UNIVERZITET U SARAJEVU

FAKULTET POLITIČKIH NAUKA

ODSJEK SIGURNOSNE I MIROVNE STUDIJE

CYBER SIGURNOST U EVROPSKOJ UNIJI I COVID-19: STANJE I IZAZOVI

- magistarski rad -

Kandidat:

Dževad Mujadžić

Broj indeksa: 7-IS/21

Mentor:

Prof. dr. Mirza Smajić

Sarajevo, septembar 2022.

2022	Dževad Mujadžić	Cyber sigurnost u Evropskoj uniji i COVID-19: Stanje i izazovi

ODSJEK SIGURNOSNE I MIROVNE STUDIJE

CYBER SIGURNOST U EVROPSKOJ UNIJI I COVID-19: STANJE I IZAZOVI

- magistarski rad -

Kandidat:
Dževad Mujadžić
Broj indeksa: 7-IS/21

Mentor:
Prof. dr. Mirza Smajić

Sarajevo, septembar 2022

SADRŽAJ

POPIS I TUMAČENJE SKRAČENICA

FPA	Analiza vanjske politike
CIA Factbook	Svjetska knjiga činjenica
GSDP	Generalni sekretarijat za razvoj i planiranje
UN	Ujedinjene nacije
GCC	Vijeće za saradnju u Zaljevu - Gulf Cooperation Council
BDP, GDP	Bruto domaći proizvod (eng. gross domestic product)
MMF	Međunarodni monetarni fond
ICJ	Međunarodni sud pravde
NTC	Nacionalno prijelazno vijeće
MKS	Međunarodnog krivičnog suda
GDPR	Opća uredba o zaštiti podataka
EU	Evropska unija
ENISA	Agencija Evropske unije za cyberu sigurnost
DDoS	Cyber napadi uskraćivanjem resursa
RFID	Radiofrekventna identifikacija
IKT	Informacione i komunikacione tehnologije
OECD	Organizacije za ekonomsku saradnju i razvoj
G8	Grupa osam Skupina industrijski najrazvijenijih i gospodarski najmoćnijih zemalja svijeta
EC3	Evropski centar za cyberi kriminal
EUROPOL	Agencija Europske unije za suradnju tijela za izvršavanje zakonodavstva
CERT	Evropski sistem upozorenja i informacija
JHA	Vijeće za pravosuđe i unutarnje poslove EU-a
EEAS	Europska služba za vanjsko djelovanje
IOCTA	Procjena prijetnje od organiziranog kriminala na internetu
APT	Napadi koji su napredne trajne prijetnje

POPIS TABELA I SLIKA

Popis tabela

Popis slika

SAŽETAK

Ovaj rad se bavi utjecajem nove krize s korona virusom i povećanog rada na daljinu na cyber sigurnost i prioritete za djelovanje EU. Akcije bi trebale uključivati poboljšanje cyber sigurnosti poslovanja, kritične infrastrukture i korisnika, te stvaranje industrije cyber sigurnosti u EU. Kako se sve više aspekata našeg života događa na mreži, postajemo ranjiviji na zlonamjerne napade. To se pokazalo 2020. godine kada su cyber napadi sve više poremetili rad bolnica, pružalaca usluga, državnih službi i preduzeća širom svijeta. Učestalost i obim napada stvorili su osjećaj hitnosti da poboljšamo našu otpornost na cyber sigurnost. Ovaj rad tvrdi da bi EU trebala iskoristiti prednosti cyber sigurnosti slijedeći ambiciozniji plan cyber sigurnosti i stavljajući vrijednosti EU u srž svog pristupa. Također poziva da se cybera sigurnost uključi u sve stupove EU, uključujući politiku EU za industrijsko istraživanje i inovacije, kao i u investicione planove EU i diplomatsku strategiju.

Ključne riječi: COVID-19, cyber sigurnost, sigurnost, izazovi i poremećaji, zaštita podataka, privatnost, zdravstveni podaci

1. UVOD

Pandemija novog koronavirusa (COVID-19) pogodila je svijet u martu 2020., promijenivši način na koji živimo, radimo i komuniciramo. Socijalno distanciranje i rad od kuće postali su norma. U Evropi, kao i u većem dijelu svijeta, sve je moralo biti digitalizirano da bi se nastavile vladine, društvene i ekonomske aktivnosti. Digitalizacija je već bila trend, ali dolazak COVID-19 doveo je do toga da se to dogodi preko noći. Tako je sigurnost naše vlade, preduzeća i građana, koja se razvijala vijekovima, za samo nekoliko mjeseci postala pitanje cyber sigurnosti.

Tokom 2020. pojačan je intenzitet i obim cyber napada. Zlonamjerni akteri iskoristili su naše strahove povezane sa zdravstvenom krizom, šaljući lažna ažuriranja COVID-19 i alarmantne phishing poruke kako bi prikupili korisničke podatke ili instalirali zlonamjerni softver na uređaje korisnika. Mnogi novi korisnici Interneta nisu bili spremni za ovu prijetnju, niti su bili upućeni kako da se s njom suoče. Procijenjeni globalni gubici od cyber kriminala u 2020. dosegli su rekord od nešto manje od 1 bilion dolara. (Morgan S., 2019.) Ako se mjeri kao BDP i uporedi sa nacionalnim ekonomijama, promet cyber kriminala bi trenutno bio na trinaestom mjestu u svijetu (između Indonezije i Turske). Kako su svi i sve sada na mreži, mogućnosti za napade su se povećale. Ovo i povećana aktivnost zlonamjernih aktera učinili su cyber sigurnost još težim za postizanje. Naravno, stoga, integracija cyber sigurnosti u sve aspekte života, uključujući rad na daljinu, bila je teška bitka.

Ovaj rad, iako predstavlja trenutno stanje, ima za cilj da definiše priliku koju cyber sigurnost ima za Evropu. Fokusira se na analizu višestrukih aspekata cyber sigurnosti i faktora koji igraju ulogu u njenom postizanju, uključujući utjecaj krize COVID-19 i povećani rad na daljinu. Tvrdi se da bi EU trebala slijediti ambiciozniji plan cyber sigurnosti s vrijednostima Unije u središtu svog pristupa i poziva kreatore politike da integriraju cyber sigurnost u EU-ovu politiku industrijskih inovacija i istraživanja, kao i politiku ulaganja i diplomatsku strategiju. Konačno, ovaj rad pruža praktične preporuke za kreatore politike kako bi se pomoglo u realizaciji mogućnosti koje cyber sigurnost predstavlja za EU.

COVID-19 je vanredna situacija za javno zdravlje širom svijeta. Agencija za cyberu sigurnost i infrastrukturnu sigurnost Ministarstva sigurnosti EU-a objavila je savjetodavni memorandum u vezi s ključnim infrastrukturnim radnicima 28. marta 2020. (Benkler, Y., Tilton, C., Etling, B., Roberts, H., Clark, J., Faris, R., Kaiser, J., Schmitt, C., 2020.) Rukovodstvo za suočavanje s COVID-19 mora razbiti silose informacija i koordinirati napore za zaustavljanje ili

obuzdavanje novog koronavirusa koji uzrokuje COVID-19. Održiva ljudska sigurnost je značajna. Širi zdravstveni sistem naglašava sigurnost u zdravstvu, zagađenje životne sredine, hranu, ekonomiju i spremnost za buduće moguće pandemije. Južna Koreja je shvatila važnost praćenja kretanja zaraženih osoba i osoba koje su s njima kontaktirale. (CybSafe, 2020.; Collett, R., Barmpalious, N., Pawlak, P., 2021.)

Mnogi ljudi morali su raditi kod kuće, birati telemedicinu i izvoditi učenje na daljinu i online školovanje zbog pandemije COVID-19. Zahtjevi za ove ljude uključuju računare, internet, softver za zaštitni zid, kamere, itd. Sastanci se mogu održavati putem video konferencija. Iako se pozivi mogu šifrirati radi sigurnosti, COVID19 je stvorio nove izazove u cyber sigurnosti. (Collett, R., Barmpalious, N., Pawlak, P., 2021.; ENISA, 2019.) Rad i učenje kod kuće zbog COVID-19 uzrokuje povećanu upotrebu interneta, podstiče više ljudi da provode mnogo vremena na mreži i pruža više mogućnosti za cyber kriminal. (ENISA, 2021.) Smrtonosne prijetnje cyber sigurnosti uključuju zlonamjerni softver, neželjenu e-poštu, zlonamjerne web stranice, ransomware, zlonamjerne domene, DDoS napade, kompromitaciju poslovne e-pošte, zlonamjerne poruke na društvenim mrežama, itd. (Evropska komisija (2021a., 2021b.) Razvoj upotrebe IKT-a je podređen sigurnosnim zahtjevima. Faktori koji se odnose na sigurnost uključuju svijest osoblja o sigurnosti IKT-a, aktivnosti koje se odnose na sigurnost IKT-a, politike koje se tiču sigurnosti IKT-a, itd. (Eurostat, 2021.)

Tokom pandemije COVID-19 važno je izbjegavati bliski kontakt sa mnogim ljudima u svakodnevnom životu. Radiofrekventna identifikacija (RFID) je korisna za sisteme kupovine, upravljanje lancem snabdijevanja i sigurnost. RFID koristi radio talase i RFID oznake sa mikročipovima za skladištenje podataka i antene za prijem i prenos radio frekvencijskih signala. RFID može pružiti dodatni mehanizam protiv krađe. Mnoge RFID oznake mogu se čitati u isto vrijeme i sa velike udaljenosti. Stoga, RFID pomaže u poboljšanju efikasnosti, sigurnosti i sigurnosti različitih sistema tokom pandemije COVID-19 (Euractiv, 2021.) zbog istovremenog višestrukog očitavanja i mogućnosti daljinske identifikacije.

Svrha ovog rada je uvođenje cyber rizika i cyber sigurnosti tokom pandemije COVID-19. Naredni dijelovi rada organizirani su na sljedeći način: drugi dio predstavlja glavne tehnologije u borbi protiv COVID-19, treći odjeljak predstavlja cyber napade i cyber rizike zbog COVID-19, četvrti dio predstavlja cyber sigurnost za rad na daljinu, peti dio dio predstavlja cyber sigurnost IoT-a i telemedicine, šesti dio se bavi cyber bezbjednošću zasnovanom na blockchain tehnologiji, a sedmi dio je zaključak.

2. TEORIJSKI METODOLOŠKI OKVIR RADA

2.1. Problem istraživanja

Posljedice pandemije COVID-19 rezultirale su brojnim intervencijama koje su rezultirale brojnim intervencijama za obavezno usvajanje tehnologije kako bi se popunile praznine, što je predstavljalo izazove za probleme cyber sigurnosti koji su se pojavili. Cyber sigurnost u pandemiji COVID-19 je koristan pratilac cyber sigurnosti koji bi trebao biti biblioteci donositelja strateških odluka, tehničkih, operativnih i administrativnih menadžera, studenata tehnologije, tražitelja znanja i onih koji su odgovorni za upravljanje ili onih koji su značajno pogođeni po tehnološki rizik. U vremenu pandemije globalni uticaj ostavio je sjaćanja na paniku, neizvjesnost i tjeskobu, cyber prostor je nastavio primati veliki porast online aktivnosti povezanih s odgovorom na COVID-19, u vrijeme kada su operateri podatkovnih mreža i davatelji usluga u oblaku jurili za pokroviteljstvom internetskih tehnologija, iz razloga jer su svi svoj dio djelovanja prebacili na internet gotovo za sve, od akademskih aktivnosti, vjerskih, do širenja korporativnih informacija do potpisivanja ugovora, lansiranja proizvoda, pa sve do sportskih aktivnosti. Dakako, svemu ovome dodaje se i problem sektora zdravstvene skrbi, gdje se zdravstveni podaci klasificiraju kao osjetljivi zbog njihovog odnosa sa životom, dobrobitima i zdravim životom. Loše upravljanje zdravstvenim podacima može potencionalno rezultirati stigmatizacijom i kršenjem privatnosti. Vrijedna priroda ovih informacija čini ga vrlo privlačnim za cyber kriminalce koji su tijekom pandemije COVID-19 koristili prijevare e-pošte, ransomware i dr. oblike hakerskih napada za ciljane ranjive računalne infrastrukture u bolnicima, ljekarnama, medicinskim labaratorijima, organizacijama zdravstvenog osiguranja i drugim institucijama koji su uključeni u generiranje, upravljanje ili korištenje osjetljivih zdravstvenih podataka. COVID-19 otvorio je novu perspektivu u svjetonazoru cyber sigurnosti i daje pregled glavnih izazova s kojima se organizacije susreću u izvođenju učinkovitih intervencija cyber sigurnosti. Stoga, možemo postaviti pitanja:

2.2. Predmet istraživanja

Digitalne platforme u posljednjih nekoliko godina, kao i općenito tokom pandemije COVID-19, postale su privilegirani prostor gdje pojedinci mogu obavljati svoje radne, društvene i slobodne aktivnosti. Digitalno okruženje je ogromno i stoga je idealno tlo za cyber napade koji mogu biti neselektivni ili ciljani, usmjereni na velike i male organizacije u javnom i privatnom sektoru. Stoga korištenje Interneta i povezanih uređaja nudi nove mogućnosti ljudima i kompanijama, ali u isto vrijeme stvara nove rizike. Spektar potencijalnih napada i napadača je širok i svakim danom postaje sve veći, sve do te mjere da je na Svjetskom ekonomskom forumu

u Davosu 2021. cyber sigurnost ocijenjena kao jedan od najvećih ekonomskih rizika u tekućoj godini. Nove tehnologije, mobilni telefoni, pametni uređaji povezani na Internet stvari i mnoge aplikacije umjetne inteligencije izlažu i privatne i javne organizacije napadačima, povećavajući rizik od, na primjer, gašenja ili subverzije industrijskih kontrolnih sistema. Nadalje, napadi postaju zabrinjavajuće sofisticiraniji i skuplji za otkrivanje.

Veličina fenomena je vidljiva analizom podataka o kompjuterskim napadima koji utiču na elektronske uređaje koje svakodnevno koristimo. Prema studiji koju je Comparitech proveo u trećem kvartalu 2019. godine, 9,68% računara i 3,04% mobilnih uređaja u EU zaraženo je zlonamjernim softverom. Ovo su softveri namjerno dizajnirani da izazovu štetu na računaru, serveru, klijentu ili računarskoj mreži. Upoređujući evropske podatke sa podacima drugih velikih svjetskih ekonomija, možemo vidjeti kako je Evropska unija na prvom mjestu po postotku zaraženih računara, ispred Kine, Japana, SAD-a, Južne Koreje i Velike Britanije. Umjesto toga, kada su mobilni uređaji u pitanju, države članice EU su u prosjeku zaštićenije od onih u svim drugim geografskim područjima koja se razmatraju, s izuzetkom Japana. Analizirajući podatke država članica EU, možemo vidjeti da su najviše meta cyber napada na računare Francuska (15,09%) i Grčka (14,59%). Umjesto toga, najranjiviji na mobilnim uređajima su Rumunija (5,04%) i Italija (5,01%).

Pandemija COVIDa stvorila je nove mogućnosti za cyber kriminalce. Prema podacima Komisije EU, 40% europskih radnika iskusilo je oblike rada na daljinu od početka pandemije, čineći kućne računare, koji su općenito manje zaštićeni od uredskih i poslovnih uređaja, mjestom pristupa podacima i vrijednim digitalnim aktivnostima. Na primjer, u aprilu 2020. godine, Švicarski nacionalni centar za cyberu sigurnost primio je 350 prijava o cyber napadima (phishing, lažne web stranice, direktni napadi na kompanije, itd.) u poređenju sa uobičajenih 100-150. Pandemija i povećanje broja zaposlenih od kuće viđeni su kao glavni uzrok tome, jer pojedinci koji rade kod kuće ne uživaju isti nivo zaštite kao oni u radnom okruženju (npr. specijalizovani operateri koji se bave IT sigurnošću i naprednim sistemima za otkrivanje).

Eksponencijalni rast problema mora potaknuti evropske organizacije, javne i privatne, da povećaju svoj budžet za IT sigurnost. Izvještaj „NIS Investments“ koji je objavila ENISA u decembru 2020. pokazuje kako je prosečna potrošnja evropskih organizacija na IT sigurnost (u odnosu na IT budžet) znatno niža od proseka američkih organizacija. Gledajući podatke koje je objavila ENISA, možemo vidjeti da među evropskim zemljama francuske organizacije izdvajaju najveći dio svog IT budžeta za sigurnost. Država članica sa najlošijim učinkom (među

onima koje je razmatrala ENISA analiza) je Belgija sa samo 1,2% prosječnog IT budžeta posvećenog cyber sigurnosti. Prosječan budžet koji preduzeća ulažu u projekte implementacije NIS direktive je oko 175.000 eura, a 42,7% pogođenih organizacija izdvaja između 100.000 i 250.000 eura. Sektori u koje se ulaže najveći dio budžeta za IT sigurnost su bankarske i finansijske usluge (5,6%), farmaceutski proizvodi (5,5%) i izdavaštvo softvera i internet usluge (4,7%). Sektori koji bilježe najlošije rezultate su i dva najznačajnija - obrazovanje (2%) i transport (1%). Transport, posebno sa širenjem samovozećih vozila, mogao bi postati sve više meta cyberih napada.

Komisija je vrlo svjesna potrebe za daljim ulaganjima u sektor. Iz tog razloga, uvrstio je cyber sigurnost među probleme koje će države članice morati riješiti korištenjem sredstava iz EU sljedeće generacije. Kao i pojačanja koja se financiraju u okviru EU Next Generation, drugi programi se fokusiraju na to da Unija postane otpornija i rješavanje izazova koji su pojačani pandemijom i njenim posljedicama. To uključuje jačanje cyber odbrane Unije i podršku digitalnoj tranziciji opremanjem programa Digitalna Evropa s ukupnim budžetom od 8,2 milijarde eura.

2.3. Ciljevi istraživanja

Opći ciljevi ovog istraživanja bazirati će se na sljedeća istraživačka pitanja:

1. U kojoj mjeri cybersecurity je zaštitio kritične poslovne podatke od nezakonitog pristupa?
2. Da li je neznanje ili nemar vlasnika podataka pomoglo internetskom prevarantu da uspije u cyber napadima?
3. Koje pouke se trebaju naučiti iz slučajeva cyber kršenja tijekom pandemije?
4. Koje aspekte cyber sigurnosti treba optimizirati kako bi odgovarali trendu?

2.4. Naučni cilj

Naučni cilj rada je na osnovu temeljitog istraživanja prikazati i identificirati stanje, sigurnosne mjere i rizike donesene u doba COVID-19 pandemije (krize) i njihov utjecaj na cyber sigurnost u Evropskoj uniji.

2.5. Društveni cilj

Uspješna realizacija ovoga rada otvorila bi nova saznanja na ovu temu, ali i omogućila zainteresovanima lakši i novi pristup ovoj tematici.

2.6. Sistem hipoteza

H_g - Pandemija je stvorila niz jedinstvenih okolnosti vezanih za cyber kriminal, koje su također uticale na društvo i poslovanje, povećana anksioznost uzrokovana pandemijom povećala je vjerovatnoću da će cyber napadi uspjeti što odgovara povećanju broja i raspona cyber napada.
H_1 - U kojoj mjeri je COVID-19 utjecao na putanju politike cyber sigurnosti EU?

2.7. Način istraživanja

Teorijska osnova za pisanje ovog rada su brojni sekundarni izvori domaćih i stranih podataka, prvenstveno postojeća stručna i naučna literatura, brojni časopisi, aktuelne publikacije, članci i istraživanja relevantni za temu sigurnosti informacionih sistema za vrijeme pandemije COVID-19.

3. NOVA DIMENZIJA SIGURNOSTI: CYBER SIGURNOST

Cyber sigurnost je globalni fenomen koji vladama predstavlja značajan socio-tehnički izazov, ali zahtijeva i uključivanje građana. Iako je cyber sigurnost jedan od najozbiljnijih izazova s kojima se vlade danas suočavaju, dostupnost i svijest javnosti i dalje su niski. Iako su gotovo svi čuli za cyber sigurnost, hitnost i ponašanje pojedinaca ne odražavaju visoku svijest. Internet se previše smatra sigurnim okruženjem za razmjenu informacija, obavljanje trgovine i nametanje kontrole nad fizičkim svijetom. Bez obzira na to, cyber rat je već u toku i postoji hitna potreba za poboljšanjem pripravnosti. Nemogućnost efikasnog uokvirivanja cyber sigurnosti je rezultirala nedostatkom okvira politike. Ovaj dio rada govori o prirodi cyber prostora i pokazuje koliko je internet nesiguran za prenošenje ličnih i finansijskih informacija. Iako se čini da većina ljudi internet smatra sigurnim okruženjem i redovno ga koristi putem svojih uređaja, tableta i laptopa, značajan broj napada se dešava svakodnevno. (Arora, A., Nandkumar, A. i Telang, R., 2006.) Prijetnje cyber sigurnosti, hakovi i kršenja sigurnosti na Internetu postali su daleko češći. A kako broj ovih nesreća raste, preduzeća moraju imati veće troškove kako bi ih stavili pod kontrolu. Iako je većina cyber napada bezopasna, neki imaju ozbiljan uticaj. Sigurnosne povrede mogu biti u rasponu ozbiljnosti od minimalnih ili ograničenih posljedica do napada distribuiranog uskraćivanja usluge (DDoS), krađe podataka, manipulacije podacima, prijevare identiteta, pa čak i preuzimanja sistema koji uzrokuju fizičke ozljede.

Termin “cybersecurity” definiše široku lepezu sistema i procesa koji se implementiraju za zaštitu računara, njihovog hardvera, aplikacija, mreža i podataka od neovlašćenog pristupa i curenja informacija. (Kunnathuvalappil Hariharan, N., 2018.) Osim toga, Cyber sigurnost se bavi sprječavanjem neželjenog pristupa i izmjene vaše digitalne opreme i informacija koje su povezane na internet ili mrežu. Internet je evoluirao od izvora znanja do platforme za poslovanje, oglašavanje i prodaju naših proizvoda u različitim formatima, komunikaciju s našim potrošačima i trgovcima i obavljanje bankarskih transakcija. Internet pruža brojne prednosti i omogućava nam da promovišemo naše poslovanje na globalnom nivou uz niske troškove i uz minimalan rad ljudi u relativno kratkom vremenskom periodu. Kako internet nikada nije razvijen za praćenje i analizu ponašanja korisnika. (Leon, LD, Rafferty, PD i Herschel, R., 2012.) Internet je prvobitno kreiran da poveže automatizovane računare kako bi se olakšalo dijeljenje resursa i također pružio jedinstveni okvir za zajednicu naučnika. Kako internet pruža mnoštvo prednosti, on također pruža jednake mogućnosti cyber teroristima i hakerima. Stoga terorističke organizacije i njihovi saveznici koriste internet za različite ciljeve, uključujući sticanje i distribuciju informacija iz zlonamjernih razloga, regrutaciju novih

terorista, finansiranje napada i motiviranje terorističkih akata.[1] Često se koristi za poboljšanje komunikacije između terorističkih grupa i upravljanja i širenja obavještajnih podataka u terorističke svrhe.

3.1. Karakteristike cyber prostora

Cyber prostor je virtuelno okruženje koje koristi elektroniku i elektromagnetski spektar za skladištenje, uređivanje i deljenje podataka putem umreženih sistema i povezanih fizičkih struktura.[2] To je nematerijalni prostor koji se koristi za telekomunikacije i aktivnosti vezane za internet. Osim toga, to je potpuno virtuelni ekosistem za umrežavanje i komunikaciju koji se pridružuje preko 2,7 milijardi ljudi širom svijeta pružajući zajedničku platformu za razmjenu ideja, perspektiva, usluga i prijateljstava. Prirodno je rastegljiv i bez granica, te se brzo povećava bez obzira na fizičke ili geopolitičke granice.

3.2. Zašto je cyber sigurnost važna?

Cyber sigurnost je danas prepoznata kao kritična komponenta života pojedinaca i zajednica, kao i organizacija, vlasti, akademskih institucija i preduzeća. Zaštita djece i članova porodice od online prevare je ključna za porodice i roditelje. Što se tiče finansijske sigurnosti, ključno je osigurati finansijske detalje koji mogu oštetiti našu finansijsku situaciju. Internet je kritičan i vrijedan za akademike, studente, zaposlene i akademske institucije; stvorio je brojne mogućnosti za učenje, a istovremeno predstavljao i razne prijetnje na mreži. Većina korisnika interneta mora znati kako se zaštititi od krađe identiteta i online prijevara, jer je ta svijest za njih ključna. Odgovarajuća edukacija i sigurnost online ponašanja i sistema rezultiraju smanjenjem rizika i sigurnim onlajn okruženjem. Mala i srednja preduzeća takođe se susreću sa raznim bezbjednosnim poteškoćama zbog nedostatka resursa i dovoljno stručnosti u cyber sigurnosti. (Maruster, L., 2003.) Brzi napredak tehnologije također se razvija i dovodi u pitanje cyber sigurnost, jer još uvijek nemamo trajna rješenja za navedene probleme. Budući da aktivno štitimo i izlažemo brojne okvire i tehnologije za osiguranje naše mreže i informacija, nijedna od ovih mjera ne pruža dugoročnu zaštitu. Međutim, šire razumijevanje sigurnosti i implementacija odgovarajućih rješenja može nam pomoći u zaštiti intelektualne svojine i poslovnih tajni i ublažavanju finansijskih i reputacijskih gubitaka.[3] Vlade na saveznom, državnom i općinskom nivou pohranjuju znatnu količinu podataka i povjerljivih informacija na mreži u digitalnom obliku, što ih čini glavnom metom za cyber napade. Vlade često nailaze na poteškoće kao rezultat neadekvatne infrastrukture, nerazumijevanja i neadekvatnog

1 Izvještaj ureda Ujedinjenih naroda o drogama i kriminalu (UNODC), korištenju interneta u terorističke svrhe.
2 Izvještaj dostupan na http://searchsoa.techtarget.com/definition/cyberspace
3 Izvještaj iz CISCO-a, Cybersecurity: Svačija odgovornost, 2010.

finansiranja. Za vladine agencije je od ključnog značaja da pružaju pouzdane usluge javnosti, održavaju zdravu komunikaciju sa građanima i da obezbjede poverljive informacije.

