Petar Čelik*
Miodrag Komarčević**
Milovan Dimić***

UDK 343.53:[616.98:578.834
343.533::004

DOI: 10.5937/MegRev2004049C
Pregledni naučni članak
Primljen 28.04.2020.
Odobren 20.06.2020.

KONVERGENCIJA PANDEMIJE KOVID 19 I SAJBER KRIMINALA: KONTEKST I OPSEG******

Sažetak: *Duboka i sveopšta kriza globalnih razmera izazvana pandemijom korona virusa generisala je direktno ili indirektno brojne i različite pojave i procese koji su u potpunosti promenili percepciju i način života i rada i na taj način uspostavili novi kontekst, radikalno promenivši konfiguraciju i pejzaž bezbednosti. Aktuelna kriza je, istovremeno, postala glavni akcelerator nekoliko važnih trendova i transformacija u području sajber bezbednosti: najpre iniciranja, zatim podrške procesima privatizacije, militarizacije i sekuritizacije ovog područja. U strateškom okruženju koincidirala su dva potpuno različita, po nastanku, ispoljenim efektima i načinu delovanja, recentna procesa, čija je rezultanta jedna fundamentalna asimetrija: raste intenzitet, dinamika i učestalost sajber napada, dok se drastično smanjuju operativne sposobnosti države i drugih aktera, na planu njihovog sprečavanja i suzbijanja.*
Težišni cilj istraživanja je, najpre, sagledavanje, a zatim i utvrđivanje globalnog konteksta koji produkuje različite i vrlo kompleksne međuodnose, interakcije, uslovljenosti između širenja pandemije sa jedne, i ekspanzije rasta hibridnih pretnji, a naročito sajber kriminala, sa druge strane sa značajno redizajniranim sofisticiranim formama, modalitetima, narativima i ciljevima.
Usled složenosti, višedimenzionalnosti i relevantnosti problemsko-predmetnog sklopa, u toku istraživanja primenjen je standardni metodološki instrumentarij, sa osloncem na DESK metode.
U zaključnom delu, konverzacijski smisao i hibridna priroda sajber pretnji naglašavaju važnost i potrebu inoviranja postojećih javnih politika i bezbednosnih agendi u kreiranju kombinovanog hibridnog odgovora sa naglašenim sinergetskim efektima.

Ključne reči: *pandemija, sajber bezbednost, hibridne pretnje, disruptivne tehnologije*

* Visoka strukovna škola za preduzetništvo, Beograd; petar2celik@gmail.com

** Visoka strukovna škola za preduzetništvo, Beograd; mile.komarcevic@gmail.com

*** Pravni fakultet Megatrend univerziteta, Beograd; m.dimic@megatrend.edu.rs

**** Ovaj rad je napisan u okviru trogodišnjeg Projekta Pravnog fakulteta Megatrend Univerziteta, Beograd, broj: 2044/20 od 01.10.2020. pod nazivom „Bezbednosni izazovi savremenog društva" (FPBISD).

1. Uvod

Tekuća transformacija i „veliko resetovanje" imaju višedimenzionalni karakter, pri čemu brojni procesi, kretanja i pojave, nose sve više bezbednosnu konotaciju. Među brojnim strateškim varijablama i vektorima koji određuju stanje bezbednosti na globalnom i lokalnom nivou, posebno se danas izdvajaju dva procesa: digitalizacija i pandemija, dok njihova vremenska i prostorna podudarnost ima konvergentan značaj i smisao.

Nagli i ubrzani razvoj digitalnih tehnologija i disruptivnih inovacija za svega nekoliko godina u potpunosti su izmenili, najpre naše vizure i mogućnosti društveno-ekonomskog razvoja, a usled lake dostupnosti i masovne proizvodnje tehnoloških sredstava i uređaja, drastično su promenili način proizvodnje, rada, poslovanja, modela funkcionisanja, zabave, kulture, informisanja i sl., do granica koje su do skora bile teško razumljive i praktično nedostižne.

Takav trend razvoja generisao je novo strateško okruženje u kome transformacija pod digitalnim pritiskom postmoderno društvo prevodi u digitalno doba, odnosno doba „postnormalnosti" koga karakterišu dinamični procesi umrežavanja „svega sa svime i svuda", što rezultira uvođenjem novih „klizećih" pravila i obrazaca života i rada koji se razvijaju pod stalnom pretnjom i pritiscima tekuće disrupcije.

