optimalno, simptomi počinju postajati vidljivi. Ovakav se princip djelovanja može primijeniti upravo na računala. Postoji program Acronis Cyber Protect[42] koji ima zadaću nadgledati sumnjive aplikacije i korisnike, ali i otkriti prisutnost zlonamjernih kodova na računalu bez obzira što je kod strukturiran s ciljem njegovog sakrivanja. Reagiranje na vrijeme uvijek rezultira manjom štetom i bržim oporavkom. Acronis Cyber Protect nudi jedinstvenu sposobnost, može vratiti sustav u prethodno poznato "dobro stanje" bez gubitka podataka. Acronis Cyber Protect prvo pokušava ukloniti sve loše kodove iz sustava, no ako uklanjanje nije

[39] Usp.What to Know About the Future of Cloud Computing and Data Security. URL: https://www.blackstratus.com/what-to-know-about-the-future-of-cloud-computing-and-data-security/ (2020-09-21)

[40] Usp. Burt, David et al. Nav. dj. Str. 10.

[41] Usp. How will cybersecurity change by 2050? | Cybersecurity & Technology News | Secure Futures | Kaspersky. URL: https://www.kaspersky.com/blog/secure-futures-magazine/earth-2050-cybersecurity/28313/ (2020-09-21)

[42] Usp. Five Phases of Cyber Immunity: Acronis Cyber Protect. Str. 4. URL: https://dl.acronis.com/u/rc/WP_Acronis_Cyber_Protect_Cloud_Cyber_Immunity_EN-US_200506.pdf (2020-09-24)

moguće, tada pokušava ublažiti njegov utjecaj. Osim toga, također može automatski implementirati nedostajuće "zakrpe" u sustav te ukloniti sve ugrađene prijetnje sa sigurnosnih kopija. Ono što je bitno kod kibernetičkog imuniteta je da on ima mogućnost otkrivanja nekih novih kibernetičkih napada, pružajući snažni obrambeni mehanizam. Ovakvi sustavi (kibernetički imuniteti) usvajaju tzv. *machine learning* (ML) tehnike, u kojima programer ne mora programirati, kodirati pravila, ali pravila može naučiti potpuno sam.[43] Međutim, zbog prisutnosti višestrukih aplikacija i sustava, integracija sigurnosnih rješenja i obrane od kibernetičkih napada postaje relativno teška, ponekad u tolikoj mjeri da "simptomi" unutar sustava nisu vidljivi. Primjer toga bio bi Maze Ransomware, koji kriptira sve datoteke u određenom sustavu.[44]

[43] Usp.Wlodarczak, Peter. Nav. dj. Str. 202.
[44] Usp. Ransomware Maze | McAfee Blogs. URL: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/ (2020-09-24)

4. ZAKLJUČAK

Kibernetika je znanost o upravljanju i kontroli nad strojevima i živim bićima. Osnovna načela kibernetike kao i kibernetički sustav osmislio je matematičar Norbert Wiener, čija su djela bitno utjecala na današnju primjenu i razvoj kibernetike. Kibernetička sigurnost, kao skup praksi, politika i koncepata koji se koriste u borbi protiv kriminala u kibernetičkom prostoru (eng. cyberspace-u), znatno se oslanja na samu kibernetiku. S obzirom na to da se sofisticiranost kiberentičkog kriminala znatno povećala zadnjih nekoliko godina, kibernetička sigurnost zahtjeva međusobno djelovanje više sigurnosti, kao što su informacijska, mrežna, aplikacijska te internet sigurnost, ali i dovoljno veliku razinu svijesti društva. Od društva se očekuje da korisnici računalnih sustava budu dobri sudionici te da međusobno surađuju s većim silama u državi, a države da surađuju s drugim državama koristeći samoregulativne pravne mehanizme. Osim toga, nužno je poticati i prevenciju računalnih sustava, što se odnosi primjerice na provjeravanje autentičnosti i autorizacije, posebice u obrazovnom sustavu gdje se mogu ugroziti intelektualna vlasništva sveučilišta, fakulteta, ali i osobni podaci studenata, nastavnog osoblja itd. Mnogi znastvenici kao što je primjerice Eugene Kaspersky tvrde da će se kibernetički zločini u budućnosti odvijati potpuno drugačije. Svrha je izgradnja sigurne budućnosti koja se može graditi jedino na sigurnim temeljima, a to su "dublje" digitalne kompetencije koje se zahtijevaju od korisnika, kako bi računalni sustavi uspješno funkcionirali. Promjena okruženja odnosno rad na globalnom tržištu i pohranjivanje u oblaku jasno ukazuju na to da današnje društvo čeka ozbiljni preokret, preokret kod kojeg je uvjet imati dobar kibernetički imunitet.