3.2. Paradoks cyber sigurnosit

Prostor za kreiranje cyber politike pun je paradoksa. Odabir jedne opcije može doći po cijenu druge, dok postoje opravdanja za nastavak u oba smjera. Politika cyber sigurnosti i kreiranje politike odvijaju se unutar ekosistema koji zahtijevaju interakciju između dionika iz različite populacije, sektora politike i administracije. Odgovornosti su raspoređene na brojne javne subjekte na federalnom i lokalnom nivou, svaki sa svojim skupom izazova i poteškoća, što otežava poduzimanje kolektivnih akcija. Društvo uključuje mnoge aktere koji možda žele sigurnost, ali imaju različita očekivanja o ulozi vlade u održavanju sigurnosti i sigurnosti cyber prostora. Vlasti mogu igrati skromnu ili značajnu ulogu u cyber sigurnosti. Lideri moraju odgovoriti na zahtjeve društva, formulirati politike i alocirati resurse, dok vladine institucije moraju provoditi te politike i ciljeve. Ovo može izgledati kao jasan odnos, ali stvarnost je daleko složenija i višestruka, budući da se uloge dionika često sukobljavaju i paradoksalne su. (May, AU, 2017.) Iako vlade traže privatnost građana i kompanija, one se u potpunosti ne protive prikupljanju informacija za svoje interese. Cijela debata o "backdoor" pristupu podacima pokazuje dilemu s kojom se vlade suočavaju. S jedne strane, vlade žele da se kompanije i ljudi brane, ali ne žele da usvoje šifriranje ili druge mjere privatnosti, jer bi to moglo omogućiti kriminalcima i teroristima da prikriju svoje tragove.

Zahtjevi vlade mogu nametnuti velika opterećenja i troškove preduzećima. Često se očekuje da će organizacije zaštititi online sigurnost i sigurnost svojih klijenata; iako se mnoga preduzeća i dalje pitaju da li će se ulaganje u cyber sigurnost isplatiti u smislu troškova povrede podataka. Troškovi otklanjanja kršenja podataka uključuju obeštećenje klijenata, plaćanje novčanih kazni i sudskih taksi, ulaganje u forenzičke i istraživačke procese, te provođenje kontra i preventivnih mjera. Potpuna sigurnost nikada nije dostižna, a cyber sigurnost nije besplatna.

Reputacija preduzeća i drugih organizacija ključna je za očuvanje povjerenja klijenata. Preduzeća ne žele da budu povezana sa prijetnjama cyber sigurnosti ili da se smatraju da im nedostaju adekvatne sigurnosne mjere. Koliko novca preduzeća ulažu u cyber sigurnost? Kompanije mogu biti nesklone otkrivanju svojih troškova cyber sigurnosti javnosti. Paradoks je da nedovoljna ulaganja mogu signalizirati da nisu adekvatno zaštićeni, ali prevelika potrošnja može ukazivati na to da su previše zabrinuti zbog toga da budu meta cyber kriminalaca ili

jednostavno rasipaju novac. Što se tiče cyber sigurnosti, ne postoji jedinstvena strategija za posao.

3.3. Pregled literature o cyber sigurnosti

Ova kratka analiza pokazuje uticaj cyber sigurnosti u savremenom svijetu. Sigurnost u cijelom ITC svijetu je ključna kako za zaštitu ovlaštenog korištenja informacija od napadača, tako i za pružanje povjerenja i povjerenja u ICT koje je neophodno za njegovu upotrebu. U nastavku su neki od problema koji pokreću problem cyber sigurnosti. Cyber sigurnost se odnosi na zaštitu svega što je potencijalno izloženo korišćenju interneta; to uključuje računare, mreže, lične uređaje, lične podatke, privatnost, pametne telefone i ljudska bića.

3.3.1. Uticaj cyber kriminala na poslovanje i društvo

Sve veći broj pojedinaca koji koriste internet i to su novi korisnici koji nisu upoznati sa rizikom u cyber prostoru. Velika većina novih korisnika dolazi iz zemalja u razvoju u kojima je cyber sigurnost još uvijek u povoju, a zaštitni sistemi su nedostupni korisnicima - bilo zbog finansijskih ograničenja ili dostupnosti.

Cyber kriminal kao nova pretnja doveo je do velikog uticaja na preduzeća i društvo u cjelini. Zanimljivo je da je cyber kriminal u ovom trenutku dobio na zamahu koji čak ni pesimistični posmatrači nisu vidjeli. (ICASA, 2013) Prisustvo cyber kriminala i cyber ratovanja dovelo je do velikog broja zakonodavnih i regulatornih inicijativa na globalnoj osnovi. Cyber sigurnost je sada regulisana brojnim aktima i propisima, a sve su detaljnije odredbe za javni sektor i za preduzeća.

Kritična tehnološka infrastruktura postaje sve ranjivija na cyber napade, što je promijenilo igru organizacija u njihovim industrijama. Prije 20 godina tehnološka infrastruktura nije bila osjetljiva na cyber napade jer je arhitektura bila odvojena jer nedavno vidimo da se sistemi integriraju. Ahilova peta ovih infrastruktura su njihovi industrijski kontrolni sistemi (ICS) kao što su sistemi nadzora i prikupljanja podataka (SCADA) i distribuirani kontrolni sistemi (DCS). ICS su inicijalno dizajnirani sa vlasničkom tehnologijom i bili su odvojeni od drugih postojećih korporativnih mreža, kao što su lokalne mreže i mreže šireg područja. Zbog ove podjele arhitekture sistemi nisu bili izloženi vanjskim napadima. Težnja ka isplativosti i dostupnosti komercijalne gotove tehnologije dovela je do većeg oslanjanja na široko rasprostranjene operativne sisteme kao što su Windows kako bi se poboljšao vremenski kritičan odgovor i konkurentnost. Kao rezultat toga, mnogi od današnjih su povezani na internet i mogu im se

pristupiti na daljinu (cloud computing), što većina organizacija ima malo kontrole nad sigurnošću na svom sistemu zasnovanom na oblaku.

Povezivanje ICS-a na internet ima važne implikacije. Izlaže kontrolne sisteme hakiranju, crvima, virusima i nizu drugih ranjivosti koje se mogu uvesti putem interneta, intraneta, udaljenog dial-up-a i bežičnih aplikacija. Ranjivost se sastoji od spajanja uobičajenih informacionih tehnologija kao što su Ethernet, Windows i Web servisi u ICS.

Zlonamjerne cyber aktivnosti postaju sve sofisticiranije i lakše ih je izvršiti. Pojedinci ili grupe zainteresovani za montiranje cyber napada ne moraju imati napredno znanje o kompjuterskom programiranju, jer mogu pristupiti online kompletu alata za kriminal putem you tube-a ili kupiti gotovi komplet alata za kriminal. Stoga nije lako ući u trag pojedincu koji je počinio cyber kriminal ili prekršaj, budući da postoje softveri koji im pomažu da svoj posao obavljaju bez traga. Primjer takvog programa je komplet za zločine Zeus, čiji se zlonamjerni kod može prilagoditi, a verzije izvornih kodova za bankovni trojanski konj su dostupne na internetu. Cijena Zeusa u rasponu se kreće od 700 USD do besplatnih staza na internetu.

Iako su izgledi za cyber rat malo vjerovatni, sve je jasnije da će cyber dimenzija vjerovatno biti dio budućih sukoba. Prema preliminarnoj procjeni koju je izvršio Centar za strateške i međunarodne studije (CSIS) u Washingtonu, 33 zemlje trenutno uključuju cyber rat u svoje vojno planiranje i organizaciju. To bi moglo uključivati „cyber sposobnosti za izviđanje, informativne operacije, prekid kritičnih mreža, za "cyber napade" i kao dopunu elektronskom ratu i informacionim operacijama."

3.3.2. Izazovi cyber sigurnosti

Izazovi cyber sigurnosti mogu imati različite oblike, iako je većina usmjerena na pojedince i organizacije. U zavisnosti od prirode i načina napada, cyber operacija može imati uticaj i na ekonomiju. Sljedeći odjeljak opisuje neke od glavnih izazova cyber sigurnosti, pokrivajući prvo one koji imaju tendenciju da utiču na pojedinačne korisnike, a zatim ispitujući one koji mogu imati implikacije na organizacije. Izvještaj Svjetskog ekonomskog foruma objavljen u januaru 2014. ispituje potrebu za novim pristupima za povećanje otpornosti na cyber napade i sugerira da bi neuspjeh da se efikasno osigura cyber prostor mogao rezultirati ukupnim uticajem od približno 3 biliona USD do 2020. Rizik i odgovornost u hiperpovezanom svijetu, 2014.). Prijetnje informacijama u cyber prostoru rastu i evoluiraju tako brzo, nedavno se šire na platformama kao što su društvene mreže i mobilne tehnologije. Dok se organizacije bore da

održe korak u promjenjivom krajoliku stvorenom inovacijama u tehnologiji, svijet tehnologije koji se stalno mijenja donosi prijetnje njihovim podacima i ogroman broj podataka je izložen ranjivosti.

Složenost povezanog okruženja nastavlja da se razvija u cyber prostoru, jer potpuno elektronski svijet kreiran međusobno povezanim mrežama nalik fizičkom svijetu, karakterizira ogromna količina podataka. Osnove podataka se kontinuirano kombinuju, povezuju, porede i povezuju sa drugim informacijama dok organizacije pokušavaju da kapitalizuju njihovu vrednost i da ponude nove i poboljšane usluge svojim korisnicima. Količina podataka počinje drastično da raste kako internet stvari postaje stvarnost. Cyber prostor je postao sam po sebi složen za upravljanje i izazovan za obezbjeđivanje. Prijetnje kibernetičkog prostora nastavit će ciljati na najslabije karike u bilo kojem složenom web poslovanju ili bilo kojem vladinom procesu, organizacije i dionici imaju ulogu u cyber sigurnosti i zaštiti infrastrukture i informacija koje kroz nju teku. Prioritet svakog dionika trebao bi biti zaštita interesa svog poslovanja u zaštiti svojih klijenata od cyber kriminala.

Suočavanje sa cyber baziranim i drugim sigurnosnim prijetnjama zasnovanim na mreži nekada je bila tema ograničena na IT odjel u većini kompanija, ali to više nije slučaj (Paul Taylor 2013). Cyber sigurnost je ključno organizaciono pitanje koje se tiče zainteresovanih strana, direktora, menadžmenta i drugih, uključujući revizore. Uz trenutno rastuće tehnološko okruženje, pritisak na cyber sigurnost dolazi iz različitih područja - hakera, aktivista, špijunskih aktivnosti i curenja podataka gdje se podaci ili informacije uzimaju iz organizacije i namjerno ili nehotice dospiju u pogrešne ruke.

Sigurnosni problemi koji utiču na poslovanje su slični širom svijeta. Većina uključuje zaposlenike koji nedužno unose zaraženi osobni mobilni uređaj u korporativnu mrežu ili kliknu na link društvenih medija koji izgleda bezopasno, ali skriva trojanca ili crva koji će potajno ukrasti podatke i novac i potencijalno ostati neotkriven sa ozbiljnim utjecajem na sigurnost zaraženih uređaj (Dmitrij Ajrapetov 2013). Ranjivost cyber sigurnosti u mobilnom uređaju i upotreba ličnih uređaja u poslovanju drastično su porasli jer se svima sviđa pogodnost mobilizacije i ideja mobilnog sistema plaćanja; ovo je učinilo mobilnu platformu privlačnom metom za finansijsku motivaciju cyber kriminala.
Cyber pretnje mogu biti nevidljive, ali uticaji su stvarni, a međusobno povezani sistemi koji su globalno povezani su najranjiviji sistemi. Kako se širi obim informacija koje teku u cyber prostoru, tako se povećava i vrijednost za saradnju, vladu i pojedince širom svijeta. Naši podaci

igraju ulogu u ostavljanju traga u cyber prostoru i ostavljaju nas izloženim cyber prijetnjama. Cyber prostor ima mogućnosti za one organizacije koje žele da profitiraju na online tržištu, ali malo znaju da su te prilike obično tržište za kriminalne aktivnosti, postoji osećaj profesionalizma u cyber kriminalu, što ove aktivnosti čini sofisticiranijim. Zaštita podataka postaje sve važnija. Organizacije, programeri i vlada imaju povećanu odgovornost da osiguraju sigurnost online platformi i back-end sistema, gdje se prikuplja, obrađuje i pohranjuje toliko ličnih podataka.

3.3.3. Upravljanje podacima, politikama i pristupom

U današnjem globalnom, digitalnom svijetu, podaci su najvažnija imovina za preduzeća. „Očuvanje intelektualne svojine, finansijskih informacija i reputacije vaše kompanije je ključni deo poslovne strategije. Ipak, kako raste broj prijetnji i sofisticiranost napada, to je ogroman izazov" (Loveland i Mark Lobel 2012.)

Kompanije se sada moraju braniti od stalno prisutnih cyber napada; prijetnja cyber kriminalaca ili čak nezadovoljnih zaposlenika koji objavljuju osjetljive informacije, oduzimaju intelektualno vlasništvo konkurenciji ili se upuštaju u online prevare (James Kaplan, Shantnu Sharma i Allen Weinberg 2011.).

Od organizacija se traži da se pridržavaju različitih zakona i propisa kako bi poslovale u određenim jurisdikcijama ili u različitim jurisdikcijama. Međutim, kada je u pitanju sigurnost cyber prostora, mehanički pristup usklađenosti ne znači da su pojedinci, organizacije sigurne. Cyber sigurnost je složena i menja pitanja politike; cyber sigurnost to je više od tehničkog problema jer utiče na sigurnost cijele komunikacione mreže. Kreatori politike i zakonodavci igraju ulogu u osiguravanju da propisi štite i čuvaju informacije u mirovanju i u tranzitu.

Pravac razvoja cyber sigurnosti, privatnosti u cyber prostoru i vlasti za zaštitu podataka imaju ulogu u jačanju vrijednosti privatnosti kako bi se osiguralo da politika cyber sigurnosti poštuje prava na privatnost i daje prioritet zaštiti ličnih podataka.

3.3.4. Uloga privatnosti u operacijama cyber sigurnosti

Cilj cyber sigurnosti je bolje omogućiti korisnicima i organizacijama da izraze zaštitu i kontrolu povjerljivosti svojih privatnih podataka čak i kada to odluče - ili kada se od njih traži da ih dijele s drugima putem mreže. Stavovi organizacija i pojedinaca prema privatnosti njihovih privatnih podataka evoluiraju i kao rezultat slučajno povećavaju izazov cyber kriminala. Osnovne prijetnje po kompjuterskoj sigurnosti na koje se ukazuje insajderima uključuju greške, slučajno probijanje, pogrešnu konfiguraciju i zloupotrebu ovlaštenih privilegija, kao i

insajdersko iskorištavanje nedostataka interne sigurnosti. Prema Homeland Security (2009, str. 84) „centralni problem u sigurnosti svjesne privatnosti je napetost između suprotstavljenih ciljeva u otkrivanju i korištenju privatnih informacija“.

Kreatori politike na nacionalnom nivou imaju odgovornost da preuzmu dominantan rizik u formulisanju odgovora na cyber pretnje, nauštrb zaštite privatnosti. U ovoj manifestaciji, politika cyber sigurnosti mogla bi omogućiti ono što Deibert opisuje kao “sekuritizaciju cyber prostora - transformaciju domena u pitanje nacionalne sigurnosti”. To ne znači da napori u cyber sigurnosti ne bi trebali proširiti promatranje na štetu privatnosti pojedinca ili drugih demokratskih vrijednosti. Neophodne provjere i kontrole moraju biti izgrađene tako da odražavaju norme privatnosti odobrene društvu.

Kako pojedinci rastu u broju i postaju sve zavisniji i povezaniji u cyber prostoru, oni se sve više oslanjaju na efektivnu implementaciju cyber sigurnosti od strane organizacija i osjetljivi su na privatnost.

Cyber sigurnost je zajednička odgovornost jer je cyber prostor međusobno povezan i međuzavisan elektronski svijet. Organizacije imaju ulogu da se postaraju da njihove akcije ne unose bezbjednosne rizike u cyber prostor ili da ne poštuju principe privatnosti.

4. POLITIKA CYBER SIGURNOSTI U EVROPSKOJ UNIJI

Cybera sigurnost Evropske unije (EU) je relativno nova oblast, koja se pomaknula od igranja manje uloge podrške u evropskim integracijama u svoju posebnu oblast politike 2013. godine. Rastući od ad hoc skupa mehanizama zaštite jedinstvenog tržišta do potpuno ostvarene agende sa sopstvenim unutrašnjim obrazloženjem, cyber sigurnost je sada centralna za napore EU za integraciju, sa transverzalnim učinkom na većinu drugih oblasti politike. Pokriva niz aktivnosti, uključujući zaštitu kritičnih informacionih sistema i infrastrukture od cyber napada, prevenciju i istragu cyber kriminala i cyber odbranu. Slično tome, u kontekstu trenutne pandemije, upotreba digitalnih komunikacijskih tehnologija se proširila, podižući i profil i važnost cyber sigurnosti u podršci modernom društvenom, ekonomskom i političkom životu. Kako se oslanjanje na digitalne komunikacije povećalo, tako su se pojavile i prilike za aktere da zloupotrebe ove tehnologije za političku i ekonomsku dobit.

Imajući ovu pozadinu na umu, ovaj rad postavlja pitanje je li COVID-19 rezultirao idejnom promjenom u politici cyber sigurnosti EU ili umjesto toga vidimo kontinuitet ideja i politike. Za potrebe ovog rada, predlažemo da kontinuitet uključuje sljedeća tri elementa:

1. idejni kontinuitet - postoji li promjena osnovna filozofija i opravdanje izbora politike cyber sigurnosti EU?,
2. kontinuitet politike - postoji li ponovno orijentacija/prekid postojećih instrumenata?, i
3. kontinuitet upravljanja- da li se oblast upravlja na isti način i da li se održavaju odnosi između različitih aktera prisutnih u ovoj oblasti?

Kroz pristup koji se oslanja i na historijski i na diskurzivni institucionalizam, u ovom dijelu rada se tvrdi da povijesni i diskurzivni kontekst u kojem nastaje i razvija se politika cyber sigurnosti EU direktno oblikuje razvoj same politike, kao i ponašanje aktera prisutnih unutar politike. (Mahoney, J. i K. Thelen, ur. 2010.) Istražujući diskurse u porijeklu politike, u radu se predlaže da je razvoj i formalizacija cyber sigurnosti EU rezultat zavisnosti od idejnog puta zasnovanog na ekonomskim i sigurnosnim razlozima koji su se preorijentisali tokom kritičnih trenutaka. Cyberu sigurnost EU najbolje je shvatiti kao razvoj kroz postupno slojevitost institucija i politika i kroz kritične prekretnice, a ne isključivo kao rezultat bilo kojeg drugog. U radu se zaključuje da, iako je pandemija imala dramatičan utjecaj na svakodnevni život, ona nije rezultirala značajnim diskurzivnim pomakom u cyberoj sigurnosti, već prije jačanju postojećih narativnih trendova.

Konkretno, širenje dezinformacija na internetu dovelo je do “bifurkacije” u razinama povjerenja u različite aktere uključene u pružanje cyber sigurnosti, s platformama društvenih

medija za koje se smatra da ne dijele vrijednosti EU u pogledu slobode izražavanja i štetnog govora, što je pogoršano proliferacijom teorija zavjere povezanih s pandemijom. Ova studija slučaja EU o cyberoj sigurnosti ima za cilj da doprinese historijskoj literaturi o institucionalizmu pokazujući kako se ona može obogatiti kroz angažman s fokusom diskurzivnog institucionalizma na to kako ideje i diskurs olakšavaju institucionalne promjene. (Mahoney, J. i K. Thelen, ur. 2010.) To čini predstavljanjem razvoja cyber sigurnosti EU kroz historiografsku analizu, preoblikovanjem nastanka, formalizacije i trenutnog ubrzanja cyber sigurnosti EU u svjetlu temeljnih filozofija koje oblikuju njene programe i politike, te identificiranjem obrazaca promjene i kontinuiteta.

4.1. Razumijevanje politike cyber sigurnosti EU kroz sočiva historijskog i diskurzivnog institucionalizma

Kako bi se razumjela institucionalna promjena u okviru politike cyber sigurnosti EU, autori predlažu kombiniranje uvida historijskog institucionalizma, posebno elemenata ovisnosti o putu, kritičnih prekretnica i postupnih institucionalnih promjena, s onima novijeg diskurzivnog institucionalizma, odnosno fokusom na uloga ideja i diskursa. Ovaj dio rada objašnjava kako diskurzivni institucionalistički analitički okvir nadopunjuje povijesni institucionalistički materijalistički paket alata kako bi se u potpunosti razumjele ideje prisutne u nastanku i tokom razvoja politike cyber sigurnosti EU, njihovo diskurzivno uokvirevanje i njihovo oblikovanje dizajna i putanje ove politike, kako bi se rasvijetlio utjecaj COVID-19.

Historijski institucionalizam se bavi načinom na koji se institucionalne strukture razvijaju tokom vremena i kako to oblikuje njihove sadašnje skupove i njihovo okruženje. Objašnjava institucionalnu evoluciju prikazujući je kao rezultat „ovisnosti o putu“. (Fahey, E. 2014.) Sadašnje institucije su rezultat prošlih razvoja i političkih odluka, koje razgraničavaju spektar trenutnih i budućih opcija. (Uredba 2019/881, 2019.) Ovo institucionalno nasljeđe, ili „ovisnost o putu“, ograničava institucionalne konfiguracije i preferencije pojedinaca unutar njih. (Kunnathuvalappil Hariharan, N., 2018.) Prema ovom stavu, isti egzogeni fenomen može dovesti do veoma različitog uticaja na slične i uporedive institucije zbog historijskih puteva kojima su te institucije išle. Institucionalne putanje, međutim, mogu pomjeriti putanje u određenim vremenskim trenucima kada dostignu “kritične točke”. Definisano od strane Colliera i Colliera kao periodi značajnih promjena, koji se mogu odigrati drugačije u različitim okruženjima, očekuje se da će utjecaj kritičnih raskrsnica na ovisnost o putanji varirati prema njihovoj dužini, vremenu i efektu (1991.). Kritična tačka ima kapacitet da promijeni putanju institucije tako što će proizvesti novo naslijeđe u obliku novih ideja i prethodnika za donošenje odluka, što će zauzvrat ograničiti buduće ponašanje. (Hoffman, B. L., E. M. Felter, K.-H. Chu,

A. Shensa, C. Hermann, T. Wolynn, D. Williams i B. A. Primack. 2019.) Mi, međutim, tvrdimo da kritični prekretnici sami po sebi nisu u stanju da objasne sve oblike institucionalnih promjena, postupni procesi također igraju važnu ulogu u razumijevanju evolucije politika EU (Schmidt, V. A. 2008.): kritične tačke služe kao prozori mogućnosti za dublje reforme koje proizvode ovisnost o putu, koje uokviruju svakodnevne mikro promjene koje se i dalje dešavaju i da jednakost doprinosi promjeni institucionalnih putanja, iako na manje primjetan način. Kao što će pokazati naredni odjeljci ovog rada, postepene promjene u institucijama EU koje se odnose na cyber sigurnost najbolje se razumiju kroz način „slojavanja“ - gdje se nove institucije dodaju povrh starijih. (Uredba 2019/881, 2019.)

Međutim, da li je moguće u potpunosti razumjeti razloge iza institucionalnih promjena jednostavnim praćenjem evolucije u procedurama, normama, rutinama i konvencijama? Slijedeći korake Schmidtove kritike historijskog institucionalizma (May, AU, 2017.), ovaj rad također tvrdi da iako ovaj pristup nudi važne alate za razumijevanje načina na koji dolazi do promjena, njegovo razumijevanje institucija često ima tendenciju da ignoriše ulogu ideja i njihove diskurzivno uokvirivanje doprinoseći toj promjeni. Previđajući ideje i njihov izraz, historijski institucionalizam je zapravo dao prioritet materijalističkom i determinističkom razumijevanju institucija, fokusirajući se na njihov dizajn, a ne na idejni sadržaj, što rezultira njihovom reprezentacijom kao strukturama u kojima konstrukti značenja agenata igraju ograničenu ulogu.

Možda je moguće identificirati “ovisnost o putu” koja oblikuje putanju politike cyber sigurnosti EU-a, a također bi moglo biti moguće odrediti kritične točke i postupne promjene u ovoj oblasti, ali ako ne otkrijemo ideje koje je čine, način na koji se saopštavaju i prati njihov uticaj, svakako nam nedostaje ključni dio odgovora na slagalicu.

Kako bi se suprotstavio ovom jazu, Schmidt je predložio četvrtu vrstu novog institucionalizma, diskurzivni institucionalizam, koji naglašava da diskurzivno izražavanje ideja ima moć samo po sebi (2008, 2002). Oblikovanjem percepcije agenata o njihovoj društvenoj, političkoj i ekonomskoj stvarnosti, ideje[4] i diskurs[5] su ključni za razumijevanje kako se interesi, vrijednosti i ponašanja razvijaju i zašto se institucije mijenjaju.

4 Za potrebe ovog rada, ideje se podrazumijevaju kao skup rješenja politike koja su ugrađena u sistem uvjerenja i implementirana od strane aktera na pozicijama odlučivanja, koja direktno oblikuju instrumente i rezultate politike, nakon identifikacije političkih problema i otvaranje prozora mogućnosti za institucionalne promjene (Steinmo 2008).

5 Izražavanje ovih ideja, ili diskurs, shvata se kao relacioni sistem označavajućih praksi usmjerenih na datu publiku, bilo da je diskurs pisani, usmeni ili u bilo kom drugom obliku komuniciranja značenja (Torfing 1999).