Široka primena novih ili tzv. konvergentnih tehnologija dovela je do opštih trendova rasta, uvodeći revoluciju ne samo u ekonomiji i industriji, već i u svim drugim povezanim oblastima. Međutim, dinamični tehnološki napredak prate i brojni izazovi, pretnje i rizici iz sajber prostora što iziskuje potrebu oblikovanja prema promenama, adekvatnog odgovora u vidu sajber bezbednosti.

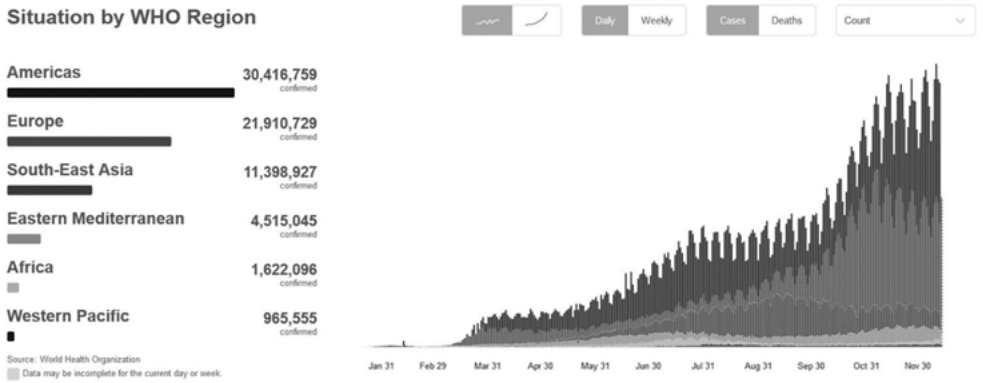
Upravo takvo dinamično i nestabilno okruženje nastalo dubokim promenama u digitalnom prostoru, trasira i usmerava razvoj društva koje se prema naučniku H. Saurungu naziva „VUCA" pravac ili doba, što je u stvari akronim za nestabilnost, ugroženost, složenost i dvosmislenost vremena u kome živimo[1].

Postojeći pravac i okruženje dodatno usložnjava i opterećuje pojava nastanka, a zatim i razmere pandemijske krize uzrokovane korona virusom 19, produkujući sinergetski efekat u sadejstvu sa ugrožavajućim pretnjama i rizicima koji dolaze iz sajber prostora. Neočekivana konvergencija između digitalne transformacije i pandemije kao rezultantu ima eksponencijalni rast sajber izazova i pretnji koji podjednako ugrožavaju, kako pojedince, tako i kompanije i ekonomiju, ali i vojno-bezbednosni sektor i državu kao celinu.

[1] Ovaj tekst je originalno napisan 2016. godine kao doprinos knjizi, ali je objavljen u blago izmenjenoj verziji nešto kasnije na blogu na web stranici http://www.herbert.saurugg.net/2016/blog/vernetzung-und-komplexitaet/complexity-systemic-risks-and-converging-technologies, pristupljeno 11. decembra 2020.

2. Uticaj pandemije i sajber bezbednosti

Prema mišljenju brojnih stručnjaka, pandemija uzrokovana korona virusom, obzirom na globalne razmere, intenzitet, obuhvat, dinamiku širenja, učestale pikove i njihovu trajnost, kao i mnoštvo različitih agregatnih uticaja, posledica i pratećih i sukcesivnih implikacija, spada u najveću globalnu elementarnu nepogodu – katastrofu u poslednjih 100 godina.



Izvor: Svetska zdravstvena organizacija (WHO), decembar 2020

Grafik 1: *Globalna pandemijska situacija na dan 14.12.2020. godine*

Upravo zbog tih karakteristika i naglašenih specifičnosti, tekuća pandemija se suštinski razlikuje od drugih elementarnih nepogoda ili katastrofa, u prvom redu zbog širine i obuhvata svetske ugrožene populacije, mikro i makro-ekonomskih posledica koje su bez presedana u istoriji, velike nezaposlenosti, siromaštva, otežanog funkcionisanja kritičnih usluga i javnih službi, preopterećenosti globalne digitalne infrastrukture i internet platformi, itd.