5. LITERATURA

1) Bayuk, L. Jennifer et al. Cyber Security Policy Guidebook. Wiley, 2012. Str. 4. URL: https://www.programmer-books.com/wp-content/uploads/2018/07/Cyber-Security-Policy-Guidebook-1st-Edition-2012.pdf (2020-08-27)
2) Bruijn de Hans; Janssen, Marijn. Building Cybersecurity Awareness: The need for evidence-based framing strategies. Government Information Quarterly, 2017. Str. 2. URL: https://www.sciencedirect.com/science/article/pii/S0740624X17300540 (2020-08-25)
3) Burt, David et al. Cyberspace 2025 Today's decisions, tomorrow's terrain - navigating the future of cybersecurity policy. Microsoft Corporation, 2014. Str. 2. URL: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/Events/netconference_march2015_submissions/C/reference_from_microsoft_cyberspace2025.pdf (2020-09-20)
4) Five Phases of Cyber Immunity: Acronis Cyber Protect. Str. 4. URL: https://dl.acronis.com/u/rc/WP_Acronis_Cyber_Protect_Cloud_Cyber_Immunity_EN-US_200506.pdf (2020-09-24)
5) Graham, James et al. Cyber Security Essentials. New York: Auerbach Publications. Str. 1. URL: http://www.bandido.ch/programming/Cyber_Security_Essentials.pdf (2020-08-30)
6) Hamidović, Haris. Mjesto i uloga cyber sigurnosti u razvoju modernih društava. // Sarajevski žurnal za društvena pitanja, vol 4, 1-2(2015). Str. 82. URL: https://www.researchgate.net/publication/302901758_Mjesto_i_uloga_cyber_sigurnosti_u_razvoju_modernih_drustava (2020-08-15)
7) Helmbrecht, Udo et al. Cybersecurity: future challenges and opportunities. Greece, 2011. Str. 6. URL:

https://www.btg.org/wp-content/uploads/2012/01/ENISA-Cyber-Security-Report-2011.pdf (2020-09-20)

8) How will cybersecurity change by 2050? | Cybersecurity & Technology News | Secure Futures | Kaspersky. URL: https://www.kaspersky.com/blog/secure-futures-magazine/earth-2050-cybersecurity/28313/ (2020-09-21)
9) Kibernetika. // Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2020. URL: https://enciklopedija.hr/natuknica.aspx?id=31381 (2020-08-15)
10) Nacionalna strategija kibernetičke sigurnosti. Zagreb, 2015. Str. 20. URL: https://www.uvns.hr/UserDocsImages/dokumenti/Nacionalna%20strategija%20kiberneticke%20sigurnosti%20(2015.).pdf (2020-08-30)
11) Q1 2020 Cyber Attacks Statistics – HACKMAGEDDON. URL: https://www.hackmageddon.com/2020/04/14/q1-2020-cyber-attacks-statistics/
12) Ransomware Maze | McAfee Blogs. URL: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/ (2020-09-24)
13) Tehrani, Pardis et al. Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. Computer Law & Security Review 29(3). Faculty of Law, The National University of Malaysia (UKM) Bangi: Malaysia, 2013.Str. 207-208. URL: https://www.researchgate.net/publication/257101606_Cyber_terrorism_challenges_The_need_for_a_global_response_to_a_multi-jurisdictional_crime (2020-08-30)
14) The Importance Of Cyber Security Awareness. URL: https://www.ogl.co.uk/the-importance-of-cyber-security-awareness (2020-08-25)
15) Vuković, Hrvoje. Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj. National security and the future, vol. 13, br. 3, 2012. Str.15. URL: https://hrcak.srce.hr/100728 (2020-08-15)
16) What to Know About the Future of Cloud Computing and Data Security. URL: https://www.blackstratus.com/what-to-know-about-the-future-of-cloud-computing-and-data-security/ (2020-09-21)

17) Why Is Higher Education the Target for Cyber Attacks? URL: https://www.blackstratus.com/why-is-higher-education-the-target-for-cyber-attacks/ (2020-08-30)
18) Wlodarczak, Peter. Cyber Immunity - A Bio-Inspired Cyber Defense System. University of Southern Queensland: Australia, 2017. Str. 206. URL: https://www.researchgate.net/publication/315861769_Cyber_Immunity_-_A_Bio-Inspired_Cyber_Defense_System (2020-08-30)
19) 16-30 September 2020 Cyber Attacks Timeline – HACKMAGEDDON URL: https://www.hackmageddon.com/2020/11/09/16-30-september-2020-cyber-attacks-timeline/ (2020-11-10)