Analitički okvir koji je stvorio Schmidt za hvatanje uloge ideja i diskursa u institucionalnoj promjeni je stoga posebno koristan za razumijevanje da se kritični prekretnici pojavljuju kao periodi promjena jer su diskurzivno uokvireni kao takvi, te da su ograničenja ovisnosti o putu rezultat naslijeđene ideje i diskursi koji se stalno iznova tumače u svjetlu savremenog konteksta. Prema Schmidtu, da bismo razumjeli kako ideje i diskurs konstituiraju ovisnost o putu i promjenu okvira, moramo dalje istražiti različite uloge koje ideje mogu usvojiti u kreiranju politike. Oni se mogu kategorizirati prema sistemu Matrjoške na tri nivoa, koji karakteriziraju procesi nasljeđa ideja, usklađivanja i koherentnosti. Prva lutka stvara idejnu vanjsku ljusku sastavljenu od "filozofija" - svjetonazora ili ideologija - koje služe kao kapsula za drugu lutku, sastavljenu od "programa" - gdje se filozofije primjenjuju na specifična polja politike i prevode u temeljne principe i strateške vođenje. Treća i najskrivenija lutka odgovara „politikama" koje proizlaze iz praktične primjene filozofija i programa (2008). Ovaj rad predlaže primjenu ovog okvira identificiranjem implicitnih filozofskih ideja koje oblikuju ovisnost i promjenu putanje cyber sigurnosti u EU, kako bi se razumjelo kako su one rezultirale idejno usklađenim programima i politikama, što nam zauzvrat omogućava razumijevanje utjecaja COVID-19 na ovo polje.

4.2. Porijeklo i formalizacija politike cyber sigurnosti EU

Kombinujući historijski institucionalizam sa diskurzivnim institucionalizmom, drugi dio ovog rada će sada istražiti nastanak i formalizaciju politike cyber sigurnosti EU. Koristit će se Schmidtovom idejnom kategorizacijom kako bi se precizirale temeljne filozofije ove politike, pratila je ovisnost o diskurzivnom putu i identificirala kritične točke i postupne promjene koje su oblikovale programe i politike. Predlaže da se put politike cyber sigurnosti EU-a podijeli u dvije glavne faze:

1) geneza (1980. do 2010.) i
2) formalizacija (2010.-2020.).

Svrha ovog odjeljka je objasniti da se odgovor politike cyber sigurnosti EU-a na COVID-19, naime u smislu njenog odnosa s privatnim sektorom, prioriteta u pogledu otpornosti i borbe protiv dezinformacija, te koordinirajuće uloge EU-a, ne može shvatiti kao reakcija do egzogenog šoka, već se prije treba smjestiti u mnogo širi idejni i diskurzivni historijski kontekst.

4.3. Geneza: od očuvanja jedinstvenog tržišta do zaštite građana EU

Početni interes Europske zajednice za cyberu sigurnost 1980-ih bio je duboko usađen u ekonomski pristup koji se odnosi na zaštitu jedinstvenog tržišta u kontekstu novih tehnologija, što bi duboko uticalo na razvoj kasnijih programa i politika, a posebno na njen stav da je cybera sigurnost najbolja upravlja kroz javno-privatna partnerstva. Ova bezbjednosna zabrinutost se

odrazila na diskurse na međunarodnom nivou, sa prijedlogom Savjeta Evrope da se stvori kategorija kompjuterskog kriminala početkom 1980-ih, kao i Organizacije za ekonomsku saradnju i razvoj (OECD) i Grupe osam (G8) inicijative koje preporučuju stvaranje i harmonizaciju evropskog zakonodavstva o kompjuterskom kriminalu sredinom 1980-ih. (Preporuka Komisije 2020/518, 2020.)

Međutim, uprkos dominaciji ovog bezbjednosnog diskursa na međunarodnom nivou, Evropska zajednica, kojoj je nedostajala pravna nadležnost u ovoj oblasti, krenula je drugim putem. Iako možemo uočiti prelazak sa međunarodnog nivoa na evropski u smislu brige o kompjuterskom i mrežnom kriminalu, njegovo uokvirivanje nije bilo ugrađeno u sigurnosnu filozofiju već ekonomsku. Ovaj temeljni diskurs fokusirao se na centralnu ulogu slobodne trgovine i privatne inicijative u donošenju prosperiteta evropskim zemljama, kao i na ulogu Evropske zajednice u regulisanju pravnog okruženja koje omogućava zdravu tržišnu konkurenciju. (Eurofound, 2020.) Informacione i komunikacione tehnologije su predstavljene i kao budućnost jedinstvenog tržišta, ali i kao njegova Ahilova peta, jer bi njihova zloupotreba od strane stranih sila i pojedinačnih kriminalaca mogla ozbiljno potkopati ekonomski razvoj, narušavajući funkcionisanje unutrašnjeg tržišta. (Evropska komisija, 1990.) Ova ekonomska filozofija označila bi početak ovisnosti o putu koji će oblikovati razvoj ovog područja, sa programima i politikama usmjerenim na zaštitu informacionih i komunikacionih tehnologija kao ključnog elementa ekonomskog prosperiteta. (Evropska komisija, 1985.)

Kako je postalo jasno da su kompenzacijski sigurnosni mehanizmi i instrumenti neophodni za zaštitu otvorenih granica jedinstvenog tržišta, sigurnosni diskurs koji proizlazi iz razvoja stuba pravosuđa i unutrašnjih poslova počeo je prožimati pristup EU-a cyberoj sigurnosti. (Verizon, 2021.) Ovo prelijevanje s ekonomskog polja na sigurnosno otvorilo je prozor mogućnosti za prvu kritičnu tačku u putanji cyber sigurnosti, mijenjajući ovisnost usmjerenu na ekonomiju koja je uspostavljena ranih 1980-ih. Mogućnost razvoja evropskih instrumenata, zajedno sa rastućom percepcijom da kompjuterski kriminal predstavlja prijetnju koja se pojavljuje u kontekstu stalne neizvjesnosti, omogućila je da se pojavi nova hibridna filozofija, fokusirajući se na ulogu informacijskih tehnologija u olakšavanju nesigurnosti Europske unije. i njenih građana, i ide mnogo dalje od ekonomskog uticaja. Rezultat je bio hibridni ekonomski/sigurnosni diskurs koji bi omogućio zabrinutostima usmjerenim na sigurnost da oblikuju buduće programe i politike. Sredinom 1990-ih, evropske institucije su već izražavale osjećaj hitnosti u rješavanju ilegalnih i štetnih sadržaja na Internetu (Evropska komisija), kao i

korištenja informacionih tehnologija od strane organiziranog kriminala. (Steinmo, S., K. Thelen, i F. Longstreth, ur. 1992.)

Na osnovu ove hibridne filozofije, i kao odgovor na osjećaj hitnosti, postojao je niz programskih ideja, ili vodećih principa, razvijenih između kasnih 1990-ih i sredine 2000-ih:

1) projekcija EU kao koordinirajući akter koji je dobro pozicioniran da se bavi problemima prekogranične cyber sigurnosti, (Evropska komisija, 1993.)
2) potreba da se fokusira na otpornost kao strategiju zaštite informacijskih mreža i infrastrukture, (Streeck, W. i K. A. Thelen. 2005.)
3) važnost postizanja koherentnost između akcija i instrumenata EU u oblasti koja je posebno raznolika (Evropsko vijeće, 1999.); i,
4) centralni značaj rada sa privatnim sektorom s obzirom na njegovo vlasništvo nad informatičkom infrastrukturom i njegovu percipiranu ekspertizu. (Evropska komisija, 2010a.)

Rezultirajuće politike uključivale su postepeno širenje mreže vrlo različitih mjera, koje jasno rade kroz proces slojevitosti, uključujući uvođenje evropskog sistema upozorenja i informacija (CERT), povećanje istraživačke podrške za informacijsku tehnologiju, ohrabrivanje država članica da usvoje slične norme cyber sigurnosti, stvaranje Evropske agencije za cyberu sigurnost (ENISA) i podizanje svijesti stanovništva o cyber ranjivosti.

Iako je ovo polje evoluiralo kroz proces slojevitosti, gdje su nove ideje, norme i instrumenti postepeno dodavani povrh postojećih, sa jasnom ovisnošću o putu oblikovanom hibridnom ekonomskom/sigurnosnom filozofijom, važnu ulogu su odigrali i eksterni faktori, uključujući događaje i dinamiku politike van ove specifične oblasti. Što se potonjeg tiče, postoji jasna veza između razvoja Trećeg stuba, a kasnije i Područja slobode, sigurnosti i pravde i politike cyber sigurnosti EU, kako u smislu osnovnih filozofija, tako i u smislu prelivanja iz drugih JHA politike. Percepcije kreatora politike o vanjskim događajima također su doprinijele evoluciji ove politike, odnosno rastućem broju cyber napada, kao i terorističkih napada u kojima je informacijska tehnologija igrala važnu ulogu. Slučaj napada u Madridu (2004.) i Londonu (2005.) posebno je važan jer su otvorili prozor mogućnosti za drugu kritičnu fazu u ovoj oblasti. Iako nema promjene na nivou osnovne filozofije, postoji vrlo važan pomak u programskom smislu, opravdan na osnovu nivoa prijetnje, pri čemu se EU kreće od pristupa mekog prava na mnogo formaliziraniji pristup, okarakteriziran obavezujućim instrumentima i stvaranjem

namenske oblasti politike. (Hoffman, B. L., E. M. Felter, K.-H. Chu, A. Shensa, C. Hermann, T. Wolynn, D. Williams i B. A. Primack. 2019.)

4.4. Formalizacija politike cyber sigurnosti EU

Formalizacija cyber sigurnosti kao posebne oblasti politike počela je 2010. godine objavljivanjem Strategije unutrašnje sigurnosti. (Evropska komisija, 2010b.) Inicijalni prijedlozi u oblasti cyber sigurnosti bili su po prirodi postupni, a predložene su reforme za dopunu inicijativa koje su se razvijale u kontekstu Digitalne agende za Evropu. (Evropska komisija, 2010b.) Ovaj program imao je za cilj rješavanje krhkosti ekonomija EU kroz mjere za olakšavanje stvaranja „digitalnog" jedinstvenog tržišta. (Evropska komisija, 2010b.) Povjerenje i povjerenje u internetsko okruženje identificirani su kao problem politike koji treba riješiti, ali dok je povijesno ovo bilo uokvireno gotovo isključivo u smislu prijetnji od cyberog kriminala, vidimo efekat "slojevitosti" jer Digitalna agenda ističe da cyber kriminal nije samo pitanje ekonomski vođenih aktivnosti, ali može biti i političko, diskurzivno koristeći primjer cyber napada na informacijske sisteme u Estoniji, Litvaniji i Gruziji koji zahtijeva pristup cyberoj sigurnosti, a ne isključivo fokus na cyber kriminal. (Evropska komisija, 2010b.)

Strategija unutrašnje sigurnosti uključila je jačanje postojećih agencija kao što je Europol s proširenim nadležnostima u oblasti cyberog kriminala kroz Evropski centar za cyberi kriminal (EC3) i povećano javno-privatno partnerstvo kroz ENISA-u za razvoj standarda najbolje prakse za otpornost na cyber napade. (Evropska komisija, 2010a.) Osnovni idejni okvir EU kao koordinatora, sa javno-privatnom saradnjom predvođenom ekspertima, i naglaskom na otpornosti i koherentnosti politika evidentan je u ovim dokumentima. Umjesto da predstavlja kritičnu tačku, to je postupni pristup formalizaciji politike cyber sigurnosti, koji radi unutar postojećih institucionalnih struktura kako bi se olakšalo širenje akcija, umjesto da ih radikalno preispituje.

Do 2013. ovaj prijedlog je postao potpuna, samostalna politika. Zanimljivo je da je rezultirajuća Strategija cyber sigurnosti spojila tri bivša stuba EU u sveobuhvatnom pristupu pitanjima internetske sigurnosti, oponašajući njenu strukturu stuba kroz mjere koje imaju za cilj zaštitu unutrašnjeg tržišta borbom protiv cyberog kriminala, osiguravajući otpornost mrežnih i informacijskih sistema i kritičnih informacija Infrastrukture u okviru cyber sigurnosti, kao i uvođenje koncepta cyber odbrane u kontekstu Zajedničke sigurnosne i odbrambene politike. (Evropska komisija, Visoki predstavnik Evropske unije za vanjske poslove i sigurnosnu politiku, 2013.) Strategija cyber sigurnosti nastavlja ovaj postupni pristup slojevitosti, međutim,

uspostavljanjem proširenih nadležnosti za agencije kao što je ENISA, poziva na pojačanu suradnju između nacionalnih vlasti, pružatelja internetskih usluga iz privatnog sektora i stručnjaka za sigurnost, te povećanu koordinaciju između nacionalnog i europskog nivoa kao i između agencija EU kako bi se osigurala koherentnost. U tom pogledu, osnovni idejni okvir ostaje dosljedan, s naglaskom pretežno na važnosti ekonomije EU-a uz izvjesno priznanje neekonomskih pokretača cyberih napada, uz kontinuiranu ovisnost o putu zasnovanoj na idejama koordinacije, koherentnosti i uloga tehničkih stručnjaka kao "rješavača problema". Kao rezultat toga, iako vidimo uspostavljanje samostalne evropske strategije cyber sigurnosti, čini se da to nije rezultat prepoznatljivog egzogenog šoka, već endogene promjene kao rezultat ubrzanja i produbljivanja trendova u okruženju idejnog kontinuiteta.

4.5. Platforme društvenih medija, dezinformacije i gubitak povjerenja

Dok je period 2010-2016 predstavljao period relativnog kontinuiteta, period 2016-2019 može se smatrati periodom idejnog poremećaja. Visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku i Komisija objavili su u aprilu 2016. godine Komunikaciju o hibridnim prijetnjama. (Evropska komisija i visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku, 2016.) Uokvireno je da se EU suočava sa promijenjenim pejzažom prijetnji, sa zamagljenim linijama između države i nedržave, te ekonomski motiviranim i politički motiviranim napadima. Dok osnovna filozofija rizika formulisanja programa otpornosti ostaje, narativ o prirodi tih prijetnji je onaj u kojem je razlika između unutrašnje i vanjske sigurnosti manje značajna, što rezultira da saradnja između visokog predstavnika i Komisije postaje ključna. Konkretno, Zajedničko saopštenje naglašava da je rastući rizik da se zlonamjerni akteri upuštaju u kombinacije ekonomskih, tehnoloških, vojnih i diplomatskih aktivnosti kako bi narušili stabilnost država i njihovih ekonomija "dok ostaju ispod praga formalno objavljenog rata". (Evropska komisija i visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku, 2016.)

Idejni kontinuitet i zavisnost od putanje očigledni su u odjeljku Komunikacije o cyberoj sigurnosti, koji naglašava koordinaciju, koherentnost i otpornost, uz pojačanu ulogu nacionalnih vlasti koje sarađuju s privatnim sektorom kako bi osigurale otpornost informacijskih sistema i kritične informacijske infrastrukture. (Evropska komisija i visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku, 2016.) Ovdje možemo vidjeti da je naglasak i dalje na saradnji između stručnjaka iz javnog i privatnog sektora, bez izrazite promjene u filozofiji ili programu, i politika koje se mijenjaju putem postepenog slojevanja; Uspjeh ENISA-e i suradnje privatnog sektora koristi se kao legitimna osnova za proširenje

mandata ENISA-e i pružanje „tržišnih" rješenja kroz Zakon o cyberoj sigurnosti EU. (Madrigal, A.C., 2018.)Prema ovom zakonu, „stručnjaci" za cyberu sigurnost se dovode u regulatornu sferu davanjem akreditacije i sertifikacije za ICT proizvode, procese i usluge, na osnovu osnovne filozofije da su stručnjaci u najboljoj poziciji da nadgledaju ove aktivnosti.

Dezinformacije se, međutim, predstavljaju kao novi oblik prijetnje, a društveni mediji kao ključni kanal za širenje. Iako dezinformacije same po sebi nisu nova pojava, one se pomjeraju s periferne brige EU na središnju poziciju u njenim inicijativama usmjerenim na sigurnost, u početku zbog ruske ekspanzije svojih kampanja dezinformacija iz Rusije i njene periferije u prvom i drugom periodu faze da bi se zatim fokusirali na poremećaje i destabilizaciju u Evropi 2014., što se poklapa sa njenim vojnim upadom u Ukrajinu. (Treverton, G. F., A. Thvedt, A. R. Chen, K. Lee i M. McCue. 2018.) Europsko vijeće je izrazilo posebnu zabrinutost zbog dezinformacija na internetu u ovom kontekstu, pozivajući "visokog predstavnika, u suradnji s državama članicama i institucijama EU, da do juna pripremi akcioni plan". (Evropsko vijeće, 2015.) Upravo ovdje spajanje pristupa koji dolaze iz historijskog i diskurzivnog institucionalizma postaje vrlo relevantno; dok postoji kontinuitet koji proizlazi iz povijesnih ovisnosti o ulozi privatnih aktera u upravljanju cyberom sigurnošću zasnovanom na razumijevanju stručnosti i usklađenih interesa, mi vidimo pukotinu kao rezultat egzogenog šoka koji je rezultat percipiranih informacijskog rata koji vodi Rusija. U smislu diskurzivnog institucionalizma, ovaj raskid stvara kritičku tačku ideje, u kojoj je način na koji se ti privatni akteri shvataju podložan divergenciji između onih aktera koji dijele interese EU (uključujući pružaoce sigurnosnih rješenja CII) i onih za koje se smatra da nisu da dijele iste interese, koji uključuju određene platforme društvenih medija.

Dezinformacije postaju sve istaknutije u sigurnosnom programu Komisije, jer se identificiraju kao izvor rastuće nestabilnosti u EU, kao i da predstavljaju prijetnje za efikasno kreiranje politika u oblastima kao što su zdravlje i klimatske promjene. (Evropska komisija, 2018c.)Kako navodi Komisija, "dezinformacije narušavaju povjerenje u institucije i digitalne i tradicionalne medije i štete našim demokratijama ometajući sposobnost građana da donose odluke na temelju informacija" (Evropska komisija, 2018c.), a posebno se izdvajaju platforme društvenih medija - zbog toga što „nije proporcionalno djelovao, ne ispunjavajući izazove koji predstavljaju dezinformacije i manipulativno korištenje infrastrukture platformi". (Evropska komisija, 2018c.) Ova komunikacija je skoro odmah uslijedila nakon otkrića "Cambridge Analytica", u kojoj je Facebook dozvolio "prikupljanje" podataka miliona korisnika. Prikupljene informacije korištene su u predizbornoj kampanji Donalda Trumpa, kao i Leave.eu u kampanji za

referendum o Bregzitu, što se smatra jednom od najvećih zabilježenih povreda podataka. Nadalje, podaci do kojih je došla Cambridge Analytica bili su umiješani u razvoj ciljanih kampanja dezinformacija koristeći konspirativne ideje osmišljene da služe interesima ovih kampanja. (Streeck, W. i K. A. Thelen. 2005.)Dok je Zuckerberg priznao ovo „kršenje povjerenja“, kreatori politike su izrazili svoje nezadovoljstvo nespremnošću Facebooka da se efikasno bori protiv širenja dezinformacija na svojoj platformi, kao i ponovljenih odbijanja da prisustvuju saslušanjima. (Wolff, S., A. Ripoll Servent i A. Piquet. 2020.) Zuckerberg je prisustvovao saslušanju u Evropskom parlamentu nakon skandala Cambridge Analytica, gdje su zastupnici u Evropskom parlamentu ukazali na dubok skepticizam u pogledu Zuckerbergove posvećenosti borbi protiv dezinformacija. (Madrigal, A.C., 2018.) U središtu ovog sve dubljeg nepovjerenja je percepcija među akterima u EU da mnoge platforme društvenih medija sa sjedištem u SAD-u ne dijele vrijednosti EU kada je u pitanju sloboda izražavanja, pri čemu Zuckerberg podržava “tehno-libertarijanske” ideale i navodi Evropskom parlamentu da Facebook ne bi trebao regulirati šta je istina ili ne, što predstavlja filozofski ideal da bi svaki politički govor trebao biti dopušten uz zastupljenost pluraliteta stavova. (Lischka, J. A. 2019.) Posebno opasan oblik dezinformacija koji se širi preko Facebooka, navodno na osnovu pluraliteta mišljenja, je onaj “anti-vaksera”, koji kritiziraju (često na osnovu teorija zavjere i pogrešno predstavljenih naučnih studija) savremene programe vakcinacije, koji su povezan sa povećanom transmisijom bolesti kao što su boginje. (Hoffman, B. L., E. M. Felter, K.-H. Chu, A. Shensa, C. Hermann, T. Wolynn, D. Williams i B. A. Primack. 2019.) Ovakav pristup govoru se ne doživljava kao usklađen sa principima izražavanja EU, u kojima je govor koji se smatra aktivno štetnim, kao što je govor mržnje ili veličanje terorizma, eksplicitno nezakonit i treba ga aktivno regulirati. (Mahoney, J. i K. Thelen, ur. 2010.) Ova percepcija rezultirala je odlukom Komisije da predloži Uredbu kojom se od društvenih medija zahtijeva uklanjanje materijala za koji se smatra da predstavlja širenje materijala koji promovira terorizam. (Evropska komisija, 2018a.)

Sve više vidimo, kao rezultat ove promjene odnosa povjerenja, odgovarajuću promjenu u osnovnoj filozofiji u vezi sa odnosom između javnih i privatnih aktera, što utiče na ideje programa i politike. Percepcija EU o demokratiji i ulozi privatnih aktera u njoj podložna je preorijentaciji; dok su neki privatni akteri pouzdani partneri u cyberoj sigurnosti i za koje se vjeruje da dijele vrijednosti EU-a, platforme društvenih medija se sve više postavljaju kao dio problema, a njihovi operateri u privatnom sektoru ne dijele te iste vrijednosti. Na nivou politike, ovo se odražava u diskursu koji ove platforme više ne stavlja u središte kreiranja politike kao kod drugih “stručnjaka” za cyberu sigurnost, već radije kao agente koje treba regulisati kroz

Kodeks prakse koji je izradila Komisija za borbu protiv dezinformacija u onlajn okruženje. (Evropska komisija, 2018a.) Komisija je 2019. izričito navela da će 2020. godine izvršiti reviziju efikasnosti platformi društvenih medija u primjeni Kodeksa prakse, a ukoliko utvrdi da je usklađenost nezadovoljavajuća, razmotrit će alternativne načine rješavanja ovog problema politike, uključujući regulatorni nadzor. (Evropska komisija, 2018a.)U tom pogledu, stoga, idecionalna promjena može se identificirati u tome kako se razlikuju privatni akteri; oni kojima se vjeruje i koji učestvuju u mreži upravljanja, i oni kojima se manje vjeruje, i kao rezultat toga više nisu dio te mreže, već podležu regulatornom nadzoru.

Digitalne tehnologije zauzele su vodeću poziciju u politici pod novim predsjedavanjem Komisije, a jedan dio dnevnog reda Komisije pod nazivom Oblikovanje digitalne budućnosti Europe. (Evropska komisija, 2018c.) Odjeljak dokumenta fokusiran na cyber sigurnost predstavlja postojeće trendove koji su prethodno identifikovani iu skladu sa dominantnom idejnom filozofijom, u kojoj je prisutna neophodnost suočavanja sa rizicima i stručnost privatnog sektora; predloženi program je proširenje marketinga proizvoda cyber sigurnosti i stvaranje jedinstvenog tržišta za cyberu sigurnost, uz angažman sa stručnjacima iz privatnog sektora i uspostavu zajedničke jedinice za cyberu sigurnost kako bi se olakšala kohezija i koordinacija. (Evropska komisija, 2020c.) Ova ideološka zavisnost i kontinuitet je takođe demonstrirana u programima politike koji su povezani sa ovom agendom, uključujući Evropsku strategiju za podatke (Evropska komisija, 2020c.) i Novu industrijsku strategiju za Evropu, koja predlaže povećan angažman privatnog sektora u pravilima cyber sigurnosti za 5 G. (Evropska komisija, 2020c.) Bijela knjiga o umjetnoj inteligenciji sadrži odjeljak o korištenju AI u kontekstu cyber sigurnosti, ponavljajući važnost javno-privatne saradnje između stručnjaka za umjetnu inteligenciju i ENISA-e u ovoj oblasti, te mogućnost novih proizvoda za cyberu sigurnost koji proizlaze iz razvoja ovih tehnologija. (Evropska komisija, 2020c.) Dezinformacije se, međutim, ne pominju u kontekstu podataka ili dokumenata industrijske strategije. Umjesto toga, dezinformacije su drugačije uokvirene u Oblikovanju digitalne budućnosti Europe, gdje je naglasak stavljen na rizik za demokraciju od dezinformacija i potrebu za transparentnošću u vezi s manipulacijom informacijama na internetu, pri čemu Komisija predlaže Akcioni plan za demokratiju. (Vijeće Evropske unije, 2020c.) Dok se napadi na informacijske sustave i kritičnu informacijsku infrastrukturu predstavljaju kao prijetnje cyberoj sigurnosti, dezinformacije i manipulacija informacijama na tim sistemima ne predstavljaju se samo kao prijetnja cyberoj sigurnosti već i kao prijetnja temeljnom poretku i vrijednostima EU-a. Kao što će biti razmotreno u sljedećem odjeljku, ovo su ideje koje je sadašnja pandemija ojačala, a ne osporila.

4.6. Nove inicijative u politici cyber sigurnosti

4.6.1. Politike cyber sigurnosti

Cyber sigurnost se odnosi na mjere, tehnologije ili tijelo koje se koristi i postavlja za zaštitu programa, mreža i računara od napada ili neovlašćenog pristupa koji su obično za eksploataciju sistema. Poznata je i kao elektronička ili tehnološka sigurnosna informacija. Statistike pokazuju da Sjedinjene Američke Države troše više od 12 milijardi godišnje na cyber sigurnost u zemlji i upozoravaju na sigurnosne napade. Napadi na cyber sigurnost su klasifikovani u tri glavne grupe koje uključuju; Cyber kriminal koji uključuje grupe ljudi koji napadaju i ciljaju sistem radi finansijske svrhe ili dobiti. Cyber rat koji je uvijek politička i socio-kulturna tortura i posljednji oblik cyber napada je cyber teror koji obično prekida rad kompjuterskih sistema i programa izazivajući napad panike kod članova društva, obično pokriva veću populaciju. Napadači koriste različite metode za hvatanje i kontrolu računala putem virusa i crva. Ove tehnike oštećuju sistem i kompjuterske fajlove, na primjer kada neko vidi poslatu poruku ili e-poruku koja sadrži prilog kada se preuzme misleći da je to legitimna datoteka, ali sadrži viruse koji pokreću sve datoteke i programe u računarskom sistemu.