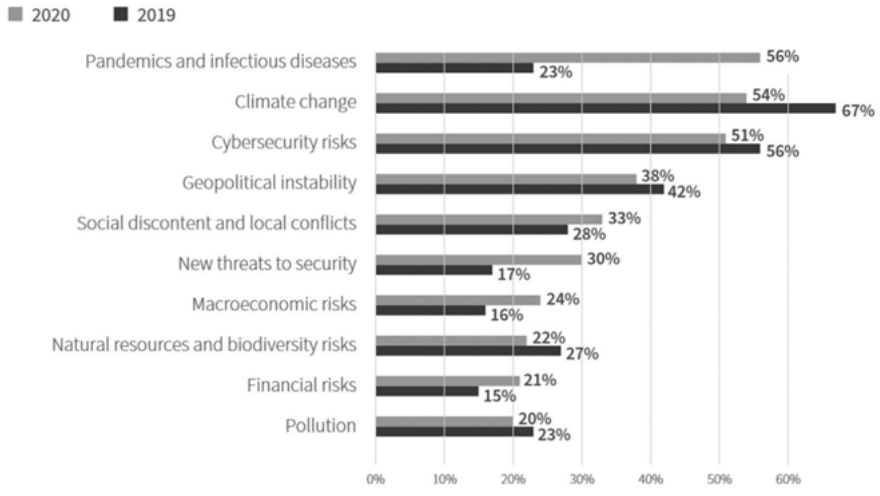
Pandemija nije samo zdravstvena kriza, kao što se u početku smatralo, već je tokom širenja postalo jasno da se radi o globalnoj krizi širokih razmera i nesagledivih posledica, tj. nesvakidašnjem i vanstandardnom fenomenu i izazovu koji prevazilazi mogućnosti i kapacitete bilo koje nacionalne države pojedinačno. Imajući u vidu evolucijski kontekst, termin pandemija kao zdravstvena kriza, uporedo sa širenjem virusa, postepeno se, više spontano, nego intencionalno, impostira kao nova diskurzivna formacija zbog svoje visoke frekventnosti i procesa sekuritizacije koji je ubrzo zahvaljujući tome dobio svoje političke i bezbednosne fundamente[2].

Kako na globalnom, tako i na nacionalnom nivou, tekuća pandemija je različitom snagom preoblikovala, ne samo ekonomski, socijalni, geopolitički, već i

[2] Mark Lacy, Daniel Prince, Securitization and the global politics of cybersecurity, Global Discourse: An interdisciplinary journal of current affairs, Volume 8, Number 1, January, Bristol, Engleska, 2020, 2018, pp. 100-115

bezbednosni pejzaž. U atmosferi rastućeg osećaja straha, neizvesnosti i nemogućnosti uticaja na dalji tok i razvoj pandemije, države i njihovi nadležni sektori su na različite načine reagovali u cilju zaustavljanja širenja epidemije, primenjujući širok spektar, često i zaboravljenih mera, poput policijskog časa, vanrednog stanja i situacije, ograničavanja kretanja i rada građana i poslovnih subjekata, uvođenje karantina i samoizolacija, zatvaranja granica i sl. Pod dejstvom navedenih mera, prestaju sa radom brojna preduzeća, kompanije i državni organi i zbog potrebe nastavka proizvodnje i rada uvodi se sistem rada od kuće i redukovana proizvodnja. Rezultanta takve iznuđene situacije jeste smanjivanje rada u fizičkoj i povećanje učešća rada u digitalnoj sferi, što je u praksi izazvalo i ubrzan rast sajber kriminalnih aktivnosti, najčešće sa transnacionalnim obeležjima.

Osim toga, pandemija kovid 19 je za sve države, gotovo bez izuzetka, predstavljala svojevrsni test za ocenu pripremljenosti i funkcionisanja zdravstvenih i socijalnih sistema, posebno sa aspekta ranjivosti i otpornosti i proveru institucionalnih kapaciteta države na planu pružanja adekvatnog sveopšteg odgovora. Defakto, pandemija razotkriva globalnu ranjivost u javnom zdravlju ističući slabosti nacionalne i globalne spremnosti u domenu zdravstvene zaštite, raspoloživih kapaciteta, logistike i operativnih efektiva, koordinacije odgovora, te ukupne spremnosti za pružanje preventivnih i terapijskih mera uključujući i razvoj vakcine i njene distribucije. U akademskoj zajednici preovladava mišljenje da pandemija nije samo aktuelni rizik, već ona, za razliku od drugih elementarnih nepogoda i sama produkuje čitav spektar novih rizika u nastajanju. Među tim rizicima, u prvi plan tokom pandemije izbijaju pretnje i rizici iz sajber prostora. Povećana anksioznost i unutrašnji i kolektivni strahovi stanovništva doveli su do rasta verovatnoće rizika od sajber kriminala, što odgovara porastu broja i opsega sajber napada u celini.