Cyber kriminal je u svijetu već vijekovima i prijavljen je u različitim dijelovima svijeta. Postupno je kompliciran i sofisticiran otuda i sigurnost iza toga. Morrisov crv koji je bio najstariji i prvi crv kojeg je stvorio naučnik Robert Morris. Ovo je bio smrtonosni virus koji se brzo širio u kompjuterskim sistemima i uglavnom je oštetio internet jer nije bio toliko razvijen koliko sadašnji internet. Morrisov crv je zabilježen kao najsmrtonosniji napad svih vremena. Ovaj cyber kriminal dovodi do izuma različitih sigurnosnih mjera, na primjer, osnivanja tima za kompjuterske hitne reakcije (CERT) koji je bio zadužen za svu sigurnost i hitne slučajeve prijavljene o cyber napadima širom svijeta. Razvili su se različiti virusi koji su zarazili milione personalnih računara. Porast kompjuterskih virusa dovodi i do izuma antivirusne tehnologije koja je bila olakšanje za ljude u različitim dijelovima svijeta. Većina ovih virusa je napala finansijske sisteme, a imali su i pozitivne i negativne uticaje na ljudsku populaciju, na primjer, podstakli su kompjutersku svjest da ne otvaraju nijednu e-poštu ili datoteku od nepoznatog pošiljaoca ili izvora i ako je postojala bilo kakva prijetnja onda bilo ko mogao prijaviti zaustavljanje stvari kako bi se spriječilo širenje virusa.

Cyber zločini su postali napredni tokom godina kada su sada kreditne kartice i pljačka novca postale ogroman negativan uticaj na sigurnost, i tada su stvari postale ozbiljne u pogledu sigurnosti. Ciljanje kreditnih kartica u kompanijama postalo je sofisticirano i napredno,

uzrokujući ozbiljne gubitke posebno u Sjedinjenim Američkim Državama gdje je izgubljeno više od 200 milijardi dolara tokom napada koji se bilježe godišnje. To je dovelo do dugova bilo na ličnom nivou ili u cijeloj zemlji. To također dovodi do ostavki izvršnih direktora različitih kompanija i javnost više nije mogla vjerovati finansijskim kompanijama s tim sredstvima zbog nesigurnosti i gubitka.

Postoji različita važnost cyber sigurnosti. Jedan od uobičajenih je pronalazak antivirusne tehnologije koja se donosi u različitim softverima, na primjer, onima koji se koriste u računarima i pametnim telefonima. Preuzima se i instalira, a zatim testira kako bi se skenirao sistem kako bi se očistio operativni sistem i na računarima i na pametnim telefonima. Bilo koja osoba može upravljati antivirusnom aplikacijom, a od svakoga se traži da poduzmu različite mjere prema navodima Državne sigurnosti u Sjedinjenim Državama u vezi s prijetnjama cyber zločina. Neke od ovih mjera uključuju; ne dostavljajući nikakve lične podatke ili reference nepoznatom primaocu putem e-pošte ili bilo koje druge stranice. Cyber napadači su veoma upućeni u kompjuterske sisteme i u određenoj mjeri mogu doći u ruke bilo čijih detalja. Savjetuje se da ignorišete sve nepoznate poslane mejlove ili poruke koje obično dolaze od lažne agencije. Druga mjera je ažuriranje vašeg operativnog sistema i antivirusa. Postavljanje naprednije lozinke je također važna mjera koju treba uzeti u obzir, jer se savjetuje izbjegavanje jednostavnih lozinki jer je sigurnosnu lozinku uvijek teže probiti. Napadači na cyber sigurnost obično ciljaju na pojedince gdje ljudi otvaraju nove račune i preduzeća koja uključuju snimanje ličnih podataka.

Razvoj različitih sigurnosnih cyber kompanija. Takve kompanije se sastoje od različitih struktura i odjela sigurnosti koje čine profesionalci i visoko obučeni zaposlenici i poslodavci. Ove kompanije stvaraju svijest i oglašavaju pozitivne mjere o tome kako zaštititi naše sisteme od bilo kakvih hakova ili napada. Važno je imati na umu ove reklame i primijeniti ih u praksi kako bi bili sigurniji. U slučaju pokretanja posla, bilo ličnog, porodičnog, institucije ili organizacije: osiguravajuća društva uzimaju, na primjer, naprednu sigurnost u svakom slučaju gubitka i partnerstva s različitim kompanijama za cyberu sigurnost, bilo lokalno ili međunarodno. (Arora, A., Nandkumar, A. i Telang, R., 2006.) Kompanije pružaju podršku odgovarajućim organizacijama. Uspon tehnologije koji većina kompanija koristi je računalstvo u oblaku gdje se pohranjuju i uglavnom osiguravaju velike informacije.

Koliko god je cybera krađa uobičajena u IT društvu, onda je potrebna odgovarajuća obuka zbog evolucije informatike i računarskih škola u kojima su učenici opremljeni naprednim znanjem o

tome kako se uhvatiti u koštac sa bilo kojim cyber kriminalom kako bi zaštitili ljude u društvu i ovo može biti olakšanje za sve. Nakon obuke se mogu zaposliti u IT kompanijama.

Većina ideja je implementirana i podržana od strane vlasti drugih zemalja i uvjeravam da ako ih sve provedemo u praksi, cyber napadi više neće postojati. Vjerujem da postoji rješenje za svaki problem i cyber maltretiranje ne bi trebalo biti jedna od naših prijetnji. Odvojili smo visoko obučeno osoblje iz tajnih službi, FBI-a, CIA-e i domovinske sigurnosti. Oni će biti u potpunom pregledu svih internet servera u zemlji, nadgledajući svaki kompjuterski sistem u školama, organizacijama, kompanijama i još više u vladi. Oni će vršiti redovne ankete u sistemima i uvjeravam vas da će svi ovi kriteriji o kojima ću s vama razgovarati biti uspješni.

Za uspješno zaustavljanje cyber napada određuju se sljedeći kriteriji.

1) Održavanje operativnih sistema za samostalan rad - U različitim organizacijama, operativni sistemi računara su stavljeni da rade zajedno, na primjer, informacije kroz poslovni operativni sistem prolaze kroz sistem organizacionog rasporeda koristeći internet. Svaki operativni sistem na svim kompjuterskim serverima ne treba kombinovati već im omogućiti da rade nezavisno na svakom nalogu. Ovu grešku obično ne otkrivaju razne kompanije, a ona uzrokuje curenje informacija hakeru. Internet, bilo eksterni ili interni, trebao bi biti visoko osiguran kroz upravljanje lozinkom koja se ne može hakovati. Ove veze su obično skrivene, ali dobro obučeni cyber haker koristi takve prostore da uđe u sisteme i uzrokuje drastičnu eksploataciju vladinih ili industrijskih resursa što dovodi do ogromnog gubitka. Rješenje za ovu grešku je redovna procjena u operativnim sistemima računara tako što će se uveriti da su računarski operateri nezavisni od servera, a da su internetska vlakna i konekcije visoko zaštićeni.

2) Implementacija mreže segmenta i aplikacija firewall-a - Ovo uključuje klasifikaciju podataka u određene grupe i davanje strogih mjera za programe podataka koji sadrže vrijedne informacije. To se radi kada su različite mreže izolirane u svojim procesima. Štaviše, zaštitni zid je filtrirani softver koji kontroliše dolazne i odlazne informacije koje se prenose do operativnih sistema servera. Firewall je važan na način da smanjuje kanale na kojima se prenose različite formacije u operativnim sistemima računara. Na ovaj način postoje manje ili nikakve šanse da cyber napadač pristupi bilo kojoj datoteci ili dokumentu u operativnom sistemu putem interneta. Prisustvo zaštitnog zida i stvaranje

granične mreže je sigurniji način da se osiguraju operativni sistemi i ovlašćuje vladu ili bilo koju organizaciju da otkrije bilo kakvo hakovanje i razvija zaštitne mjere.

3) Upotreba zaštićenih tehnika daljinskog pristupa - Ovo je takođe jedno od sredstava za zaštitu operativnih sistema korišćenjem virtuelne privatne mreže (VPN). Tehnika (VPN) je daljinski osigurana i šifrirana kako bi se osigurale interne i eksterne informacije koje se prenose s interneta. Korisnici ličnih računara mogu pristupiti dokumentima, datotekama i programima putem interneta bez ikakvih prijetnji zbog dostupnosti VPN-a. Svi računari i operativni sistemi su obezbjeđeni preko virtuelne privatne mreže. Šifrirani podaci mogu otkriti bilo koji oblik prijetnje, bilo interne ili eksterne. Svi fajlovi i programi u operativnim sistemima su šifrovani ako postoji bilo kakav oblik hakovanja, pa se sve informacije čuvaju u računaru bezbjedne i zdrave.

4) Upotreba jakih naprednih lozinki - Ovo je jedno od uobičajenih sredstava sigurnosti. Statistike pokazuju da je većina zaposlenih u Sjedinjenim Državama komore kroz koje hakeri pronalaze priliku za napad. Neki od radnika u kompanijama ili čak u vladi postavljaju jednostavne lozinke u svoje softvere koje cyber lopov lako pogađa, navodeći ga/nju da se prijavi na svaki operativni sistem što dovodi do eksploatacije resursa. Lozinke bi trebalo da budu duže jer što su duže lozinke uvijek one jače. Dobra lozinka treba da ima najmanje osam znakova i velikih i malih slova koje je nemoguće pogoditi. Kada se novi softver ili aplikacije preuzmu i ažuriraju, prethodnu ili zadanu lozinku treba promijeniti i kreirati nove kako bi se osigurala odgovarajuća sigurnost.

5) Stvaranje i implementacija svijesti koja uključuje cyber zaštitu - Zaposleni u organizaciji i studenti u različitim institucijama za učenje, na primjer, IT treba da imaju široke informacije i da budu uključeni u odgovarajuću obuku od strane profesionalaca o načinima da osiguramo naše internet i kompjuterske sisteme za borbu protiv cyber napada. Cyber sigurnost je proširenо polje gdje se neki aspekti moraju uzeti u obzir kao društveni inženjering, posebno phishing; Ovo uvijek koristi cyber napadač putem e-pošte ili telefonskih poziva, a također pokušava doći do ličnih podataka od ljudi kroz vođenje lažnih seminara na internetu koristeći nepoznate naloge gdje od vas traže vaše podatke i informacije i čim dobiju ono što žele oni neće ponovo komunicirati. Zaposleni su također prisiljeni obavljati neke neželjene zadatke poput preuzimanja kontaminiranih datoteka ili plaćanja određene naknade na lažni račun gdje morate unijeti svoje podatke uključujući lozinku i broj bankovnog računa. Tokom obuke, poslodavcima i studentima

se savjetuje da se prijave na sumnjive internet stranice kako bi otkrili bilo kakvu prijetnju. Uz dobru obuku i svijest, zaposlenima se daje zadatak da osiguraju da se u vladi ili organizaciji ne otkriju cyber napadi.

Tokom godina, mjere cyber sigurnosti su evoluirale sa nižih nivoa na viši nivo. Trenutne vladine politike koje su određene za zaustavljanje cyber kriminala su skoro slične prethodnim mjerama, na primjer, prethodne politike su uključivale mrežne implementacije gdje su operativni sistemi računara bili povezani sa serverima nezavisno i dozvoljeno im je da se povežu na internet koji kontrolišu operativni sistem, a trenutno isto je i dalje uključeno. Mrežni segmenti i zaštitni zidovi su povezani nezavisno kako bi se osiguralo da nema informacija; fajlovi ili aplikacija procure u ruke hakera. Ranije je postojala upotreba lozinki za zaštitu aplikacija računarskih sistema gdje su preporučivali jaču lozinku koju cyber napadač nije mogao da pogodi; isto kao i trenutno gdje se čak i na stranicama koje su ulogovane daju instrukcije koje pokazuju da lozinka treba da se sastoji od malih i velikih slova i ne smije biti manja od 8 karaktera.

Trenutne politike uključuju praćenje internetskih veza i redovno provođenje procjena na web stranicama za koje se sugerira da predstavljaju prijetnju vladi. Ove procjene su uključivale provjeru operativnih sistema i intervjuisanje zaposlenih u svim sumnjivim aktivnostima koje su takođe slične prethodnim politikama za zaustavljanje cyber hakovanja. Procjene su također obavljene kako bi se osiguralo pravilno korištenje resursa koje je obezbijedila vlada ili organizacija koja sprječava bilo kakvo curenje informacija. I prethodna i sadašnja politika su iste, ali su se u određenoj mjeri i razlikovale o čemu će biti riječi u sljedećem članku.

Koliko god da su trenutne politike slične prethodnim politikama, one se takođe razlikuju u različitim djelovima od operativnog sistema do promjena napravljenih u praćenju softvera na računaru. Jedna od razlika je u tome što se trenutno provodi odgovarajuća obuka i svijest kako bi se procijenila rješenja cyber napada. Polaznici su opremljeni širokim znanjem o različitim kompjuterskim softverima i sposobni su da upravljaju prijetnjom ako se ona dogodi dok su prethodne politike redovno izazivale cyber napade jer zaposleni nisu bili adekvatno obučeni i izostanak nestručnih ureda koji nisu davali odgovarajuće ideje boriti se protiv cyber prijetnji i cyber napada. (Arora, A., Nandkumar, A. i Telang, R., 2006.) Druga razlika između ovih politika je ta što su trenutne politike napredne gdje postoji evolucija različitog softvera poput antivirusnih aplikacija koje variraju od tipa pametnih telefona do elektronske aplikacije. Antivirus je trenutno ažuriraniji od prethodnog koji trenutno može skenirati telefon ili računar

kako bi otkrio bilo kakvu umiješanost u cyber napad uništavanjem virusa u datotekama, pa čak i e-mailovima.

Evolucija tehnologije mora dovesti do smanjenja cyber hakovanja, a to je bilo olakšanje za ljudsku populaciju. Ljudi sada mogu vjerovati osiguravajućim kompanijama i bankarskim organizacijama jer su angažovali profesionalce da nadziru njihove operativne sisteme i kompjuterizirani sigurnosni softver do nivoa bez ili minimalne prijetnje maltretiranja i napada cyber hakiranjem. (Arora, A., Nandkumar, A. i Telang, R., 2006.) Ovi profesionalci su visoko obučeni i osiguravaju da kompanije ili organizacije budu više upozorene na bilo koju cyber prijetnju. Prijavljeno je manje slučajeva, a hakeri su podvrgnuti zakonu na sudu i optuženi prema vrsti zločina. Posljedice koje su date cyber kriminalcima bile su prijetnja ostalim cyber napadačima zbog straha da će biti uhvaćeni. U posljednjih pet godina nije zabilježen nijedan cyber hakiranje, već samo neki manji slučajevi cyber maltretiranja koji se obično dešavaju na stranicama društvenih medija poput Facebooka i Instagrama. Ove stranice se sastoje od velikog broja ljudi širom svijeta, a savjetuje se da komunicirate samo s nekim ko vam je poznat kako biste izbjegli slučajeve hakovanja i cyber maltretiranja.

Upoređujući sigurnosne politike Sjedinjenih Američkih Država i politike Evropske unije, postoje slične, a također i različite. Evropska unija ulaže većinu svojih finansija u razvoj organizacija za cyberu sigurnost stvaranjem partnerstva sa međunarodnim kompanijama i državama koje održavaju sastanke i dijele ideje o tome kako razviti cyber sigurnost. (Arora, A., Nandkumar, A. i Telang, R., 2006.)
Ovo nije uobičajeno u organizaciji Sjedinjenih Američkih Država; po mom mišljenju, trebalo bi da uključimo i međunarodne odnose sa drugim povezanim kompanijama za cyber sigurnost. Evropska unija ima drugačija pravila i propise koji regulišu organizacije koje daju slobodu ljudskoj populaciji, razvoj cyber industrijskih resursa i pobunu protiv cyber sigurnosti što je takođe ista strategija u Sjedinjenim Američkim Državama gdje ne samo da imamo pravila i regulative, ali i posljedice cyber kriminala.

4.6.2. Da li je cyber sigurnost nacionalni prioritet ili poslovno pitanje?

Bilo je komplikovanih debata širom svijeta da li bi cyber sigurnost trebala biti odgovornost vlade ili bi to trebala biti odgovornost ličnih kompanija, mislim da bi obje strane trebale učestvovati u zaustavljanju cyber kriminala i napada. Na primjer, vlada bi trebala obezbijediti adekvatne sigurnosne resurse ličnim kompanijama ljudi jer kompanije sadrže lične podatke većeg broja ljudi u zemlji. Lične kompanije i vlada treba da rade ruku pod ruku ili zajedno kako

bi razgovarali o mjerama i politikama koje će se koristiti u odbrani zemlje od cyber napada. Još jedan razlog zašto bi trebalo da rade zajedno na zaustavljanju cyber napada je taj što bi vlada trebalo da izgradi institucije za obuku u kojima će unajmiti profesionalne službenike za obuku zaposlenih koji će kasnije raditi u ličnim kompanijama koje se bave bezbjednošću ljudi. Polaznici bi trebali naporno raditi da bi dobili diplomu ili bilo koji viši dokument da bi se zaposlili u kompaniji, kada se jednom zaposli u ličnoj kompaniji, tada se pravila i propisi moraju poštovati.

Zbog konkursa raznih organizacija i kompanija, država bi nezaposlenim mladima u zemlji trebalo da obezbijedi mogućnost zapošljavanja. Nedostatak zaposlenja u zemlji dovodi do nerada gdje su mladi pod utjecajem uzimanja droge, pljačke, a neki od njih uzimaju i titulu cyber hakera. Mnogi mladi u zemlji imaju diplome, ali nemaju zaposlenje. Nalazite ih samo prikovanima za društvene mreže i ne rade ništa što bi izazvalo cyber maltretiranje. Oni misle da je to zabavno, ali mnogi ljudi koje se maltretiraju su jako pogođeni, a neki od njih počine samoubistvo jer su možda njihovi lični podaci ili detalji procurili u javnost, a neke od tih informacija su tajne. Da bi sve ovo zaustavila, vlada treba da se pobrine da svi mladi prolaze obuku u različitim kompanijama, a ne nužno u organizaciji za cyber sigurnost. To će smanjiti nerad među članovima omladine, smanjiti pljačku i nasilje. Svima treba dati jednake mogućnosti.

Lične kompanije treba da pružaju redovne savjete zaposlenima o njihovom načinu života, pa čak i o tome kako da zaštite svoje porodice od slučajeva cyber maltretiranja i cyber napada. Prilikom ovog otkazivanja, svaki zaposlenik ili poslodavci moraju biti iskreni i otvoreni prema osobi zaduženoj za savjetovanje kako bi im lakše pružili pomoć. Štaviše, vlada bi trebala biti otvorena prema ličnim kompanijama u smislu da mogu pristupiti različitim sigurnosnim industrijskim resursima za razvoj i širenje kompanija. Koliko god da su ova dva tiela različita, ali po mom mišljenju, uvijek bi trebalo da rade zajedno kako bi obezbjedili povoljno i sigurno okruženje za korišćenje kompjuterskog interneta i telefona.

U zaključku, cyber sigurnost je zaista važan faktor koji treba uzeti u obzir kako bi se osigurala sloboda komunikacije u svijetu. U ovom dijelu rada raspravljali smo o glavnim uzrocima cyber napada i kako ih izbjeći.

5. PANDEMIJA COVID-19 I POLITIKA CYBER SIGURNOSTI EVROPSKE UNIJE: ISKUSTVA I IZAZOVI

U ovom završnom dijelu rada pokazat će se da prije izbijanja COVID-19 trendovi uspostavljeni u periodu 2016-2019. nisu podložni idejnom izazovu, već umjesto toga COVID služi za jačanje postojeće zavisnosti od idejnog puta. Filozofski okvir u cyber sigurnosti, koji uključuje elemente koji se tiču stručnosti privatnog sektora i pozitivne prirode integracije, ostao je dosljedan. Međutim, na nivou programa, dok se smatra da su neki stručnjaci iz privatnog sektora najbolje pozicionirani da olakšaju cyber sigurnost kao sredstvo za borbu protiv rizika na mreži, više se ne smatra da operateri platformi društvenih medija dijele isti pogled na svijet kao EU o neophodnosti borbe protiv dezinformacija. Nakon izbijanja COVID-19, ovi trendovi su nastavljeni, iako ubrzanim tempom. Ovo sugerira da je temeljna filozofija i razumijevanje na nivou programa da svi stručnjaci iz privatnog sektora dijele slične vrijednosti kao i EU u oblasti cyber sigurnosti bilo efikasno osporeno i imalo trajne efekte. Zaista, sada postoje dvije diskurzivne ovisnosti o putevima, jedna u kojoj je privatni sektor koji pruža cyberu sigurnost partner od povjerenja u upravljanju cyber prostorom, a druga u kojoj platforme društvenih medija predstavljaju izazov za sigurnost EU kroz nespremnost ili nesposobnost da se efikasno pozabaviti se dezinformacijama i stoga im je potreban veći nadzor.

COVID-19 je dominirao velikim dijelom fokusa programa i politike EU u vrlo kratkom vremenu. Krajem februara pandemija se vidljivo pojavila kao kriza na dnevnom redu EU. (Vijeće Evropske unije, 2020c.) Prije izbijanja epidemije, manje od 10% radnika u EU radilo je od kuće na dnevnoj bazi (u Velikoj Britaniji i Francuskoj ima otprilike 12% i 17% radnika koji rade od kuće), što se povećalo na 38% do aprila 2020., uključujući više od polovine radno aktivnog stanovništva u Belgiji, Holandiji, Luksemburgu, Finskoj i Velikoj Britaniji. (EEAS, 2020.) Ovo povećanje broja kućnih poslova viđeno je kao prilika za kriminalne aktere na mreži, a Europol je izvijestio o značajnom porastu napada na informacione sisteme, online prevara i napada na ransomware (2020.). Slično tome, dezinformacije o porijeklu COVID-19, njegovim efektima, reakciji svjetskih vlada i zapravo samom postojanju virusa počele su se širiti od januara nadalje. (Lomas, N., 2020.) Komisija je u travnju 2020. objavila Preporuku o zajedničkom paketu alata Unije za korištenje tehnologije i podataka za borbu protiv krize COVID-19 i izlazak iz nje. (Preporuka Komisije 2020/518, 2020.) Ova Preporuka precizira da bi efikasne mjere cyber sigurnosti bile ključne kako bi se osigurala zaštita podataka koji se koriste za rješavanje krize, uključujući podatke testiranja i praćenja. U okviru ove preporuke, provajderima ovih tehnologija iz privatnog sektora vjeruje se da će osigurati otpornost svojih

sistema na kršenje podataka ili neovlašteni pristup, u saradnji sa tijelima za zaštitu podataka i zdravstvenim institucijama.

Diskurzivno, ovi akteri iz privatnog sektora dio su okvira upravljanja cyber sigurnošću, sa filozofskim i programskim kontinuitetom, i promjenom politike koja uzima postepeno slojevit pristup. Ova se tema nastavlja u inicijativi politike „Popravi i pripremi“ koju je Komisija predložila u svibnju (Evropska komisija, 2020d.), a koja je obuhvatila niz različitih aktivnosti za poticanje ekonomskog oporavka nakon COVIDa. U oblasti cyber sigurnosti, akteri iz privatnog sektora su predstavljeni kao doprinosi i sigurnosti onlajn okruženja u Evropi, uz diskusiju o njihovoj uključenosti u proširenu inicijativu za zaštitu kritične infrastrukture, kao i kao izvor potencijalnog oporavka kroz uspostavljanje mala i srednja preduzeća orijentisana na cyber sigurnost. (Evropska komisija, 2020d.) U vrijeme pisanja ovog teksta, najnovija publikacija s dimenzijom cyber sigurnosti su Zaključci Vijeća o agendi za oblikovanje digitalne budućnosti Evrope. (Vijeće Evropske unije. 2020a.) Ovi zaključci naglašavaju da je cybera sigurnost bitan doprinos ekonomiji i sigurnosti EU zasnovan na principima otpornosti i javno-privatne saradnje, ohrabrujući nastavak i proširenje ovih aktivnosti, slažući se da će „ubrzanje digitalne transformacije biti suštinska komponenta odgovora EU na ekonomsku krizu izazvanu pandemijom COVID-19”. (Vijeće Evropske unije. 2020a.)

Odgovori na dezinformacije ojačali su percepciju EU da platforme društvenih medija ne dijele iste vrijednosti ili filozofiju u vezi s ovim oblikom komunikacije koji izaziva podjele. Strategija Vijeća za ublažavanje rizika od COVID-19 naglašava da se jedan neophodan odgovor politike odnosi na napore usmjerene na sprječavanje širenja dezinformacija u vezi s virusom. (Evropska komisija, 2018c.) To se ponavlja u Komunikaciji Komisije i visokog predstavnika o globalnom odgovoru EU na COVID-19, gdje su dezinformacije o virusu diskurzivno uokvirene kao prijetnja temeljnim vrijednostima EU-a i njenoj zdravstvenoj sigurnosti. (Vijeće Evropske unije. 2020a.) Prema Europolu, dezinformacije u vezi s izbijanjem i odgovorom na COVID-19 brzo su se širile od početnog izbijanja u Wuhanu, a navodni izvori uključuju strane vlade, aktere koje podržava država, političke oportuniste i kriminalne organizacije (2020.). Komisija se u svibnju pozvala na “infodemiju” u kojoj su se širile lažne poruke, često s propagandom ili narativom zasnovanom na mržnji. Ova dezinformacija je predstavljena kao prijetnja javnom zdravlju i demokratiji, s potrebom za hitnim djelovanjem. (Evropska komisija, 2020e.)

Divergentan pristup platformama društvenih medija je pojačan u zaključcima Vijeća. Ovdje su provajderi online platformi kategorizirani odvojeno od “stručnjaka” i “nacionalnih vlasti”, pri

čemu su te platforme predstavljene kao dio prijetnje dezinformacijama, a predmet su zahtjeva "za veću transparentnost i odgovornost". (Vijeće Evropske unije. 2020b.) Komisija i visoki predstavnik brzo su slijedili zaključke Vijeća Zajedničkom komunikacijom o borbi protiv dezinformacija o COVID-19, u kojem je ponovo naglašena priroda dezinformacija kao značajne prijetnje zdravlju i demokratiji. Iako se navodi da je zahtjev niza aktera, uključujući nacionalne vlasti, novinare, provjere činjenica i operatere platformi, da sarađuju na identifikaciji i rješavanju dezinformacija, narativ u vezi s platformama je da "platforme nisu dovoljno ovlastile [provjere činjenica] tokom trenutne krize javnog zdravlja […] postoji potreba za dodatnim naporima i razmjenom informacija, kao i povećanom transparentnošću i većom odgovornošću". (Vijeće Evropske unije. 2020b.) Prijedlozi politika u ovoj oblasti zahtijevaju obnovljene napore platformi da rade s nacionalnim vlastima i provjeravačima činjenica kako bi se identificirale dezinformacije i njihovi izvori, kao i otkrivanje manipulativnog ponašanja koje se provodi putem njihovih platformi. (Vijeće Evropske unije. 2020b.) U svojoj ocjeni širenja dezinformacija, EEAS je primijetio da, iako su platforme društvenih medija imale određeni uspjeh u borbi protiv dezinformacija u vezi s virusom, „platforme su još uvijek ranjive da budu alat za viralnu distribuciju lažnih informacija [... i] to pokazuje da dalje a trajni napori platformi su neophodni izvan Kodeksa prakse". (EEAS, 2020.) Nadalje, prilikom objavljivanja Zajedničkog saopštenja, potpredsjednica Komisije za vrijednosti i transparentnost Vera Jourova izjavila je da „iako su internetske platforme poduzele pozitivne korake tokom pandemije, moraju pojačati svoje napore […] Na primjer, znamo samo kao koliko nam platforme govore - ovo nije dovoljno dobro. Moraju se otvoriti i ponuditi više dokaza. (Schmidt, V. A. 2020.)Nije nepredviđeno da ubrzanje EU-ovog programa dezinformacija može u konačnici dovesti do politike pojačane regulacije društvenih medija, umjesto da se poseban pristup koji se temelji na tržištu primjenjuje na aktere u drugim poljima cyber sigurnosti.

U središtu razmimoilaženja u osnovnoj filozofiji i rezultirajućim programskim i političkim odgovorima EU u oblasti cyber sigurnosti je promjenjivo razumijevanje uloge privatnih aktera u upravljanju. Konačno, to je zbog povjerenja uloženog u te aktere - u okviru ordoliberalnog filozofskog okvira, stručnjak iz privatnog sektora je aktivan učesnik u upravljanju različitim oblastima politike u saradnji sa EU i nacionalnim vlastima, pri čemu je EU najbolje pozicionirana za koordinaciju. djelovanje na kohezivan i koherentan način. U većini domena cyber sigurnosti, privatnom sektoru se može vjerovati da čini djelotvoran dio te mreže i na taj način doprinosi efektivnoj sigurnosti i ekonomskom razvoju EU, što ne rezultira značajnim izazovom ovisnosti o putu koji su se razvili od nastanka i formalizacija cyber sigurnosti EU. Iz tog razloga, u većini domena cyber sigurnosti, promjene su postepene, slojevite prirode.

Međutim, kritični trenutak koji je poslužio za preusmjeravanje ove zavisnosti od idejnog puta nije bila finansijska kriza, pa čak ni trenutna pandemija. Umjesto toga, gubitak povjerenja u određene aktere na mreži, odnosno platforme društvenih medija, rezultat je preokreta i globalne nestabilnosti (s tim da je 2016. bila kritična godina u ovoj promjenjivoj percepciji) kojoj kreatori politike EU smatraju da su platforme društvenih medija doprinijele i odbijaju prihvatiti odgovornost za. Ovdje vidimo diskurzivnu promjenu, s promjenama na nivou programa i politika koje se tiču uloge platformi društvenih medija u borbi protiv dezinformacija. Iako svi akteri iz privatnog sektora mogu doprinijeti osiguravanju sigurnosti i ekonomskog rasta u EU, nekima se više vjeruje da će to učiniti u skladu s temeljnim vrijednostima EU od drugih.

5.1. COVID-19 i cyber sigurnost

Pandemija COVID-19 stvorila je mnoge teške izazove i zahtijevala je donošenje mnogih odluka kako bi se brzo prilagodili situaciji na dnevnoj bazi. Međutim, COVID-19 ima ozbiljne posljedice vezane za cyber sigurnost i ljudsko pravo na privatnost, sigurnost, pa čak i fizički integritet. Mnoge od ovih posljedica su direktno povezane s liječenjem bolesti, kao što je razmjena ličnih i osjetljivih podataka za istraživanje i liječenje ili praćenje kontakata pacijenata; u međuvremenu, druge posljedice mogu biti indirektno povezane s pandemijom, ali su jednako opasne. Ove posljedice uključuju kontinuirano liječenje drugih bolesti dok su pacijenti zatvoreni u svojim domovima i povećanu ranjivost i rizike fizičke i internetske sigurnosti kada se ljudi oslanjaju na internet za većinu svojih svakodnevnih aktivnosti (npr. rad od kuće, školovanje kod kuće, kupovina na webu, kućno bankarstvo, kontakt sa prijateljima i porodicom, vježbanje i zabava).

U literaturi se preporučuje da se analize podataka vrše u skladu sa zakonom i uz poštovanje privatnosti, što može povećati povjerenje i pridržavanje javnosti. (Benkler, Y., Tilton, C., Etling, B., Roberts, H., Clark, J., Faris, R., Kaiser, J., Schmitt, C. (2020.) Potreba za transparentnošću je još veća kada se lični i osjetljivi podaci koriste za praćenje kontakata pomoću tehnologije pametnog telefona. Aplikacije za praćenje kontakata su moćni alati koji mogu pomoći u ograničavanju prijenosa bolesti tokom pandemije, uvođenju pravila karantina, obavještavanju korisnika o zonama rizika ili upozoravanju zaraženih ljudi. (CybSafe, 2020) Međutim, aplikacije za praćenje kontakata predstavljaju značajnu zabrinutost za privatnost jer prikupljaju osobne podatke, kao što je lokacija, koji se također mogu koristiti za obavljanje visokog stupnja nadzora i narušavanje privatnosti pojedinaca. (Collett, R., Barmpalious, N., Pawlak, P., 2021.) Potreban je adekvatan balans između anonimnosti i kvaliteta i integriteta podataka, uz adekvatnu transparentnost od strane ovlaštenih tijela.

Iako mnoge druge bolesti ili stanja mogu zahtijevati stalnu podršku i liječenje, pandemija COVID-19 je također pogoršala hitne situacije koje se možda neće odmah riješiti, kao što su kronična, onkološka ili mentalna stanja. (ENISA, 2021.) Zdravstveni radnici moraju se odlučiti za alternativna (možda manje sigurna) sredstva podrške svojim pacijentima, kao što su telekonsultacije, e-pošta i društvene mreže. (Evropska komisija, 2021a)

Ova pitanja cyber sigurnosti su samo početak. U prvom dijelu ovog gledišta (COVID-19, Cybersecurity, Privacy, Security, and Safety), identifikuju se i raspravljaju o izazovima i posljedicama cyber sigurnosti koje je COVID-19 iznio na površinu i kojima je potrebna hitna pažnja. Ovaj dio se temelji na dostupniim informacijama. (Evropska komisija, 2021b)U drugom dijelu (Potrebne promjene u cyber sigurnosti), preporuke za nove pristupe rješavanju identificiranih problema su napredne kako bi se podstakla promjena trenutne paradigme cyber sigurnosti. Ovaj odjeljak sadrži originalne preporuke i specifične su za ovo gledište.

5.1.1. COVID-19 povezan sa cyberom sigurnosti, privatnosti i zaštitom

Identificirane probleme cyber sigurnosti kategorizirali su kao direktne i indirektne posljedice COVID-19, kao što je prikazano na slici 1.

Slika 1. Direktne i indirektne posljedice COVID-19 na cyberu sigurnost (Arora, A., Nandkumar, A. i Telang, R., 2006.)

5.1.2. Direktne posljedice COVID-19

5.1.2.1. Dijeljenje podataka

Najhitniji izazovi vezani za praćenje kontakata fokusiraju se na ravnotežu između dijeljenja i održavanja privatnosti ličnih podataka, što je ključno, ali teško postići. (CybSafe, 2020.) Aplikacije za praćenje kontakata ne bi trebale biti dostupne bez odgovarajuće procjene rizika i provjere integriteta podataka. (Evropska komisija, 2021b) Ako su podaci anonimizirani,

integritet je teže garantirati jer su anonimizirani podaci podložniji neotkrivenim smetnjama; stoga ovi podaci nisu korisni i pouzdani za predloženi cilj zdravstvene zaštite. Integritet podataka može se postići samo gubitkom određenog stepena privatnosti, u idealnom slučaju subjektu od povjerenja.

Nedostatak informatičke tehnologije i cyber pismenosti također može otežati većini pojedinaca da adekvatno instaliraju i koriste aplikacije za praćenje ugovora, dok same aplikacije mogu integrirati tehničke sigurnosne ranjivosti i rizike. (Eurostat, 2021.)Na primjer, najčešće korišteni protokol u aplikacijama za praćenje je Bluetooth, koji ima poznate i intrinzične ranjivosti, kao što je nedostatak kontrole granica. Bluetooth signali mogu proći kroz zidove i automobile, a pojedinci koji primaju signale možda zapravo nisu u kontaktu sa zaraženom osobom. Ravnoteža između čestih lažno pozitivnih ili negativnih rezultata možda će trebati prilagoditi u skladu s evolucijom pandemije, jer može biti sigurnije dobiti više lažno pozitivnih nego lažno negativnih, posebno ako je virus vrlo zarazan. (Eurostat, 2021.)

Konačno, čak i ako ove aplikacije za praćenje kontakata dobiju široku privrženost i upotrebu, postavljaju se pitanja. Koji je efektivni povrat ili korist za zdravlje pojedinca ili javnog zdravlja? Kako se ovaj povrat ili korist može mjeriti u odnosu na gubitak privatnosti? Sada je pravo vrijeme da odgovorite na ova pitanja.

5.1.2.2. Prijevara i krađa

Došlo je do velikog porasta lažnih poruka povezanih s pandemijom COVID-19. (Fernandez, S., Jenkins, P., Vieira, B., 2020.)Ove poruke se hrane širenjem dezinformacija, “lažnih vijesti”, straha, izolacije i nedostatka svijesti da se zatvoreno stanovništvo pretvori u ranjivu metu za te vrste napada (Malekos Smith, Z., Lostri, E., 2020.) i ubijedi žrtve da daju novac, lične podatke, i vjerodajnice (npr. phishing, ransomware, lažne kampanje prikupljanja sredstava). (Morgan, S., 2019.) Nadalje, kada su ljudi izolovani, oni imaju tendenciju da kupuju više proizvoda na webu; stoga, napadači mogu iskoristiti lažne poruke o isporuci proizvoda. Treba napomenuti da kršenja sigurnosnih podataka izvršena u ovom periodu neće biti samo sada iskorištena već će imati izuzetno širok utjecaj u budućnosti, jer će se ova eksploatacija nastaviti još dugo nakon smirivanja pandemije.

U drastičnim vremenima kao što je pandemija COVID-19, mogu se pojaviti i drugi ozbiljni problemi. Međunarodna špijunaža i sabotaža mogu postati češća. Nedavni primjeri su nedostatak odgovarajućeg upravljanja procedurama vakcinacije, kao i oslanjanje na velike

multinacionalne kompanije da pravedno distribuiraju i prodaju vakcine. (Statista, 2021b) Obezbjeđivanje preventivnih sredstava i odgovarajućih javnih politika za otkrivanje i izbjegavanje ovih problema je od suštinskog značaja za zaštitu života ljudi.

5.1.2.3. Ranjivi sistemi

Većina sistema zdravstvene zaštite je pod budžetom, koristi zastarjelu tehnologiju i nije interoperabilna, a često im nedostaju najnovije zakrpe i adekvatne konfiguracije. (Statista, 2021b) Pandemija COVID-19 otvorila je put napadačima da bolje iskoriste ove ranjivosti. Stres koji se stavlja na ove sisteme je veoma visok; osim toga, postoji rizik od nedostatka opreme zbog velikog broja hospitaliziranih pacijenata u jednom trenutku. Od zemalja Evropske unije se zahtijeva da se pridržavaju Opće uredbe o zaštiti podataka (GDPR) radi zaštite ličnih podataka. Nažalost, to još uvijek nije uobičajena praksa, a organizacije pokušavaju riješiti situaciju s malo ili bez resursa i, što je najvažnije, bez stručnog znanja. (UK, Odsjek za digitalno, kulturu, medije i sport, 2021.)

5.2. Indirektne posljedice COVID-19

Iako je pandemija COVID-19 ozbiljna situacija u cijelom svijetu, s prijetećom prijetnjom kolapsa zdravstvenih sistema, liječenje drugih bolesti nije moguće staviti na čekanje. Pacijenti s kroničnim, onkološkim, mentalnim, akušerskim i drugim zdravstvenim stanjima moraju se liječiti. Telekonsultacije i medicinski savjeti zasnovani na webu su dostupni (Verizon, 2020 i 2021.), ali po kojoj cijeni za privatnost pacijenata? Sigurnosni sistemi u većini kućnih infrastruktura nisu spremni za adekvatnu kontrolu i zaštitu ličnih i osjetljivih podataka.

Jedna ozbiljna posljedica pandemije COVID-19 je izolacija velikog dijela svjetske populacije. Prije pedeset godina, kada su se informacije prenosile samo putem pošte i fiksnih telefonskih kompanija, cyber sigurnost nije bila problem. Trenutno su, međutim, gotovo sve dnevne aktivnosti postale virtuelne. Ipak, u idealnom svijetu gdje je sva kućna infrastruktura osigurana i ljudi poduzimaju potrebne mjere predostrožnosti da zaštite svoje podatke i fizički integritet, cyber sigurnost će i dalje biti problem. To je zbog složenih odnosa između ljudi i tehnologije. Neki uobičajeni primjeri su navedeni u nastavku:

- Rizična ponašanja mogu se pojaviti, jer istovremeno procjenjivanje svake interakcije i poruke iz različitih konteksta, 24 sata dnevno, 7 dana u sedmici, može stvoriti stres i navesti ljude da donose loše i nesigurne odluke.
- Različiti konteksti (npr. lični, profesionalni, poznati, obrazovni) mogu lako dovesti do zabune i grešaka.

- Različite populacije su različito pogođene (npr. stariji ljudi, manjinske grupe, djeca i adolescenti). Riječi kao što su cyberbullying, lažni profili, lažno predstavljanje, trolovanje i Zoombombing (ometanje Zoom konferencija) mogu pasti na pamet. (Carrapico, H. i B. Farrand. 2017.)
- Kućna infrastruktura nije pripremljena sa sigurnosnog stanovišta, a odrasli koji rade od kuće su opterećeni i rastreseni, ostavljajući mlađe ljude ranjivijim.
- Ljudi su uključeni u česte telefonske ili video pozive i često zaborave da razmisle o okruženju u kojem se nalaze i ko ih možda sluša. Sa balkona i vrtova, pa čak i kroz vrata ili zidove, informacije mogu iskliznuti češće nego što mislimo. Špijunaža i krađa mogu i često se dešavaju neotkrivene. (Preporuka Komisije 2020/518, 2020.)
- Otključane sesije ili uređaji i mikrofoni ili kamere povezani u neželjeno vrijeme mogu dijeliti više ličnih podataka nego što bi trebali.

5.3. Potrebne promjene u cyber sigurnosti

Tokom pandemije, svijet je doživljavao jedan talas COVID-19 za drugim; ipak, vlade, kompanije i javnost svi su fokusirani na povratak svojim „normalnim“ rutinama prije pandemije. Međutim, u cyber sigurnosti (kao iu drugim oblastima), „normalno“ uključuje niske budžete, nedostatak svijesti i obrazovanja, nedostatak odgovarajuće infrastrukture i nemogućnost prilagođavanja različitim upotrebama od strane različitih ljudi iu različitim kontekstima. “Normalno” također znači da su privatnost i sigurnost i dalje među najvećim izazovima u interakciji čovjeka i računara. (Deflem, M. i E. Shutt. 2006.)

Promjena je ključna, a pandemija COVID-19 to je još više naglasila; međutim, ovu promjenu je teško postići. Stoga, poput malog kamenčića u velikom ribnjaku, autori žele da iskoriste ovo gledište da poremete postojeće ideje i paradigme i promovišu druge perspektive za diskusiju o cyber sigurnosti, kao i povezanim tehnologijama i procedurama.

Pismenost i obrazovanje o cyber sigurnosti su od suštinskog značaja, još više u vrijeme pandemije. Jedan od načina za postizanje ovih ciljeva je generiranje naučnih istraživanja, kao što je ovo gledište, da se podigne svijest, daju preporuke i isprobaju nova ili poboljšana rješenja. Međutim, sadašnja vremena zahtijevaju web-bazirane, jednostavne, brze, tačne i objektivne, ali personalizirane i smislene informacije i obrazovanje koje je prilagođeno situaciji i kontekstu i ciljnoj populaciji (EEAS, 2020.). Zbog nepredvidive prirode ljudskog ponašanja i akcija, ljudi su važan element i glavni pokretači nivoa cyber sigurnosti koji svaki sistem može i koji će imati. (EEAS, 2020.)

Međutim, obrazovanje nije dovoljno. Ljudi su uspjeli tisućama godina uspješno koristeći alate, a ne zato što su stručnjaci ili imaju potpuno znanje o svakom alatu ili aktivnosti. (Eurofound, 2020.) Zašto bi njihovi odnosi sa tehnologijom bili mnogo drugačiji? Nekoliko faktora može doći u igru u odnosima između ljudi i uređaja (npr. sigurnost, upotrebljivost, dizajn, efikasnost, demografija, prethodne interakcije); međutim, čak i kada se ovi faktori pozabave, adekvatna i sigurna upotreba tehnologije možda i dalje neće biti moguća. Postoji jedna prožimajuća linija koja prožima sve ove odnose i faktore koja je poznata kao povjerenje. Iako ovo može biti predmet straha (subjektivan) u informatici, povjerenje se može uspostaviti na webu jer tehnologija ima društveno prisustvo na koje ljudi reagiraju. (Evropska komisija, 1985.) Međutim, istraživanja ne uspijevaju obuhvatiti razloge zašto krajnji korisnici odlučuju da vjeruju ili nemaju povjerenja u sisteme (Evropska komisija, 1990.) i koji faktori doprinose povjerenju. (Evropska komisija, 1993.) Čvrsta formalizacija računalnog povjerenja, kako bi se objasnilo kako se odnosi razvijaju kroz interakcije u nizu web-baziranih konteksta, pružila bi poboljšanu sigurnost zasnovanu na webu. (Evropska komisija, 1999.) Istraživači i programeri bi trebali biti dovoljno hrabri da razmotre razvoj povjerenja u dizajnu tehnologije tako što će pružiti značajke koje podržavaju krajnje korisnike u procjeni pouzdanosti tehnologije, pomažu u promoviranju pravilne upotrebe tehnologije i minimiziraju učestalost sigurnosnih incidenata. (Evropska komisija, 2001.)

Baveći se prethodnim pitanjem, mnogo više se može razumjeti u smislu osobina ličnosti, sklonosti povjerenju i sklonosti prema manipulaciji i viktimizaciji u odnosima čovjeka i uređaja. Ovo će svakako omogućiti implementaciju adekvatnijih strategija za rješavanje jednog od najkritičnijih neriješenih problema u cyber sigurnosti - društvenog inženjeringa.

Nadalje, napredak u povjerenju u odnosima između ljudi i uređaja može otvoriti put ka sigurnijoj upotrebi inovativnih rješenja kao što su digitalni ljudi visoke vjernosti. (Evropska komisija, 2010a.) Ova poboljšanja mogu raditi na promoviranju konteksta drugog života ili proširene stvarnosti i poboljšanju privatnosti, na primjer, djece i adolescenata, s njihovim brojnim interakcijama koristeći alate za video konferencije (npr. školovanje kod kuće, vježbanje, časovi muzike). Neke od ideja o kojima se raspravljalo može potrajati duže za proučavanje i implementaciju; međutim, dok se to radi, autori predlažu korištenje anonimnih "digitalnih blizanaca" za lako i brzo testiranje interakcija između korisnika i tehnologije. Mockup interfejsi upotpunjeni anonimnim anketama dostupnim na webu mogu se brzo razviti kako bi se testirala sigurnost, privatnost i upotrebljivost tehnologije od strane velikog uzorka ljudi sa širokim spektrom iskustava, karakteristika i ponašanja.

6. CYBER NAPADI I CYBER RIZICI TOKOM PANDEMIJE COVID-19

Poremećaj zbog COVID-19 otkrio je slabosti postojećih institucija u zaštiti zdravlja i dobrobiti ljudi. Nedostatak pravovremenih i tačnih podataka i široko rasprostranjene dezinformacije uzrokovali su sve veću štetu i rastuću napetost između zabrinutosti za javno zdravlje i privatnosti podataka. U nedostatku tačnih podataka i pouzdanih informacija, patnja zbog COVID-19 je još gora. Kriza COVID-19 je kriza informacija, kao i kriza povjerenja. On je naglasio neuspjehe postojećih sistema u povjerenju i dijeljenju podataka. Tokom krize, uočeni su kvarovi u glavnom lancu nabavke, posebno za ličnu zaštitnu opremu (PPE) i respiratore za spašavanje života u klinikama i bolnicama. (Statista, 2021a)

Digitalne metode su odigrale značajnu ulogu tokom pandemije COVID-19. Međutim, postoje izazovi telemedicine i drugi digitalni pristupi privatnosti i sigurnosti zaštićenih informacija. (Statista, 2021b) Od početka pandemije COVID-19 došlo je do značajnog porasta broja cyber napada. Tokom pandemije, veliki cyber rizici uzrokovani su postupcima ljudi, kao i kvarovima sistema i tehnologije. Izvor operativnog rizika uključuje radnje ljudi, na primjer, namjerno (npr. krađa, sabotaža, prijevara i vandalizam), nenamjerno (tj. propusti i greške) i nedjelovanje (npr. dostupnost, znanje, vještine i vođenje). Greške sistema i tehnologije leže u softveru (tj. praksa kodiranja, testiranje, sigurnosna podešavanja, kontrola promjena, upravljanje konfiguracijom i kompatibilnost), hardver (tj. kapacitet, performanse, održavanje i zastarjelost) i sistem (tj. specifikacije, dizajn, integracija i složenost). (Statista, 2021a) Tabela 1 navodi dio zlonamjernih i nezlonamjernih kršenja. Neki potencijalni scenariji napada prikazani su u tabeli 2.

Tabela 1. Neka zlonamjerna i nezlonamjerna kršenja (Izvor: Statista, 2021b)

Vrste	Opis
Ukradeni uređaj	Ukradeni pametni telefon, laptop, čvrsti disk, prenosivi memorijski uređaj, itd., i podaci (npr. osjetljive informacije) zajedno sa uređajem.
Insajderska prevara	Osoba (npr. ugovarač ili zaposlenik) s legitimnim pristupom namjerno provaljuje informacije.
Vanjska prijevara, a ne uređaj	Odbačeni, izgubljeni ili ukradeni neelektronski zapisi (npr. papirna dokumenta); prevara (koja uključuje kreditne ili debitne kartice) bez izvršenja hakiranja.
Zlonamjerni softver ili hakovanje	Elektronski ulazak spoljne strane, malver, špijunski softver.
Slučajno otkrivanje	Osjetljive informacije javno objavljene na web stranici, pogrešno rukovane ili poslane pogrešnoj strani putem faksa, e-pošte ili pošte.

Tabela 2. Neki potencijalni scenariji napada (Tasheva, I., 2017.)

Napadi	Opis
Napad povezivanja	Napadač prikuplja pomoćne informacije o meti iz različitih izvora, kombinuje informacije, stvara ukupnu sliku mete i izvodi napad.
Sybil napad	Napadni mehanizmi redundantnosti podataka.
Lažni napad	Jedan objekat se pretvara da je identitet drugog objekta za sticanje povjerenja, ulazak u sistem, širenje zlonamjernog softvera, krađu podataka itd.
DoS/DDoS	Napadači koriste uskraćivanje usluge (DoS) ili distribuirani DoS (DDoS) kako bi blokirali korisnike da pristupe uslugama na mreži pokretanjem ogromnih beskorisnih informacija i time uzrokujući zagušenje mreže.

Neophodno je da organizacije rješavaju probleme sigurnosti i privatnosti ličnih podataka svih dionika kroz kreiranje primjenjivih okvira za upravljanje podacima. Sa etičke tačke gledišta, tehnička usklađenost sa zakonima o podacima i privatnosti često je nedovoljno da zaštiti organizacije od frustriranih potrošača. Trebalo bi da postoje adekvatne ugrađene zaštitne mjere za rukovanje etičkim rizicima i mogućim rizicima po sigurnost i reputaciju organizacija. Sa pravne tačke gledišta, organizacije bi trebalo da koriste odgovarajuće procese da garantuju usklađenost sa zakonima koji se odnose na prikupljanje, skladištenje, korišćenje i otkrivanje podataka. (UK, Odsjek za digitalno, kulturu, medije i sport, 2021.)

6.1. Cyber sigurnost za daljinski rad

Rad kod kuće zbog COVID-19 je "nova normala". Mnogi pojedinci se neće vratiti u ordinaciju kada se pandemija završi; većina pojedinaca u okruženju "rad od kuće" nastavit će u tom načinu rada, čak i nakon što je vakcina u potpunosti distribuirana. Škole su se vratile iz 14-mjesečne pauze jeseni 2021. godine. Sigurnost i rizici po reputaciju, posebno za preduzeća sa osjetljivim podacima koji su bili zabrinuti nakon što su propisi o samoizolaciji natjerali ljude da rade kod kuće, a organizacije su morale prilagoditi svoje poslovne modele kako bi se prilagodile značajnom porastu mrežnih aktivnosti. Mnogi hakeri su stalno preusmjeravali svoje aktivnosti od napada na poslovanje prema aktivnostima koje bi mogle doći do potrošača ili zaposlenika u njihovim domovima putem platformi, na primjer, Netflix ili Zoom. (UK, Odsjek za digitalno, kulturu, medije i sport, 2021.) Tabela 3 prikazuje neke stavke rizičnog ponašanja u cyber sigurnosti.