Izvor: AXA Future Risks Reports 2020, Pariz, Francuska

Grafik 2: *Rizici u nastajanju u uslovima pandemije*

3. Pandemija kao pozadina i strateška prilika za razvoj sajber kriminala

U etabliranim naučnim krugovima, naučnoj produkciji, međunarodnim naučnim skupovima, konferencijama, kongresima i sl., sve više dominira stav da je recentno promenljivo i turbulentno strateško okruženje omogućilo stvaranje povoljnih uslova za ubrzanje procesa digitalizacije, a time posredno dovelo i do rasta, bolje reći eksplozije sajber kriminala. U prilog tome, idu i najnovija empirijska istraživanja koja ukazuju na enorman rast sajber kriminala u odnosu na prethodne godine. Detaljnije analize i istraživački nalazi potvrđuju da to nije slučajnost, već postoje dublji razlozi, uzroci i vektori koji u uslovima pandemije pojačavaju sajber napade, kriminal i uopšte sajber kampanje.[3]

Prilikom razmatranja ovih korelacija, mora se imati u vidu da je porast sajber napada na internet sadržaje i putem interneta kao vektora i ranije postojala, ali razlika je u tome što je pandemija bila katalizator i akcelerator da se kriminalni akteri prilagode novonastalim okolnostima i u velikoj meri promene: kriminalni narativ, sredstva i metode napada, modus operandi, izbor potencijalnih meta, ciljeve svog delovanja, kao i načine prikrivanja, uključujući tu i različite atribucije. Istovremeno, situacija u vezi korona virusa, za brojne kriminalne aktere i njihovu kriminalnu infrastrukturu, predstavlja stratešku priliku, odnosno povoljno okruženje za kriminalno delovanje. U osnovi, kriminalni akteri adaptiraju svoj pristup i nastup aktuelnom društvenom kontekstu, kao izrazito pogodnom tlu za poboljšanje svojih operativnih kapaciteta, nezavisno od toga da li se radi o pojedincima, organizovanim kriminalnim grupama ili vladama pojedinih država i drugih nedržavnih aktera. Samim tim, proširuje se i dispozicija ciljeva koje kriminalni akteri nastoje preko svojih napada da ostvare.

Pored tradicionalnih ciljeva, koji uključuju protivpravnu imovinsku korist i političke ciljeve, uključujući tu i terorizam, novonastala pandemijska kriza pruža dodatne mogućnosti za ostvarenje i novih ciljeva kao što su: osveta, špijunaža i ometanje koji vrlo često imaju hibridni karakter[4]. U složenoj konfiguraciji prilagođavanja novim uslovima, kriminalni akteri su u svom nastupu pokazali visok nivo sofisticiranosti, maštovitosti, kreativnosti, inventivnosti, ali i upornosti, drskost i bezobzirnost kada su u pitanju ciljevi i mete napada.

Da i najmoćnije zemlje u vojnom i tehnološkom smislu i njihova kritična infrastruktura mogu biti meta sajber napada od strane hakera podržanih od stranih vlada, najbolje ilustruje nedavni događaj u vezi napada na Ministarstvo finansija SAD koje važi za jednu od najzaštićenijih institucija SAD. Prema najnovijem saopštenju Agencije za sajber bezbednost i bezbednost infrastrukture

[3] Harjinder Singh Lallie et all, Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic, str. 1-2

[4] The European Union External Action Service (EEAS), "A Europe that Protects: Countering Hybrid Threats", https://eeas.europa.eu/topics/eco-nomic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en accessed 27 July 2020

(CISA) koja deluje u sastavu Agencije za nacionalnu bezbednost, potvrđen je sajber napad na internet mreže vlade SAD. Naime, hiljade organizacija širom SAD koje koriste platformu Orion Solar Winds izložene su hakerskom napadu i tom prilikom je otet softver koji inače koriste i mnoge druge vladine službe i tehnološke kompanije u severnoj Evropi, Aziji i Bliskom istoku.