Tabela 3. Neka rizična ponašanja vezana uz cyber sigurnost (Izvor: ENISA, 2019.)

R.br.	Predmeti
1.	Klikom na link u neželjenoj e-poruci iz nepoznatog izvora.
2.	Korištenje iste lozinke na različitim web stranicama.
3.	Preuzimanje besplatnog antivirusnog softvera iz neidentifikovanog izvora.
4.	Unošenje informacija o plaćanju na web stranici bez jasnih sigurnosnih informacija/certifikacije
5.	Preuzimanje materijala sa web stranice na radni računar bez provjere njihove autentičnosti.
6.	Preuzimanje digitalnih medija (igara, filmova i muzike) iz nepoznatih izvora.
7.	Korištenje besplatnog javnog Wi-Fi-ja
8.	Korištenje sistema za skladištenje na mreži za čuvanje i razmjenu osjetljivih ili ličnih podataka.
9.	Čuvanje informacija organizacije na ličnom elektronskom uređaju kao što je laptop, tablet ili pametni telefon.

Tokom pandemije COVID-19, mnoge organizacije koriste model rada na daljinu, uzrokujući nedovoljnu cyber sigurnost zaposlenih. Mnoge mreže zaposlenih kod kuće mogu se sastojati od zastarjelih računara i nesigurnih uređaja IoT-a. Pandemija je izazvala tehnološke i ranjivosti krajnjih korisnika, a cyber kriminalci iskorištavaju ranjivosti rada na daljinu. (Verizon, 2020.) Tabela 4 prikazuje tehnologije, ciljane/imitirane tehnološke brendove, faktore situacije i cyber kriminal.

Tabela 4. Neke tehnologije i ciljani tehnološki brendovi (Izvor:Verizon, 2020.)

Tipovi tehnologije	Ciljane/imitirane tehnološke marke	Situacioni faktori	Cyber zločini
Online sistem za plaćanje	Paypal	Krediti za mala preduzeća	Lažna domena web stranice
Emailovi	Gmail	Donacija	Lažne e-poruke (npr. phishing)
Web lokacije za dijeljenje video zapisa	YouTube	Slobodno vrijeme/zabava	Lažni proizvodi
Tehnologija društvenih medija	Facebook	Društvene mreže	Lažni profili na društvenim mrežama
Usluge hostinga datoteka u oblaku	One Drive	Rad na daljinu	Lažni proizvodi
Kompanije sa širokopojasnim internetom i telekomunikacijama	4 G (lažna kompanija)	Internet/besplatni podaci	Lažni proizvodi
Usluge videotelefonije i chata na mreži	Zoom	Rad na daljinu	Lažni proizvodi
Streaming medijska usluga (filmovi i televizija)	Netflix	Zabava/slobodno vrijeme	Lažni proizvodi

COVID-19 je izazvao pomak sa ekosistema na virtuelno radno mjesto za zaposlene, što je dovelo do izazova u rizicima cyber sigurnosti jer postoji više ranjivosti na osobnim računarima zaposlenika i njihovom kućnom internetu. (Verizon, 2021.) Tabela 5 navodi preporuke za cyber sigurnost na daljinu za udaljene zaposlenike.

Tabela 5. Preporuke za cyberu sigurnost za zaposlenike koji rade na daljinu (Izvor: Verizon, 2021.)

Aspekti	Preporuke
Autentifikacija	Implementirajte dvofaktorsku ili višefaktornu autentifikaciju: tekstualni kod ili poziv za autentifikaciju se šalje na telefon zaposlenog prije nego što se odobri pristup mreži organizacije.
Upravljanje mobilnim aplikacijama i mobilnim uređajima	Provedite sigurnosne mjere kao što su skeniranje zlonamjernog softvera, enkripcija podataka itd.
Sigurnosne zakrpe i zaštita od virusa	Garantujemo da mobilni uređaji i računari za pristup radnim mrežama imaju zaštitu od virusa i ažurirane sigurnosne zakrpe.
Implementacija politika	- Nemojte dijeliti radne računare, smanjujući rizik od nenamjernog ili neovlaštenog pristupa zaštićenim informacijama kompanije. - Nemojte pristupati informacionim sistemima kompanije dok ste na javnoj Wi-Fi mreži uz korištenje VPN-a. - Nemojte preuzimati osjetljive informacije organizacije i čuvati ih na uslugama u oblaku (npr. Google Drive) ili ličnim uređajima (npr. fleš diskovi i računari zaposlenih).
Obuka zaposlenih	- Obučite zaposlene o tome kako su osjetljivi podaci zaštićeni i šifrirani kod kuće. - Obučite ih da koriste virtuelne privatne mreže (VPN) kako biste garantovali da je upotreba Interneta šifrovana i da je lokacija korisnika zaposlenog privatna prilikom procjene mreže kompanije.

6.2. Cyber sigurnost IoT-a i telemedicine

Cyber rizici su jedna od glavnih prepreka širokoj primjeni IoT-a u zdravstvu. Privatnost pacijenata treba biti zaštićena, kako bi se spriječilo neovlašteno praćenje i provjera. Internet stvari može pružiti prilike za cyber napade i da lične informacije budu nepropisno uhvaćene. Aplikacije zasnovane na IoT-u su ranjive na cyber napade iz dva razloga:

1) mnoge komunikacije su bežične, što čini prisluškivanje relativno lakim kada se ne koristi visoka enkripcija;
2) niska energija je karakteristika većine IoT komponenti; međutim, njima je teško izvesti šeme za garanciju sigurnosti. (Preporuka Komisije 2020/518, 2020.)

Ostvarivanje interoperabilnosti preko IoT platformi pomaže u pružanju pristupačnijih i sigurnijih usluga u zdravstvu. Razmjena podataka u različitim zemljama također predstavlja

zabrinutost. Sigurnost podataka, povjerljivost i privatnost treba da se implementiraju na saveznom nivou; međutim, međunarodni domaćini ili dobavljači možda neće poštovati domaće zakone ili propise. (Preporuka Komisije 2020/518, 2020.)

Razvijen je model za daljinsko praćenje zdravlja koji koristi lagani pristup blok šifriranja za obezbjeđivanje sigurnosti za zdravlje u IoT okruženju zasnovanom na oblaku. Data mining je korišten za analizu bioloških podataka generiranih od IoT uređaja i kroz analizu se dobiva zdravstveno stanje pacijenta. Osjetljivi podaci pacijenata zaštićeni su pristupom enkripcije. (EEAS, 2020.) IoT je korišten u kontroli COVID-19, ali postoje sigurnosni problemi i rizici po privatnost tokom skladištenja i prijenosa podataka. (EEAS, 2020.) Telehealth nudi mogućnosti za smanjenje posjeta bolnicama, što štiti pacijente i druge od infekcije COVID-19. Međutim, telezdravlje stvara rizike za cyber sigurnost i privatnost jer pacijentov dom možda nema dovoljno zaštite. Telehealth također pruža nove mogućnosti u razmjeni zdravstvenih informacija sa implikacijama na sigurnost i privatnost. (EEAS, 2020.) Područja prijetnji sigurnosti telemedicine prikazana su u Tabeli 6. *(Eurofound, 2020.)*

Tabela 6. Područja prijetnji sigurnosti telemedicine (Eurofound, 2020.)

Područja prijetnje sigurnosti	Opis
Internet	Sistemi telemedicine su osjetljivi na sigurnosne rizike vezane za njuškanje, eskalacije privilegija i izmjene/falsifikata jer se medicinske, privatne i zdravstvene informacije, kao i recepti prenose putem interneta.
Kućne mreže	Oni uključuju Bluetooth, Wi-Fi, lokalnu mrežu, komunikaciju u blizini, itd. Sistem telemedicinskih usluga baziran na kućnoj mreži je ranjiv na sigurnosne napade koji se odnose na prijenos otvorenog teksta s kraja na kraj i čovjeka u sredini (MITM) prijetnje.
Gateway uređaji	Gateway djeluje kao posrednik između pacijenta i telemedicinskog sistema, čineći sistem ranjivim na sigurnosne napade koji se odnose na lažni gateway, krađu/gubitak gateway-a i MITM prijetnje.
Telemedicinski uređaji	Telemedicinski terminal baziran na ugrađenom operativnom sistemu u realnom vremenu je bezbjedan od neovlašćenog pristupa, ali uređaj (npr. pametni telefon) zasnovan na operativnom sistemu opšte namene koristi eksterne aplikacije; stoga je ranjiv na sigurnosne napade.
Sistem telemedicine	On obrađuje podatke pacijenata i možda je povezan sa srodnim agencijama preko vladinog mrežnog čvorišta. Može se koristiti za bežičnu komunikaciju između računara i opreme za vježbanje pacijenata za telekonsultacije. Privlači sigurnosne prijetnje povezane sa zlonamjernim kodom, ilegalnim pristupom mreži, MITM napadima i izmjenom/falsifikovanjem aplikacije za telemedicinu.
Pacijenti ili korisnici	Većina njih živi u udaljenom regionu, bez ikakve obuke o cyber sigurnosti ili sa malo interesovanja za cyber sigurnost; stoga je njihovo korištenje telemedicinskih terminala lako primiti sigurnosne napade zbog gubitka uređaja, slabih lozinki, grešaka u korištenju uređaja itd.
Pružaoci telemedicinskih usluga	Sistem telemedicine uglavnom uključuje interakcije između doktora i pacijenta i doktora. Ranjiv je na sigurnosne napade zbog prisluškivanja, curenja važnih podataka, izmjena recepta i grešaka u korištenju uređaja.

Za mnoge organizacije, povećana ulaganja u usklađenost (privatnost), sigurnost informacija (telerad/kontinuitet poslovanja), lanac nabavke i upravljanje hitnim situacijama pomoći će razvoju infrastrukture. Telemedicina omogućava da zdravstveni radnici pregledaju veći broj pacijenata uz pridržavanje protokola samoizolacije za suzbijanje bolesti u vezi sa COVID-19. Pacijenti dobijaju edukaciju, praćenje i konsultacije. (Evropska komisija, 2010a.) U pandemiji COVID-19, tele-zdravstvena usluga je potrebna za smanjenje kretanja pacijenata, a time i za smanjenje infekcije. Predložena je telemedicinska laboratorijska usluga zasnovana na IoT-u i oblaku. Konkretno, liječnici, medicinske sestre i drugo medicinsko osoblje iz različitih bolnica radili su zajedno koristeći svoje udružene bolničke oblake, kreirali virtuelni zdravstveni tim i dovršili radni tok zdravstvene zaštite uz sigurnost. (Evropska komisija, 2010b.)

6.3. Cyber sigurnost zasnovana na blockchain tehnologiji

Blockchain tehnologija nudi nepromjenjive i distribuirane knjige sa zapisima koji se mogu revidirati, što je idealno za praćenje svake imovine u upravljanju lancem nabavke. Zavisi od distribuiranog, bezbjednog i nepromjenljivog okvira za čuvanje podataka koji čuva privatnost. (Statista, 2021a) Vlade i bolnice mogu identificirati slučajeve za koje se sumnja na COVID-19, lokacije povezane s prijavljenim slučajevima i zaražena područja s visokim rizicima koristeći blockchain. Blockchain je također korišten da garantuje sigurnost zdravstvenih podataka. (Fernandez, S., Jenkins, P., Vieira, B., 2020.) Tokom pandemije COVID-19 važno je pratiti pacijente i analizirati njihove simptome ili reakcije na bolest. Blockchain je korisna platforma u mnogim zemljama pogođenim COVID-19, posebno u zdravstvu. (Evropska komisija, 2010b.)

Nedovoljni podaci za procjenu rizika od zaraze ili prenošenja COVID-19 uzrokovali su brzo širenje COVID-19 općenito. Mnogi pacijenti su bili asimptomatski i mehanizam prijenosa COVID-19 nije bio dobro shvaćen sve do maja 2020. Kada cyber napadi dovedu do bloka informacija, odobreni blockchain nudi dvije prednosti: 1) bilo ko u medicinskom konzorcijumu može provjeriti kada i kako transakcije i dolazi do informacija; 2) blokiranje informacija će promijeniti heš. Stoga pacijenti mogu prenositi lične zapise bez ikakvog rizika od neovlaštenog mijenjanja. (Evropska komisija, 2010b.) Za sekvence SARSCoV-2 (uzrokuje COVID-19) stvoreno je zatvoreno čvorište koje kontrolira pristup i zabranjuje redistribuciju. Komercijalne težnje mogu odgoditi razmjenu podataka jer patentni poticaji ometaju otvorenu diseminaciju. Blockchain omogućava dokaz postojanja određenih objekata podataka i njihovog sadržaja. (Evropska komisija, 2010b.) Podaci o COVID-19 iz Centara za kontrolu i prevenciju bolesti (CDC) uključuju podatke i metapodatke. Blockchain pomaže u upravljanju medicinskim podacima, identificiranju obrazaca simptoma, praćenju lanaca opskrbe medicinskim

potrepštinama i lijekovima i povećanju dijagnostičke točnosti i efikasnosti liječenja. (CybSafe, 2020)

“Društvene iinternet stvari” (SIoT) integrira ljude i pametne uređaje koji komuniciraju unutar društvene strukture IoT-a, koja se često odvija putem IoT platformi. Cloud IoT ekosistemi su ometajući, ali sa mnogim problemima u pogledu sigurnosti i privatnosti. SIoT ima iste rizike. Zlonamjerni softver je usmjeren na ljude koji rade kod kuće i zdravstvene organizacije. Blockchain može poboljšati sigurnost i privatnost digitalnih zdravstvenih sistema. Predložen je sistem baziran na blockchainu koji nudi sigurno upravljanje kućnom karantenom. (Evropska komisija, 2020a.)

Predložen je novi okvir zasnovan na blockchainu za integraciju međudržavnih za COVID-19 i praćenje zaraženih ili testiranih pacijenata na globalnom nivou. Okvir se razvija kao novi sistem sa dvije komponente: pristupnom tačkom i jednom decentralizovanom virtuelnom mašinom sa podrškom za Ethereum. (Evropska komisija, 2020b.) Blockchain se koristi za premošćivanje jaza u vidljivosti lanca opskrbe zbog svojih sigurnosnih karakteristika kao što su otpornost na neovlašteno korištenje, otpornost na haširanje i nepromjenjivost. COVID-19 je poremetio mnoge globalne lance nabavke. Rapid Supplier Connect, IBM-ova mreža zasnovana na blokčejnu, razvijena je kako bi pomogla u jačanju medicinskog lanca opskrbe tokom pandemije COVID-19. (Evropska komisija, 2020b.)

Za nadzor COVID-19 predloženo je spajanje AI s blockchainom za sisteme za samotestiranje i praćenje. Ne samo da takav sistem samotestiranja može postići veću stopu testiranja, već omogućava i stratifikaciju rizika sumnjivih slučajeva. (Evropska komisija, 2020d.) Blockchain je također efikasan u razmjeni podataka između grupa. Primjene blockchaina i AI u zdravstvu mogu se sažeti na sledeći način: analiza zdravstvenih podataka, daljinsko praćenje pacijenata, upravljanje lancem snabdijevanja lijekovima i farmaceutskim proizvodima, upravljanje elektronskim medicinskim kartonima (EMR) itd. (Evropska komisija, 2020e.)

Upravljanje elektronskim zdravstvenim kartonima (EHR) s blockchainom može smanjiti kliničku pristranost. (Evropska komisija i visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku, 2016.) Problem interoperabilnosti između različitih EHR sistema može se riješiti korištenjem odvojenih blockchain sistema. (Evropska komisija, 2020d.) Tabela 7 prikazuje SWOT analizu korištenja modela zasnovanog na blockchain-u u zdravstvu.

Tabela 7. SWOT korištenja modela zasnovanog na blockchainu u zdravstvu (Evropska komisija, 2020e.)

	Pozitivno	Negativno
Interni	Prednosti	Slabosti
	- Transparentnost - Povjerenje - Nepromjenljivost - Privatnost - Disintermedijacija i automatizacija	- Nedostatak fleksibilnosti - Kreiranje mogućih viljuški - Operativni troškovi - Potreba za većom sposobnošću skladištenja podataka na lokalnim serverima
Eksterni	Mogućnosti	Prijetnje
	- Povećanje svijesti o tehnologiji i razvoj nove ekspertize - Veća saradnja među operaterima u sistemu zdravstvene zaštite	- Nedostatak stručnosti - Otpor na promjene - Nedostatak povjerenja u primjenu nove tehnologije od strane zdravstvenih radnika

6.4. COVID-19 izaziva trend rasta cyber kriminala

Toliko se toga promijenilo otkako je Europol objavio prošlogodišnju Procjenu prijetnje od organiziranog kriminala na internetu (IOCTA). Globalna pandemija COVID-19 koja je pogodila svaki kutak svijeta natjerala nas je da preispitamo svoja društva i izmislimo način na koji radimo i živimo. Tokom izolacije, okrenuli smo se internetu za osjećaj normalnosti: kupovina, rad i učenje na mreži u neviđenim razmjerima. U ovoj novoj normi Europol objavljuje svoju 7. godišnju IOCTA. IOCTA nastoji da mapira pejzaž prijetnji od cyberog kriminala i razumije kako na njega reagira policija. Iako nam je kriza COVID-19 pokazala kako kriminalci aktivno iskorištavaju društvo u njegovom najranjivijem dijelu, ovo oportunističko ponašanje kriminalaca ne bi trebalo zasjeniti cjelokupni pejzaž prijetnji. U mnogim slučajevima, COVID-19 je pojačao postojeće probleme. (Vijeće Evropske unije, 2020c.)

Društveni inženjering i phishing ostaju efikasna prijetnja za omogućavanje drugih vrsta cyber kriminala. Kriminalci koriste inovativne metode kako bi povećali obim i sofisticiranost svojih napada, a neiskusni cyber kriminalci mogu lakše provoditi phishing kampanje putem kriminala kao usluge. Kriminalci su brzo iskoristili pandemiju za napad na ranjive ljude; phishing, online prevare i širenje lažnih vijesti postali su idealna strategija za cyber kriminalce koji žele prodati stvari za koje tvrde da će spriječiti ili izliječiti COVID-19. (Vijeće Evropske unije, 2020c.)

Šifriranje i dalje ostaje jasna karakteristika sve većeg broja usluga i alata. Jedan od glavnih izazova za provođenje zakona je kako pristupiti i prikupiti relevantne podatke za krivične istrage. Vrijednost mogućnosti pristupa podacima o kriminalnoj komunikaciji na šifrovanoj

mreži je možda najefikasnija ilustracija kako šifrirani podaci mogu osigurati provođenju zakona ključne tragove izvan područja cyberog kriminala.

Ransomware napadi su postali sofisticiraniji, ciljajući određene organizacije u javnom i privatnom sektoru putem izviđanja žrtava. Dok je pandemija COVID-19 izazvala porast cyber kriminala, napadi ransomware-a bili su ciljani na zdravstvenu industriju mnogo prije krize. Štaviše, kriminalci su uključili još jedan sloj u svoje ransomware napade prijeteći da će na aukciji prodati sadržane podatke, povećavajući pritisak na žrtve da plate otkupninu. Napredni oblici zlonamjernog softvera najveća su prijetnja u EU: kriminalci su transformirali neke tradicionalne bankarske trojance u modularni zlonamjerni softver kako bi pokrili više digitalnih otisaka prstiju na računaru, koji se kasnije prodaju za različite potrebe. (Vijeće Evropske unije, 2020c.)

Glavne prijetnje u vezi s iskorištavanjem zlostavljanja djece na mreži ostale su stabilne posljednjih godina, međutim otkrivanje materijala o seksualnom zlostavljanju djece na mreži je naglo skočilo na vrhuncu krize COVID-19. Prestupnici i dalje koriste brojne načine da sakriju ovaj zastrašujući zločin, kao što su P2P mreže, platforme društvenih mreža i korištenje šifriranih komunikacijskih aplikacija. Dark web zajednice i forumi su mjesta susreta gdje je učešće strukturirano s pravilima afilijacije kako bi promovirali pojedince na osnovu njihovog doprinosa zajednici, što oni čine tako što snimaju i objavljuju svoje zlostavljanje djece, ohrabrujući druge da učine isto. Livestream zlostavljanja djece i dalje raste, postajući još popularniji nego inače tokom krize COVID-19 kada su ograničenja putovanja spriječila počinitelje da fizički zlostavljaju djecu. U nekim slučajevima se koriste aplikacije za video ćaskanje u platnim sistemima, što postaje jedan od ključnih izazova za provođenje zakona jer se ovaj materijal ne snima. (Vijeće Evropske unije, 2020c.)

Zamjena SIM kartice, koja omogućava počiniteljima da preuzmu račune, jedan je od novih trendova u ovogodišnjoj IOCTA-i. Kao vrsta preuzimanja naloga, zamjena SIM kartice omogućava kriminalcima pristup osjetljivim korisničkim nalozima. Zločinci na prijevaru mijenjaju ili prenose SIM kartice žrtve u onaj koji je u posjedu kriminalaca kako bi presreli korak jednokratne lozinke u procesu autentifikacije. (Vijeće Evropske unije, 2020c.)

U 2019. i početkom 2020. godine bio je visok nivo volatilnosti na dark webu. Životni ciklus Dark web marketa je skraćen i ne postoji jasno dominantno tržište koje je poraslo u protekloj godini. Tor ostaje poželjna infrastruktura, međutim kriminalci su počeli da koriste druge

decentralizovane tržišne platforme fokusirane na privatnost za prodaju svoje ilegalne robe. Iako ovo nije nova pojava, ove vrste platformi su počele da se povećavaju tokom prošle godine. OpenBazaar je vrijedan pažnje jer su se određene prijetnje pojavile na platformi tokom prošle godine, kao što su artikli povezani sa COVID-19 tokom pandemije. (Vijeće Evropske unije, 2020c.)

7. UTJECAJ COVID-19 NA CYBER KRIMINAL I CYBER PRIJETNJE U EVROPSKOJ UNIJI

Ovaj dio rada opisuje evoluciju cyber napada, na osnovu različitih zvaničnih izvještaja agencija za provođenje zakona i kompanija za cyber sigurnost. Fokusira se na prioritetne EMPACT-ove "cyber kriminalne napade na informacione sisteme" i analizira glavne vrste zlonamjernog softvera (bankarski trojanci, ransomware, cryptojacking i botnet malver) i njihovu evoluciju tijekom pandemije COVID-19. U ovom dijelu radu su predstavljeni vektori prijetnji na mreži (napadi bazirani na e-mailu, napadi zasnovani na webu, prijevare na društvenim mrežama) i oflajn prijetnje i njihov utjecaj na informacione sisteme. Disruptivne tehnologije poput umjetne inteligencije, kvantnog računarstva, 5G tehnologije, interneta stvari (IoT) i društvenih mreža predstavljaju mnoge prednosti, ali ih loši akteri mogu iskoristiti protiv nas. Ovaj članak naglašava važnost obrazovanja i obuke u ovoj oblasti i preporučuje mjere za borbu protiv fenomena cyber kriminala.

Mjere koje su poduzele nacionalne vlade od marta 2020. povećale su korištenje digitalnih aplikacija za više od 10 posto, a uz to i nesigurnost stanovništva. Koronavirus je napravio jasan put za cyber kriminalce, koji su korištenjem društvenih medija i platformi za razmjenu poruka stekli lak pristup potencijalnim žrtvama uz značajan porast aktivnosti povezanih sa seksualnim zlostavljanjem i eksploatacijom djece i medicinskim prijevarama. Prema Facebook-ovim Vladinim zahtjevima za korisničke podatke, platforma društvenih medija (uključujući Instagram) primila je više od 150.000 ukupnih zahtjeva agencija za provođenje zakona u Evropskoj uniji u 2020. (prvih šest mjeseci) - sa preko 40.000 zahtjeva više nego u 2019. godini. U istom periodu 2020. godine, Europol je dobio od Nacionalnog centra za nestalu i eksploatisanu djecu i sve veći broj uputnica, u poređenju sa istim periodom 2019.

Internetska distribucija krivotvorenih farmaceutskih i sanitarnih proizvoda, uključujući testove i vakcine povezane s koronavirusom, također se pokazala kao kriminalni oportunizam tokom pandemije COVID-19. U avgustu 2020. godine, evropske carinske agencije presrele su više od 8,5 miliona maski bez CE sertifikata.

Prema najnovijim statistikama, pandemija COVID-19 ubrzala je proces digitalne transformacije, s brojnim uslugama koje su se preselile na internet. Nova tehnologija nudi mnoge prednosti, ali predstavlja i određene opasnosti, budući da bi sadašnje nedostatke mogli iskoristiti cyber kriminalci. Učestalost cyber incidenata i cyber napada nedavno je dramatično porasla zbog nedostatka svijesti i obuke o cyber sigurnosti.

Cyber kriminal trenutno koristi prednost nesigurnosti ljudi i potražnje za informacijama. Rasprostranjenost bezbjednosnih incidenata poslednjih godina potkrepljuje kontinuiranu eskalaciju eksploatacije ranjivosti u virtuelnom informacionom okruženju, pretežno od strane organizovanih grupa i državnih aktera. Složenost cyber napada se također razvija alarmantnom brzinom, što je kulminiralo tako što su neki od njih objavljivani kao globalne epidemije zbog njihovog utjecaja i zamaha širenja. Jačanje spremnosti i zagovaranje proaktivnog pristupa u fazama dizajniranja i kreiranja digitalne infrastrukture ključni su napori da se cyber prostor učini sigurnim mjestom za sve.

Preovlađujući tipovi cyber napada koji se danas primjenjuju izvode se kroz malver aplikacije, uskraćivanje usluge (DoS, DDoS), ometanjem i iskorišćavanjem elektronske pošte i web aplikacija, a posljednju kategoriju predstavljaju APT napadi (Advanced Persistent Threats). Podaci sa najkorišćenijih platformi društvenih medija ukazuju na porast korisnika u periodu od tri godine, koji se povećava iz godine u godinu, zbog pristupa internetu i pametnim uređajima koje ljudi dobijaju svake godine i porasta uzrokovanog pandemijom.

Eurofond sugerira da je blizu 40% ljudi koji rade u EU pretvoreno u puni rad na daljinu 2020. godine. Više od 80 posto ljudi širom svijeta ohrabruje rad na daljinu, nadalje, kao i najveći broj cyber kriminala na phishing napadima na društvenim mrežama, zlonamjernom softveru koji se šalje putem ćaskanja, prijevarama na društvenim mrežama i materijalima o seksualnom zlostavljanju djece. Društveni inženjering i phishing promijenili su se i evoluirali, zbog čega su korisnici žedni informacija uglavnom o temi COVID-19.

7.1. Vrste krivičnih djela

7.1.1. Malware napadi

Kako je izvijestila Agencija Evropske unije za cyber sigurnost (ENISA) u svom najnovijem izvještaju, ovo je najrašireniji tip cyber napada. Zlonamjerni softver ili zlonamjerni softver je svaki zlonamjerni kod ili program koji je štetan za računarski sistem. Ti dijelovi zlonamjernog koda mogu biti virusi, trojanci, crvi i, na osnovu njihovog opsega, ransomware, špijunski softver, lažni ili zastrašujući softver. (ENISA, 2021.)

Prema ENISA-i, svaki dan se na internetu objavi više od 230.000 novih vrsta zlonamjernog softvera. Osim toga, postoji porast od 50% malvera dizajniranog za krađu ličnih podataka i 265% porast zlonamjernog softvera bez datoteka. (ENISA, 2021.) Tradicionalni zlonamjerni softver je umetnut u datoteke, tako da su korisnici mogli zaraziti svoje kompjuterske sisteme

kada preuzimaju ove zaražene datoteke sa web stranica ili e-pošte. Danas, cyber kriminalci koriste zlonamjerne skripte koje mogu kompromitirati mete kada korisnici pristupaju ugroženim web stranicama, a nemaju pravilno konfigurirane alate za cyber sigurnost.

U vrijeme pandemije došlo je do porasta zlonamjernog softvera dizajniranog za mobilne uređaje. Većina korisnika nedovoljno štiti svoje mobilne uređaje, tako da ih cyber kriminalci lako mogu kompromitovati kako bi ukrali lične podatke ili akreditive za online bankarstvo.

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	—	—
2	Web-based Attacks	—	↗
3	Phishing	↗	↗
4	Web application attacks	—	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	—	—
9	Insider threat	↗	—
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	—	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Slika 2. Najveće prijetnje prema ENISA za period 2019-2020 (ENISA, 2021.)

Kompjuterski virusi su aplikacije s različitim destruktivnim mogućnostima, razvijene da zaraze jedan ili više računarskih sistema. Virusi imaju dvije glavne karakteristike: vezuju se za bezopasni softver i sami se razmnožavaju u zaraženom sistemu. Trojanci su softver koji prikriva

njihovu pravu prirodu kroz legitimne operacije, ali u stvarnosti, oni pokušavaju da razotkriju sistemske i aplikativne ranjivosti i otvore portove u operativnom sistemu, kako bi napadačima omogućili daljinski pristup. Kompjuterski crvi su aplikacije sa destruktivnim efektima, koje inficiraju kompjuterski sistem, a zatim se šire internetom. (Arora, A., Nandkumar, A. i Telang, R., 2006.) Crvi su dizajnirani da traže sisteme sa ranjivostima, zaraze ih i izvode štetne operacije, a zatim pokušaju da se dalje razmnožavaju.

Adware je klasa softvera koji, jednom instaliran na sistem, agresivno prikazuje oglase korisniku. Špijunski softver je softver koji tajno bilježi različite informacije o aktivnostima korisnika, kao što su pritiskanja tipki, snimci ekrana pokrenutih aplikacija ili privatni detalji o njihovoj upotrebi Interneta. Ransomware je vrsta zlonamjernog softvera koji ograničava pristup podacima računala šifriranjem datoteka i traži od korisnika da izvrši plaćanje kako bi uklonio šifriranje. Neki tipovi pokrenutog softvera šifriraju podatke na tvrdom disku sistema, kao i sve datoteke kojima može pristupiti preko lokalne mreže iu Cloud skladištu, kako bi utjecali na sigurnosne kopije, dok drugi mogu jednostavno blokirati računalni sistem i prikazati poruke kako bi primorali korisnika na plaćaju otkupninu.

Rogueware su aplikacije koje obmanjuju korisnike o lažnim infekcijama otkrivenim u njihovom operativnom sistemu i traže plaćanje kako bi ih uklonile. Najčešće, oni tvrde da uklanjaju zlonamjerni softver pronađen na računarima, ali u stvari instaliraju dodatni softver sa sve štetnijim efektima. Scareware je softver koji izaziva anksioznost i strah kod korisnika u svrhu reklamiranja lažnih aplikacija. (Arora, A., Nandkumar, A. i Telang, R., 2006.)

7.1.2. Napadi uskraćivanja usluge

Kompromitacija rada određenih internet servisa je eksplicitna, namjeravana posljedica napada uskraćivanja usluge (DoS/DDoS). Jedan od najčešćih DDoS napada je preplavljivanje paketa, kroz koje se nesrazmjeran broj Internet paketa šalje sistemu žrtve s ciljem blokiranja svih dostupnih konekcija i usporavanja mrežnog prometa do crawl-a, što dovodi do potpunog zaustavljanja usluge koje pruža napadnuti sistem.

7.1.3. E-mail napadi

Napadi koji koriste ili ciljaju e-poštu eksponencijalno su porasli u posljednje vrijeme. Na osnovu krajnje svrhe cyber kriminalaca, napadi e-poštom mogu pripadati jednoj od nekoliko kategorija. E-mail bombardovanje se sastoji od slanja značajnog broja e-mailova sa velikim prilozima na određenu adresu e-pošte. To dovodi do iscrpljivanja slobodnog prostora na serveru, čineći taj nalog e-pošte nedostupnim. (Evropska komisija, 2021a.) Prevara e-pošte je

praksa slanja e-pošte sa izmijenjenom, najčešće lažnom adresom pošiljaoca, kako bi se sakrio pravi identitet pošiljaoca i potencijalno izvukli povjerljivi detalji ili podaci potrebni za pristup nalogu. Spam je napad koji se sastoji isključivo od slanja neželjene e-pošte s komercijalnim sadržajem. Svrha ovih e-poruka je da prevare svoje primaoce da pristupe nepristojnim - stranicama i kupe usluge ili proizvode sumnjive prirode. Krađa identiteta putem e-pošte je vrsta napada koja se brzo širi, u kojoj se šalju posebno kreirane poruke kako bi se odredilo da primaoci pruže informacije o bankovnom računu, podatke o kreditnoj kartici, lozinke ili druge privatne podatke (ENISA, 2021.) ili da izvrše plaćanje naizgled u ime nekoga poznatog žrtvi.

7.1.4. Napadi na web aplikacije

Napadi usmjereni na web aplikacije doživljavaju brzi rast, potaknuti eksplozivnim razvojem web tehnologija koje podržavaju i poboljšavaju dizajn visoko interaktivnih, dinamičnih platformi sadržaja, uz dosljednu interakciju korisnika. Takve platforme neizbježno sadrže ranjivosti koje cyber kriminalci mogu iskoristiti da zaobiđu sigurnosne mjere i dobiju neovlašteni pristup korisničkim podacima. (ENISA, 2021.)

Najčešći oblici ovog napada su:

- SQLi: SQL injekcija (Structured Query Language) je praksa izmjene SQL upita koji se prenosi u bazu podataka umetanjem podataka, što mijenja logiku i svrhu upita. Ovo omogućava napadaču da izbjegne mehanizme provjere autentičnosti.
- XSS (Cross-Site Scripting) dozvoljava napadaču da modifikuje ili ubaci skripte u web lokaciju, koje se zatim izvršavaju u pretraživaču žrtve kada pristupe zaraženom sajtu.
- Falsifikovanje zahtjeva na više lokacija (CSRF): zlonamjerni akter iskorištava uspostavljeni odnos povjerenja između autentifikovanih korisnika i web aplikacije. Na taj način oni dobijaju kontrolu nad sesijom žrtve, dozvoljavajući im da se imitiraju kao legitimni korisnik i izvrše bilo koju radnju u svom kontekstu.
- Čovjek u sredini: cyber kriminalci presreću komunikaciju između korisnika i web stranica kako bi dohvatili nešifrirane vjerodajnice.

7.1.5. Napredne trajne prijetnje

Napredne trajne prijetnje predstavljaju složene cyber napade koji se izvode tokom dužeg vremenskog perioda, usmjereni na određenu metu, s brojnim ciljevima, kao što su kompromitiranje sistema, izvlačenje informacija o/iz žrtve ili, povremeno, podmetanje obmanjujućih informacija. Mete mogu biti vlade, vojne instalacije, korporacije ili čak pojedinci.

(Arora, A., Nandkumar, A. i Telang, R., 2006.) APT se obično sastoji od nekoliko komplementarnih cyber napada. Generalno, takva operacija obuhvata prikupljanje podataka o meti, identifikaciju potencijalnog eksploatacije i njegovo praćenje, inficiranje mete i iskorištavanje bilo koje izvađene formacije, u skladu sa sveobuhvatnim opsegom. Konvencionalno, samo terorističke organizacije ili nacionalne države posjeduju tehnološku sposobnost i potrebna finansijska sredstva da ispolje ovako razrađene cyber napade.

7.1.6. Materijal o seksualnom zlostavljanju djece

Tokom pandemije, većina škola je prešla na online učenje. Neprekidni pristup internetu, platformama društvenih medija i aplikacijama za slanje poruka, povećao je opasnost za potencijalne žrtve. Tokom početka pandemije 2020. i karantina koje su vlade nametnule, više od 168 miliona djece moralo je ostati kod kuće zbog zatvorenih škola, kaže UNICEF- ov fond za hitne slučajeve Ujedinjenih naroda.[6]

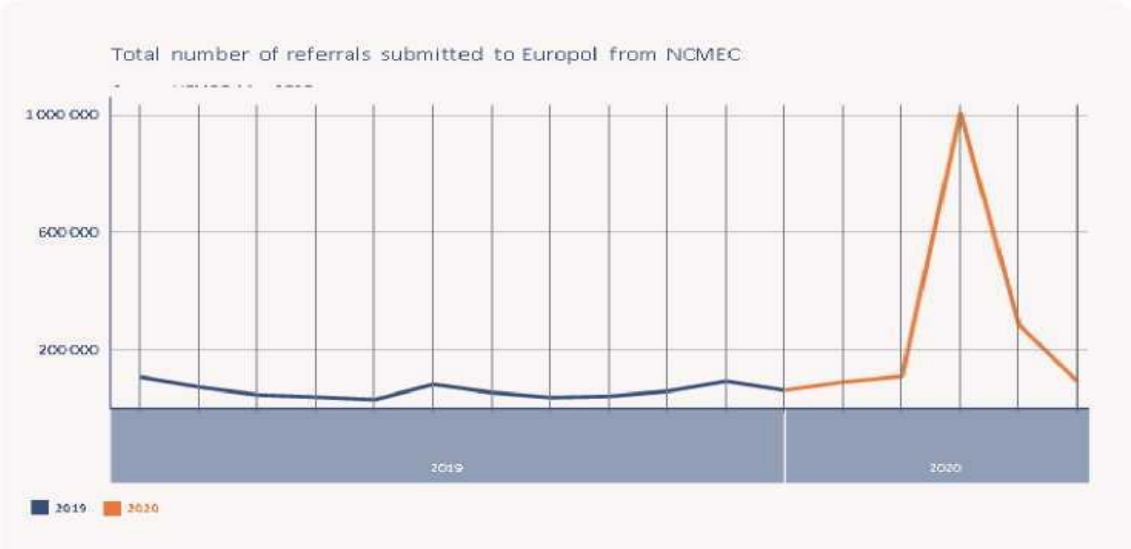
Na osnovu dostupnih podataka[7] od Evropske agencije za saradnju u provođenju zakona (Europol), povećan je nivo aktivnosti za distribuciju CSAM-a između marta i aprila 2020. (Slika 3). Aktivnosti se kreću od djece koju kriminalci prisiljavaju da proizvode materijal, ili prestupnika koji dobijaju pristup putem društvenih medija ili platformi za messenger koristeći metode phishinga. (Vijeće Evropske unije, 2020c.)

Za vrijeme pandemije modus operandi cyber kriminalaca u vezi sa CSAM-om, posebno se dogodio putem dijeljenja P2P mreže, distribucije jedan na jedan i masovnog dijeljenja na platformama društvenih medija, korištenjem lažnih naloga na društvenim mrežama, enkripcijom (TOR, VPN), na kraju materijali koji završavaju na dark webu. (Vijeće Evropske unije, 2020c.) Podaci NCMEC-a, Nacionalnog centra za nestalu i eksploatisanu djecu i Europola ukazuju na 106% porasta ove vrste aktivnosti.[8]

6 https://www.unicef.org/press-releases/schools-more-168-million-children-globally-have-been-completely-closed

7 Izvještaj EUROPOL-a o iskorištavanju izolacije: Prestupnici i žrtve seksualnog zlostavljanja djece na internetu tokom pandemije COVID-19, jun 2020.

8 Izvještaj Europola, Hvatanje virusa - cyber kriminal, dezinformacije i pandemija Covid-19, 3. april 2020.



Slika 3. Ukupan broj preporuka koje je NCMEC dostavio Europolu (Vijeće Evropske unije, 2020c.)

Još jedna vrsta cyber uznemiravanja koja se povećala 2020. je zoom bombardovanje, kada neželjeni korisnici ulaze na video sastanke sa zlonamjernim ciljem, uključujući dijeljenje pornografskih slika ili slika mržnje. (Vijeće Evropske unije, 2020c.)

Što se tiče potreba za obukom za provođenje zakona, na osnovu izvještaja[9] koje je objavila CEPOL, Evropska agencija za obuku za provođenje zakona, OSINT alati, metode istraga, dark web, kao i prevencija i saradnja trebale bi se dalje baviti potrebama obuke za provođenje zakona. (Vijeće Evropske unije, 2020c.)

7.1.7. Medicinske prevare

Prevare vezane za COVID-19 svjedoče o tri talasa razvoja, počevši od prvog i drugog talasa koji se odnose na lijekove, prevenciju i lažne testne komplete i završavajući lažnim farmaceutskim tretmanima. (Vijeće Evropske unije. 2020a.)

Studija[10] koji je objavio Journal of Medical Internet Research Public Health and Surveillance, spominje preko 6 miliona tweetova i preko 200.00 Instagram postova sa sumnjivom marketinškom prodajom zdravstvenih proizvoda COVID 19 od marta do maja 2020. Objave su uključivale lažne COVID proizvode za prodaju, lažni kompleti za testiranje, preventivni lijekovi, efikasna vakcina ili terapeutski tretmani. (Arora, A., Nandkumar, A. i Telang, R., 2006.)

9 Izvještaj CEPOL-a o utjecaju COVID-19 na operacije provođenja zakona i potrebe za obukom, 1. jula 2020.
10 Tim KM i ostali, Veliki podaci, obrada prirodnog jezika i duboko učenje za otkrivanje i karakterizaciju nelegalne prodaje proizvoda COVID-19: Infoveillance studija na Twitteru i Instagramu, avgust 2020.

7.1.8. Cyberbullying

Evropska komisija definiše cyber maltretiranje kao ponovljeno verbalno ili psihičko uznemiravanje koje pojedinac ili grupa sprovodi protiv drugih putem internetskih usluga i mobilnih telefona, a na osnovu nedavnih izvještaja, mržnja između djece i tinejdžera tokom onlajn časova porasla je za 70%, posebno tokom Zoom-a ili druge platforme za video konferencije, ali i na platformama za igre kao što su Discord ili druge popularne aplikacije društvenih medija.

8. MJERE OTPORNOSTI

Pandemija COVID-19 potaknula je društvo na nepredviđenu novu normalu. Uz povećano usvajanje digitalne tehnologije, svjedoci smo novijih oblika izazova cyber sigurnosti. U ovom radu, mi naučno ispitujemo ovaj uticaj izazvan pandemijom na cyber sigurnost identifikujući ključne teme, ispitujući njihovu vremensku i prostornu evoluciju. Tehnički, da bismo to učinili, koristimo najsavremeniji algoritam za mašinsko učenje bez nadzora tematskih modela. Izgradili smo ogroman korpus od preko 50 izvora literature uzete iz perioda 2010-2021, uključujući i recenzirane i nerecenzirane izvore literature. Zanimljiva zapažanja koja nalazimo su da su nakon pandemije COVID-19, zdravstvena zaštita, cyber otpornost novije dodane teme cyber sigurnosti koje se istražuju u recenziranoj literaturi. Tipično, u periodu prije COVID-19, fokus je bio na izgradnji novih modela napada, sistema za otkrivanje upada, između ostalog. U literaturi koja nije vršnjakinja, nakon COVID-19, primjećujemo da su noviji oblici napada kao što je društveni inženjering, sporedni kanal koji su podstakli interesovanje. Obično se ova zajednica u periodu prije COVID-19 fokusirala mnogo na finansijski cyber kriminal. Pored toga, nekoliko cyber tema, kao što su sigurnost mreže, otkrivanje zlonamjernog softvera, sistemi kontrole upada i sigurnost industrijskog kontrolnog sistema ostaju važni zauvjek. Zanimljivo je da dok radimo vremensku analizu cyber tema u literaturi koja je recenzirana svih vremena, primjećujemo da su blokada i kršenja privatnosti postali manje popularni u odnosu na prethodne godine. Slično tome, istraživanja mrežne privatnosti su u trendu u literaturi koja nije recenzirana svih vremena, što može biti odraz nedavnog fokusa industrije na modele rada od kuće i prelazak na infrastrukturu u oblaku, što je posljedično vodeći put istraživanja. Takođe je primetno da cyber sigurnost u poddomenama kao što su skimeri uređaja i kršenje kreditnih kartica pokazuje znake pada.

Cyber sigurnost se odnosi na ljude. Ova sažeta fraza objašnjava neraskidivu vezu između bioloških i tehnoloških domena. Ljudi upravljaju uređajima i mrežama. Oni su najvažniji akteri na kraju svakog procesa koji se nalazi u cyber prostoru. Ljudi su ti koji razvijaju tehnologiju i kreiraju pravila upravljanja njom. Oni se također moraju suočiti s posljedicama svakog negativnog ili neprijateljskog ponašanja u cyber prostoru.

Kada je u pitanju (još uvijek) najvažniji oblik društvene organizacije, države, pitanja kibernetičkog prostora i cyber sigurnosti su izuzetno složena. Oni su politički, društveni i ekonomski. Kada je u pitanju još viši oblik organizacije, odnosno zajednica država, što je primjer Evropske unije, pitanje koherentne politike je izuzetno teško.

EU želi cyber otpornost na sistemskom, panevropskom nivou. Dokumenti analizirani u ovom radu svjedoče o takvom pristupu. Parametri ovog „stanja otpornosti“ potiču iz ukupnog *modusa operandi EU*. Zajednica nije jedinstvena struktura sa jasnim razdvajanjem nadležnosti unutar ogromnog ekosistema institucija. Važan nivo otpornosti će se postići kada cela konstrukcija funkcioniše efikasno, posebno u vremenima teških kriza. Hitne situacije velikih razmjera, koje počinju neprijateljskim akcijama u evropskim mrežama, zahtijevat će fleksibilnost. EU se nije suočila sa ovakvom situacijom. Za sada nije bilo velikih smetnji u mreži. Naravno, ozbiljni cyber napadi, poput slučajeva ransomware-a u Evropi ili aktivnosti dezinformisanja u vezi sa pandemijom u cyber prostoru, DDoS napadi a drugi su pogodili evropsku infrastrukturu. Ovim napadima upravljano je u okviru mogućnosti i resursa država članica. Međutim, postoji osjećaj opasnosti od velikog cyber napada na cyber elemente kritične infrastrukture i rasplamsavanja multisektorske krize. Neki događaji u bliskoj geografskoj blizini EU mogu se opisati kao predznake nadolazećih kriza. Malver “Industroyer”, koji je pogodio ukrajinsku energetsku mrežu, bio je prvi cyber napad koji je ciljao fizičku infrastrukturu od operacije protiv iranskih nuklearnih instalacija sa Stuxnet bugom. Ovaj konkretan slučaj nudi uvid u ono što se može očekivati u konfliktnom svijetu, gdje se neprijateljske operacije protiv EU u borbi mogu kanalisati kroz cyber prostor sa potencijalno razornim efektima u umreženim evropskim društvima. EU ima ograničene autonomne potencijale koji ne zavise od država članica. Dakle, cyber otpornost EU znači prije svega njenu efikasnost u koordinaciji država članica koje održavaju superiornost u donošenju odluka i izvođenju stvarnih operacija u cyber prostoru. Iako je EU bezbjednosna zajednica, njene nadležnosti i mogućnosti su ograničene politikama država članica. U strategijama cyber sigurnosti EU, otpornost je koherentnost. U osnovi, povećan nivo koordinacije i saradnje EU tretira kao uspjeh, posebno u sferi sigurnosti. Očigledno je da tako složeno pitanje kao što je cyber sigurnost zahtijeva jasan pravni okvir. Kreiranje gore navedenih sistema propisa je korak ka postizanju otpornosti ovog tipa. Treba napomenuti da ogromna količina privatnih subjekata funkcioniše u okviru evropskog sistema cyber sigurnosti, pa je postojanje sveobuhvatne pravne kičme ključno. Odnosi se ne samo na zajedničku političku reakciju na krize velikih razmjera, već i na strogo tehničku koordinaciju u slučaju napada na više nivoa na elemente kritične infrastrukture, koji mogu biti u vlasništvu privatnih operatera. Postizanje ove vrste koherentnosti svakako je jednako otpornosti odozgo prema dolje i korak ka panevropskoj spremnosti.

Sistemska otpornost na nivou EU mora biti upotpunjena otpornošću izgrađenom odozdo prema gore. To je pitanje od najveće važnosti u slučaju cyber zaštite (oko 80% cyber napada su posljedice neadekvatnih navika), svijesti o prijetnjama svakodnevnim aktivnostima građana EU

i, posebno, u slučaju eksternih dezinformacija. EU delegira veliki dio odgovornosti za ove sfere na države članice, ali i vodi vlastite programe, usmjerene na izgradnju znanja i širenje obrazaca dobre prakse (također za MSP i institucije civilnog društva).

Cyber ranjivosti nisu ograničene na tehničku domenu - integritet firewall-a, softvera i hardvera u njihovim najnaprednijim funkcijama (SCADA). Oni obuhvataju široku konstelaciju prijetnji, ali autor tvrdi da su dezinformacije inducirane kroz cyber prostor potencijalno najštetniji fenomen iz perspektive EU. Prema ENISA-i, „društva će morati razviti odbranu od takvih napada, posebno onih koji imaju za cilj potencijalno utjecati na demokratske procese kao što su izbori, zakonodavne procedure, provođenje zakona i pravosuđe. U kontekstu cyber sigurnosti, kampanje dezinformacija treba pažljivo pratiti i temeljito analizirati kako bi se suprotstavili sličnim napadima u budućnosti. ”Ovaj način razmišljanja je razrađen u konkretnim aktivnostima institucija EU i oličen u East StratCom Task Force-u, koji je odgovoran za otkrivanje, analizu i razotkrivanje lažnih vijesti u ekosistemu evropskih elektronskih medija. Značaj otpornosti u ovom sektoru cyber sigurnosti pokazalo je nekoliko značajnih događaja - migracijska kriza, referendum o Bregzitu, ruske informativne operacije i agresivne aktivnosti Kine tokom pandemije. Otpornost na operacije dezinformacija postaje jedna od najvažnijih karakteristika cjelokupnog sigurnosnog stava. Dezinformacije imaju potencijal da poremete čitave društvene sisteme, razotkriju i pogoršaju negativne emocije. Ruske i kineske kampanje dezinformacija su objedinjene u opštem cilju slabljenja EU kao celine i njene sposobnosti da djeluje kao konsolidovani akter. Stoga je cyber otpornost, iako nije toliko „efikasna“ kao antiterorizam ili vojna sigurnost, strateška potreba u sve nestabilnijem svijetu.

Složeni evropski sistem cyber sigurnosti opterećen je ozbiljnim nedostacima. Ako je cyber otpornost u odnosima između institucija EU (horizontalno) i odnosa između njih i država članica (vertikala) ključna, renacionalizacija političkog stava ovih potonjih je najvažnija prepreka. Države članice imaju tendenciju da akumuliraju odgovornosti za politike cyber sigurnosti na nacionalnom nivou. Evropske vlasti su svjesne superiornosti država u domenu sigurnosti i priznaju njihovu ulogu u zvaničnim propisima. To proizilazi iz duboke dileme projekta evropskih integracija - nevoljkosti da se izgrade međusektorski mehanizmi vođeni EU i, kao rezultat, ograničavanje uloge država članica. EU prepoznaje potrebu za transnacionalnim, međusektorskim pristupom pitanjima poput cyber sigurnosti, ali njene napore efektivno blokiraju države članice. Stoga, fragmentacija politike cyber sigurnosti EU ostaje najvažniji izazov na putu postizanja sveobuhvatne cyber otpornosti. Drugi nivo cyber otpornosti, imuniteta na dezinformacije i pravilnih navika u umreženom okruženju građana i organizacija

izuzetno je teško postići. EU ulaže mnogo sredstava u podizanje svijesti. U slučaju dezinformacija, tehnike su toliko sofisticirane da, kako Ondrej Filipec tvrdi, „čak i stručnjaci ponekad mogu upasti u zamku kada misle da mogu to otkriti i razgraničiti“. Pitanje je kompleksno, a glavna prepreka je često nespremnost da se reformiše tradicionalni obrazovni sistem, usmjeri ka vještinama kritičkog mišljenja i razvije digitalna pismenost među starijima. Što se tiče cyber zaštitnih navika, napori na izgradnji otpornosti često su uskraćeni nedostatkom usklađenosti sa sigurnosnim politikama i dobrim praksama. Stvaranje pravilnih, odgovornih stavova je dug proces temeljnog rada. Nema sumnje da su vlade država članica svjesne ovog izazova, ali ekonomske determinante, politička pitanja i tradicionalni pristupi obrazovanju mogu biti u suprotnosti sa širokom vizijom EU o strateškoj cyber otpornosti. Gore analizirane tačke samo su manifestacija složenog pitanja cyber otpornosti u EU. Oni proizilaze kako iz složenosti pitanja tako i iz strukturnih problema same Zajednice.

Hipoteze postavljene na početku ove ograničene studije bile su pozitivno potvrđene. Okvir cyber sigurnosti EU predstavlja duboko razumijevanje okruženja kibernetičkog prostora, posebno sadašnjih i budućih prijetnji. Postoji i jasan dokaz da će implementacija politika programiranih okvirom naići na velike prepreke, koje su rezultat strukturnih nedostataka u samoj EU i dinamično mijenjajući politički, ekonomski i društveni pejzaž. EU vidi cyber sigurnost kao multidimenzionalni sigurnosni domen, gdje se transnacionalne prijetnje velikih razmjera ukrštaju s opasnostima za građane, organizacije i poslovne subjekte. Dakle, područje evropskog interesa za kibernetičku sigurnost odražava zamršenost samog cyber prostora. EU konstruiše sopstvene resurse i sposobnosti da efikasno koordinira politike cyber sigurnosti država članica i, prije svega, operacije odgovora na krize.

Evropska agenda o cyber sigurnosti također pretpostavlja ulaganje u inicijative odozdo prema gore kao što su obrazovanje i podizanje svijesti. Glavni cilj ovog širokog skupa aktivnosti je dvostruka cyber otpornost. EU ima za cilj postizanje otpornog operativnog sistema i glatke horizontalne (ekosistem evropskih institucija) i vertikalne (institucije i države članice) koordinacije. Drugi, ali ne manje važan, cilj je otpornost građana i društvenih institucija različitih tipova (od NVO do preduzetništva) odozdo prema gore protiv dezinformacija i „svakodnevnih“ opasnosti širenja prisustva u cyber prostoru. Te aktivnosti susreću se s preprekama zbog sukoba interesa država članica i nevoljnosti da se promijene navike ponašanja u cyber prostoru. Ostaje da se vidi da li će EU prevazići ove prepreke. Ipak, cyber sigurnost i cyber otpornost su pitanja od ključne važnosti. Snaga i pozicija EU u međunarodnom okruženju koje se brzo mijenja ovisit će o ishodu ovih napora.

Vjerujem da moj rad pruža ključne uvide u trendove i izazove cyber sigurnosti korisni i za akademike i praktičare. To će pomoći preduzećima da identifikuju sopstvene strateške nedostatke, čime će racionalno prepoznati svoje potrebe za cyber bezbjednošću, unajmiti radnu snagu i upravljati zalihama. Akademici će imati koristi od našeg rada tako što će prisvojiti svoja istraživanja o predstojećim izazovima cyber sigurnosti i trendovskim nišnim domenima. Budući rad je da se korpus učini inkluzivnijim i uključi medijske izvještaje. Još jedno zanimljivo proširenje je automatsko zaključivanje oznake iz distribucije tema.

9. ZAKLJUČAK

Preoblikovanjem razvoja cyber sigurnosti EU kroz sočiva historijskog i diskurzivnog institucionalizma, bilo je moguće identificirati ključne ideje koje su proizvele diskurzivne ovisnosti o putevima u ovoj oblasti. Isto tako važno je da je korištenjem ovog pristupa bilo moguće bolje razumjeti uslove u kojima se nastavlja ili mijenja zavisnost od idejnog puta u institucijama i kako to može utjecati na narative na nivou programa i politike. U oblasti cyber sigurnosti, iako su kritične tačke poslužile da se olakšaju promjene u osnovnim idejama koje oblikuju programe i politike, to nisu nužno kritične tačke koje se mogu očekivati. Dok je širenje COVID-19 u velikoj mjeri destabiliziralo ekonomije, društva i svakodnevni život javnih i privatnih aktera, čini se da samo po sebi nije poslužilo kao kritična točka u razumijevanju cyber sigurnosti u EU. Umjesto toga, pandemija je rezultirala postojećom idejnom pozicijom da je provajderi društvenih medija, umjesto da doprinose efikasnoj cyber sigurnosti, zapravo ometaju. Shvatajući ih i kao oblik hibridne prijetnje cyberoj sigurnosti, ali i kao širu prijetnju demokratskim vrijednostima EU, pozicija EU na platformama društvenih medija oblikovana je ranijim kritičnim momentom, 2016. godine. U tom trenutku, diskurs o uloga ovih platformi u digitalnom okruženju bila je podložna retoričkim promjenama naglašavajući njihovu ulogu u širenju dezinformacija. Povećano širenje dezinformacija u vezi sa COVID-19 u 2020. godini pružilo je osnovu za kontinuitet politike, a ne za prekid, pojačavajući zabrinutost u vezi sa ulogom ovih platformi kao izvora nesigurnosti, u poređenju s privatnim dobavljačima rješenja za cyberu sigurnost, za koje se smatra da dijele interese i vrijednosti EU. Porast cyber napada i povećano širenje dezinformacija tokom pandemije, posebno u vezi s prirodom bolesti i njenim porijeklom, stoga nije rezultiralo značajnim pomakom u razmišljanju EU na ovom polju, već je umjesto toga ojačalo postojeće percepcije o uloge različitih pružatelja sigurnosti, te je stoga služio da se osigura idejni kontinuitet u postojećim pristupima politike, a ne da rezultira njihovom promjenom.

Općenito, ovaj rad naglašava da događaji koji na svojoj površini izgledaju kao da "mijenjaju sve", bilo da se radi o realizaciji masovne potrošačke upotrebe interneta u kasnim 1990-im, ili zaista o pandemiji 2020, moraju biti pažljivo procijenjeni u smislu promjena. oni zaista usađuju. Iako može doći do dalekosežnih i dugotrajnih promjena u aspektima kreiranja politike EU u područjima kao što su zdravstvo ili migracije, jer nastojimo bolje razumjeti i kontrolirati aspekte odgovora na pandemiju koji se odnose na tretman i kretanje ljudi koji mogu biti zaraženi novim koronavirusom, u području cyber sigurnosti, ne vidimo istu dramatičnu promjenu u politikama, već umjesto toga, jačanje postojećih ideja i stavova, iako s obnovljenim zamahom i ubrzanjem djelovanja. Dezinformacije i uloga društvenih medija u njihovom širenju nisu nove i

neočekivane. Umjesto toga, nesposobnost ili nespremnost društvenih medija da ga efikasno suzbiju rezultirala je potvrdom prethodno postojećeg idejnog stava Komisije, što je rezultiralo najavama politika koje teže prethodno navedenim ciljevima, a ne predstavljaju dramatičnu promjenu. Ovo gledište je naglasilo mnoge izazove cyber sigurnosti povezane s COVID-19; međutim, nijedan od identificiranih izazova nije nov, ali je jasno da ih je pogoršala pandemija. Dakle, problemi su postojali i prije pandemije, a adekvatna rješenja još uvijek nisu dostupna. Promjene i poremećaji moraju se dogoditi u srži interakcija i odnosa između čovjeka i uređaja, s fokusom na povjerenje i na to kako su ljudi napredovali jedni s drugima tokom hiljada godina, čak i u prijetećim situacijama.

Trebali bismo iskoristiti ovu priliku da se suočimo s tim izazovima prije nego što se nagomilaju na pandemiji. U ekstremnim situacijama, normalno je da se moraju napraviti izuzeci kako bi se dali prioritet određenim dijelovima društva ili infrastrukture. Međutim, to se mora postići na transparentan i kontroliran način kako bi nakon što se izuzetna situacija smirila, ljudi lako mogli vratiti svoje temeljno pravo na privatnost (Evropska komisija, 2018b.), čiji je gubitak u prošlosti utjecao na mnoge živote. Također moramo tražiti pravo na povjerenje u tehnologiju, uz prikladniju i poboljšanu cyber sigurnost, za sigurniju i zdraviju ljudsku populaciju.

Tokom pandemije COVID-19, postoji mnogo cyber rizika zbog djelovanja ljudi, kao i kvarova u sistemima i tehnologiji. Rad na daljinu i aplikacije zasnovane na IoT-u su ranjive na cyber napade. Telehealth pruža mogućnost zaštite pacijenata, liječnika, medicinskih sestara itd. od infekcije COVID-19. Međutim, telehealth stvara rizike za cyber sigurnost i privatnost. Blockchain pomaže u upravljanju pandemijom i poboljšava privatnost i sigurnost digitalnih zdravstvenih sistema. Kombinacija blockchaina i AI olakšava analizu zdravstvenih podataka, daljinsko praćenje pacijenata, upravljanje EMR-om, upravljanje lancem nabavke lijekova i farmaceutskih proizvoda, itd.

COVID-19 ušao je u novo doba cyber svijesti jer kompanije sada šalju svoje zaposlenike da rade od kuće uz ograničenu sigurnost. Virtuelne privatne mreže (VPN) i serveri će igrati značajnu ulogu u cyber sigurnosti budućnosti. Ne samo da mnoge kompanije širom svijeta rade po modelima od kuće, hiljade kompanija koje rade od kuće sada niču i suočavaju se sa sličnim problemima. Cyber kriminalci su previše svjesni ograničene sigurnosti koju pojedinci mogu pružiti kod kuće. Novi izazovi za pojedince koji rade kod kuće uključuju pronalaženje jednostavnih, ali sigurnih rješenja za cyber sigurnost.

LITERATURA

1. Arora, A., Nandkumar, A. i Telang, R., 2006. Da li se učestalost napada na sigurnost informacija povećava s otkrivanjem ranjivosti? Empirijska analiza. Granice informacionih sistema , 8(5), str.350-362.
2. Benkler, Y., Tilton, C., Etling, B., Roberts, H., Clark, J., Faris, R., Kaiser, J., Schmitt, C. (2020.) Prevara glasača putem pošte: Anatomija dezinformacione kampanje. Istraživačka publikacija Berkman centra br. 2020-6. 2. oktobar. https://ssrn.com/abstract=3703701.
3. CybSafe (2020) Ljudska greška je kriva za 9 od 10 kršenja cyber podataka u Velikoj Britaniji u 2019. 7. februar. https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber data-breaches-in-2019/.
4. Collett, R., Barmpalious, N., Pawlak, P. (2021) Međunarodna izgradnja cyber kapaciteta: Globalni trendovi i scenariji. Institut za sigurnosne studije EU. Luksemburg. https://www.iss.europa.eu/content/international-cyber capacity-building-global-trends-and-scenarios.
5. ENISA (2019) Izazovi i mogućnosti izborne cyber sigurnosti. Februar. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities.
6. ENISA (2021) Cyber sigurnost za MSP - Izazovi i preporuke. 28. jun. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes.
7. Evropska komisija (2021a) Borba protiv dezinformacija. https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation_en.
8. Evropska komisija (2021b) Obraćanje predsjednice von der Leyen o stanju Unije. 15. septembar. https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701.
9. Eurostat (2021) IKT specijalisti - Statistika o teško popunivim radnim mjestima u preduzećima. juna. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_-_statistics_on_hard-to-fill_vacancies_in_enterprises.
10. Euractiv (2021) Njemačka ispituje tvrdnje o hakovanju predizbornog poslanika od strane Rusije. 10. septembar. https://www.euractiv.com/section/global-europe/news/germany-probes-claims-of-pre-election-mp-hacking-by-russia/.
11. Fernandez, S., Jenkins, P., Vieira, B. (2020.) Digitalna migracija Evrope tokom COVID-19: prevazilaženje širokih trendova i prosjeka. McKinsey, 24. jul. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/europes-digital-migration-during-COVID-19-getting-past-the-broad-trends-and-averages.

12. Malekos Smith, Z., Lostri, E. (2020) Skriveni troškovi cyber kriminala. McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.
13. Morgan, S. (2019.) Talenata za cyber sigurnost za stvaranje 3,5 miliona nepopunjenih radnih mjesta širom svijeta do 2021. Cybercrime Magazine, 24. oktobar. https://cybersecurityventures.com/jobs/.
14. Grupa za saradnju NIS (2018) Zbornik o cyber sigurnosti izborne tehnologije, Aneks 1. CG Publikacija 03/2018, jul. https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf.
15. Statista (2021a) Oblasti sa najvećim nedostatkom vještina cyber sigurnosti u organizacijama širom svijeta u 2021. godini, prema kategoriji tehnologije. https://www.statista.com/statistics/1259502/cybersecurity-skills-shortage-tech-categories-worldwide/.
16. Statista (2021b) Potrošnja na cyber sigurnost širom svijeta od 2017. do 2021. (prilagođeno za COVID-19). https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending.
17. Tasheva, I. (2017) Evropska politika cyber sigurnosti: trendovi i perspektive. EPC Policy Brief, 8. jun. https://www.epc.eu/content/PDF/2017/European_cybersecurity_policy.pdf.
18. UK, Odsjek za digitalno, kulturu, medije i sport. (2021) Istraživanje kršenja cyber sigurnosti 2021. 24. mart. https://www.gov.uk/government/statistics/cyber_security-breaches-survey-2021/cyber security-breaches-survey-2021
19. Verizon (2020) 2020 izvještaj o istragama o kršenju podataka. https://enterprise.verizon.com/resources/reports/dbir/2020/dbir-report/.
20. Verizon (2021) 2021 izvještaj o istragama o kršenju podataka. Rezultati i analiza. https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/.
21. Carrapico, H. i B. Farrand. 2017. „“Dijalog, partnerstvo i osnaživanje za sigurnost mreže i informacija”: Promjena uloge privatnog sektora od objekata regulacije do onih koji oblikuju regulativu.” Promjena društva za kriminalno pravo 67 (3): 245-263. doi:10.1007/s10611-016-9652-4.
22. Preporuka Komisije 2020/518, 2020. „O zajedničkom paketu alata Unije za korištenje tehnologije i podataka za borbu protiv krize COVID-19 i izlazak iz krize, posebno u vezi s mobilnim aplikacijama i korištenjem anonimnih podataka o mobilnosti.”
23. Deflem, M. i E. Shutt. 2006. “Primjena zakona i prijetnje i mjere kompjuterske sigurnosti.” U Handbook of Information Security, Information Warfare, Social, Legal,

and International Issues, and Security Foundations, urednik H. Bidgodi, 200-209, John Wiley & Sons, Bakersfield, California.

24. EEAS, 2020. „Kratka procjena narativa i dezinformacija oko pandemije COVID-19 (ažurirano 23. april - 18. maj) “ EU Vs DEZINFORMACIJE. 30. avgust 2020. https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-COVID19-pandemic-updated-23-april-18-may/
25. Eurofound, 2020. “Rad, rad na daljinu i COVID-19 ” Eurofound. 22. avgust 2020. https://www.eurofound.europa.eu/data/COVID-19/working-teleworking
26. Evropska komisija, 1985. “Bijela knjiga: Završetak unutrašnjeg tržišta (br. COM(85) 310 Final).” Evropska komisija, Brisel.
27. Evropska komisija, 1990. “Prijedlog odluke Vijeća u oblasti sigurnosti informacija (br. COM(90) 314 final-SYN288).”
28. Evropska komisija, 1993. „Rast, konkurentnost, zapošljavanje: Izazovi i putevi naprijed u 21. vijek - Bijela knjiga (br. COM(93)700 Final).”
29. Evropska komisija, 1999. “E-Evropsko informaciono društvo za sve”. Komunikacija o inicijativi Komisije za Specijalno Evropsko vijeće u Lisabonu (br. COM(1999) 687 final).
30. Evropska komisija, 2001. „Mrežna i informaciona sigurnost: Prijedlog za pristup evropskoj politici (br. COM(2001) 298 Final). Brisel.”
31. Evropska komisija, 2010a. „Strategija unutrašnje sigurnosti EU na djelu: pet koraka ka sigurnijoj Evropi (br. COM(2010) 673 Final)“
32. Evropska komisija, 2010b. „Digitalna agenda za Evropu (br. COM(2010) 245 Final/2). Brisel.”
33. Evropska komisija, 2018a. „Borba protiv dezinformacija na mreži: Evropski pristup (br. COM(2018) 236)“
34. Evropska komisija, 2018b. “Prijedlog uredbe o sprječavanju širenja terorističkog sadržaja na internetu (br. COM(2018) 640 Final)”
35. Evropska komisija, 2018c. “Kodeks prakse EU za dezinformacije na mreži.” Evropska komisija, 2019. “Kodeks prakse o dezinformacijama: prvi godišnji izvještaji.”
36. Evropska komisija, 2020a. "Oblikovanje digitalne budućnosti Evrope."
37. Evropska komisija, 2020b. “Evropska strategija za podatke (br. COM(2020) 66).”
38. Evropska komisija, 2020c. “Nova industrijska strategija za Evropu (br. COM(2020) 102 Final).”
39. Evropska komisija, 2020d. „Bijela knjiga o umjetnoj inteligenciji: Evropski pristup izvrsnosti i povjerenju (br. COM(2020) 65).“

40. Evropska komisija, 2020e. „Trenutak Evrope: Popravite i pripremite se za sljedeću generaciju (br. COM(2020) 456 Final)“
41. Evropska komisija i visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku, 2016. “Zajednički okvir za borbu protiv hibridnih prijetnji (br. JOIN(2016) 18)”.
42. Evropska komisija i visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku, 2020a. „Saopćenje o globalnom odgovoru EU na COVID-19 (br. JOIN(2020) 11 Final)”.
43. Evropska komisija, Visoki predstavnik Evropske unije za vanjske poslove i sigurnosnu politiku, 2013. „Strategija cyber sigurnosti Evropske unije: Otvoren, siguran i siguran cyber prostor (br. JOIN(2013) 1). Brisel.”
44. Evropsko vijeće, 1996. “Zaključci Predsjedništva Vijeća (br. decembar).” Dublin.
45. Evropsko vijeće, 1999. “Zaključci Vijeća. Tampere.”
46. Evropsko vijeće, 2015. “Zaključci Vijeća (br. EUCO 11/15, CO EUR 1, CONCL 1)”
47. Fahey, E. 2014. “Kibernetski kriminal i donošenje pravila o cyber sigurnosti u EU: mapiranje internih i eksternih dimenzija sigurnosti EU.” European Journal Risk Regul. EJRR 5 (1): 46. doi:10.1017/S1867299X00002944.
48. Fioretos, O., T. G. Falleti i A. Sheingate. 2018. “Historijski institucionalizam u političkim naukama”. U Oksfordskom priručniku za historijski institucionalizam, urednik O. Fioretos, T. G. Falleti i A. Sheingate, 3-30. Oxford: Oxford University.
49. Hoffman, B. L., E. M. Felter, K.-H. Chu, A. Shensa, C. Hermann, T. Wolynn, D. Williams i B. A. Primack. 2019. „Nije sve u autizmu: novi krajolik raspoloženja protiv vakcinacije na Facebooku.” Vakcina 37 (16): 2216-2223. doi:10.1016/j.vaccine.2019.03.003.
50. Ladi, S. 2011. “Think Tanks, diskurzivni institucionalizam i promjena politike.” U Social Science and Policy Challenges-Democracy, Values and Capacities, Research and Policy, priredio G. Papanagnou, 205-220. Pariz: UNESCO Publishing.
51. Leon, LD, Rafferty, PD i Herschel, R. (2012) „Zamjena godišnjeg budžeta prognozama zasnovanim na poslovnoj inteligenciji“, Inteligentno upravljanje informacijama, 04(01), str. 6-12.
52. Lischka, J. A. 2019. “Strateška komunikacija kao diskurzivni institucionalni rad: kritička analiza diskursa razgovora Marka Zuckerberga o legitimnosti u Evropskom parlamentu.” International Journal Strategy Commun. 13: 197-213. doi:10.1080/1553118X.2019.1613661.
53. Lomas, N., 2020. „Tehnološki divovi moraju da se otvore o “infodemiji” korona virusa, kažu zakonodavci EU." TechCrunch. 30. avgust 2020.

https://social.techcrunch.com/2020/06/10/tech-giants-must-open-up-about-the-coronavirus-infodemic-say-eu-lawmakers/

54. Uredba 2019/881, 2019. "Širenje (ne)povjerenja: dezinformacije o COVID-19 i vladina intervencija u Italiji." Media Commun 8 (2): 458-461. doi:10.17645/mac.v8i2.3219.
55. Kunnathuvalappil Hariharan, N. (2018). "IZVORI PODATAKA ZA POSLOVNU INTELIGENCIJU". Međunarodni časopis za inovacije u inženjerskim istraživanjima i tehnologiji, vol. 5, br. 11, novembar 2018, str. 75-80.
56. Madrigal, A.C., 2018. „Belgijski zakonodavac kritikuje i ruga se Marku Zuckerbergu " Atlantik. 28. avgust 2020. https://www.theatlantic.com/technology/archive/2018/05/a-belgian-legislator-berates-and-scoffs-at-mark-zuckerberg/560960/
57. Maruster, L. (2003) Pristup mašinskog učenja za razumijevanje poslovnih procesa. Citeseer.
58. May, AU (2017) „Tradicionalno budžetiranje u današnjem poslovnom okruženju", Journal of Applied Finance & Banking, 7(3), str. 111-120.
59. Mahoney, J. i K. Thelen, ur. 2010. Objašnjavanje institucionalnih promjena: dvosmislenost, djelovanje i moć, ilustrovano izdanje. ed. ed. New York: Cambridge University Press, Cambridge.
60. Peters, B. G. 2019. Institucionalna teorija u političkim naukama, četvrto izdanje: Novi institucionalizam. 4 ed. Northampton, MA: Edward Elgar Publishing.
61. Uredba 2019/881, 2019. „O ENISA-i (Agencija Evropske unije za cyberu sigurnost) i o certifikaciji cyber sigurnosti informacijske i komunikacijske tehnologije."
62. Ross, A. 2019. "Vrijednosti i problemi." U Finding Political Identities: Young People in a Changing Europe, Palgrave Politics of Identity and Citizenship Series, urednik A. Ross, 45-95. Springer International Publishing, Cham, Švicarska. doi:10.1007/978-3-319-90875-52.
63. Schmidt, V. A. 2008. "Diskurzivni institucionalizam: moć objašnjenja ideja i diskursa." Godišnji pregled političkih nauka 11 (1): 303-326. doi:10.1146/annurev.polisci.11.060606.135342.
64. Schmidt, V. A. 2010. "Pomirenje ideja i institucija kroz diskurzivni institucionalizam." U Ideas and Politics in Social Science Research, edited by D. Beland and R. H. Cox, 47-64. New York: Oxford University Press, Oxford, Engleska.
65. Schmidt, V. A. 2020. "Teoretiziranje institucionalnih promjena i upravljanja u evropskim odgovorima na pandemiju COVID-19." Journal of European Integration 42: 8.

66. Steinmo, S. 2008. “Šta je historijski institucionalizam?” U Pristupi u društvenim naukama, ur. D. Della Porta i M. Keating, 118-138. Cambridge: Cambridge University Press.
67. Steinmo, S., K. Thelen, i F. Longstreth, ur. 1992. Structuring Politics: Historical Institutionalism in Comparative Analysis. New York: Cambridge University Press, Cambridge England.
68. Streeck, W. i K. A. Thelen. 2005. Izvan kontinuiteta: Institucionalna promjena u naprednim političkim ekonomijama. Oxford: Oxford University Press.
69. Torfing, J. 1999. Nove teorije diskursa: Laclau, Mouffe i Žižek. Oxford: Blackwell Publishers.
70. Treverton, G. F., A. Thvedt, A. R. Chen, K. Lee i M. McCue. 2018. Addressing Hybrid Threats. Centar za asimetrične studije prijetnji; Evropski centar izvrsnosti za suzbijanje hibridnih prijetnji, Švedski univerzitet odbrane. Dostupno na: https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf
71. Venturini, T. i R. Rogers. 2019. “„Istraživanje zasnovano na API-ju” ili kako studije digitalne sociologije i novinarstva mogu učiti od kršenja podataka Facebooka i Cambridge Analytica.” Digit Journal 7 (4): 532-540. doi:10.1080/21670811.2019.1591927.
72. Vijeće Evropske unije. 1997. “Akcioni plan za borbu protiv organiziranog kriminala (br. C251/1-15.8.97)” Službeni list Europskih zajednica,1. Brisel
73. Vijeće Evropske unije. 2005. “Okvirna odluka Vijeća 2005/222/JHA od 24. februara 2005. o napadima na informacione sisteme (br. L 69/67).” Službeni list Evropske unije
74. Vijeće Evropske unije. 2020a. “Zaključci Vijeća o COVID-19 (br.” U Oj C, 57/4)
75. Vijeće Evropske unije. 2020b. „Zaključci Vijeća o oblikovanju digitalne budućnosti Evrope (br.“ OJ 2020C: 202.
76. Vijeće Evropske unije, 2020c. “Zaključci Vijeća o medijskoj pismenosti u svijetu koji se stalno mijenja (br. OJ C 193)”
77. Vijeće Evrope (2020) Demokratija hakovana? Kako odgovoriti? Rezolucija 2326. http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=28598&lang=e.
78. Waterson, J. 2018. Pet stvari koje smo naučili iz nastupa Marka Zuckerberga u Evropskom parlamentu. Guardian. Dostupno na: https://www.theguardian.com/technology/2018/may/22/five-things-we-learned-from-mark-zuckerbergs-european-parliament-appearance

79. Wolff, S., A. Ripoll Servent i A. Piquet. 2020. “Reakcije Evropske unije na pandemiju: Prilagodljivost u vremenima trajne vanredne situacije.” Journal of European Integration 42: 8.
80. Wolff, S. i S. Ladi. 2020. “Reakcije Evropske unije na pandemiju: Prilagodljivost u vremenima trajne vanredne situacije.” Journal of European Integration 42: 8.
81. Europol, IOCTA 2020 izvještaj, 2022., Dostupno na web stranici: https://www.europol.europa.eu/media-press/newsroom/news/COVID-19-sparks-upward-trend-in-cybercrime