Istovremeno je Fire Eye kao vodeća kompanija u domenu sajber bezbednosti objavila da je i ona bila žrtva sajber napada od iste hakerske grupe. Neposredno nakon otkrivanja ovog napada, za sada sa nepoznate adrese, Ministarstvo finansija je zatražilo od CISA i Agencije koja je zadužena za izradu internet i telekomunikacione politike i Federalnog istražnog biroa da se angažuju na identifikovanju počinilaca i ublažavanju posledica izazvanih kompromitovanjem njihovih baza podataka. Američka agencija za sajber bezbednost pri Nacionalnoj bezbednosnoj agenciji (NSA) naložila je svim nacionalnim službama i agencijama da se automatski isključe sa platforme koju koriste za nadzor i upravljanje svojim sistemima i mrežama. Mejnstrim mediji su ne čekajući zvanične izveštaje objavili da je za napad odgovorna hakerska grupa pod nazivom „APT 29", koja je i ranije izvršavala slične napade pokušavajući da ukrade laboratorijske podatke i istraživače nalaze o vakcini protiv korona virusa.[5]

Novija istraživanja ukazuju da kriminal koji je povezan sa pandemijom uključuje online i offline distribuciju zaštitne opreme, farmaceutskih i sanitarnih proizvoda; lažne testove za koronu, navodne vakcine protiv kovida 19, različite forme seksualnog iskorišćavanja dece na internetu, brojne šeme prevara koje se tiču nepokretnosti i sl., različite kampanje sa temom pandemije, iza kojih stoje skriveni ciljevi, kao i brojne kampanje dezinformisanja i kompromitovanja poslovnih e-mail adresa, kao i mejl adresa državnih institucija, kompanija i pojedinaca, socijalni inženjering, itd.

Prema izveštaju Interpol-a za tekuću godinu, navodi se da „različiti kriminalni akteri nastoje iskoristiti krizu javnog zdravlja kako bi unapredili ili usavršili nove tehnike napada, a istovremeno redukovali mogućnost njihovog otkrivanja."[6] Usled nepostojanja sređenih statističkih baza i opšteusvojene metodologije evidentiranja sajber krivičnih dela, veoma je teško doći do preciznijih parametara o razmerama, veličini i opsegu globalnog sajber kriminala. Nasuprot tome, situacija na nacionalnom i regionalnom nivou je daleko povoljnija, posebno kada je reč o EU. Prema sadašnjima EU rešenjima, sajber bezbednost je zajednička odgovornost institucija EU i nacionalnih država, što implicira potrebu međusektorskog i sveobuhvatnog okvira saradnje i razmene podataka. Upravo iz tih razloga, evropske institucije koje se bave zaštitom od sajber kriminala, poput EUROPOL-a, ENISA-a, EC3, sistematski prate, registruju, obrađuju i analitički i grafički prikazuju statističke nalaze o kretanju sajber kriminala, njegovim razmerama po kategorijama, kao i potencijalnim žrtvama

[5] Fox Business, White House confirms cyberattack report on U.S. Treasury by foreign goverment, www.foxbusiness.com

[6] Izveštaj Europola o sajber kriminalu za 2020. godinu

kao metama, visini materijalne i nematerijalne štete, što predstavlja dovoljno široku osnovu za utvrđivanje trendova i planiranje i upravljanje daljim aktivnostima na planu njihovog suzbijanja, ali i platformu za dalja istraživanja. Među brojnim korisnicima tih baza, posebno se izdvaja zajednički naučno-istraživački centar EU (JRC), čije nalaze i stručna mišljenja koriste gotovo svi segmenti briselske administracije.

4. Krajolik sajber pretnji za vreme kovid 19

Evropska Unija je među prvim globalnim akterima, veoma rano prepoznala potrebu razvijanja i institucionalnog uokvirivanja politike, mehanizama i sredstava za zaštitu od sajber pretnji i rizika. U okviru toga, poslednjih godina je zaokružen proces formiranja relevantnih institucija sa odgovarajućim delokrugom i nadležnostima koji praktično pokrivaju sve aspekte sajber bezbednosti.

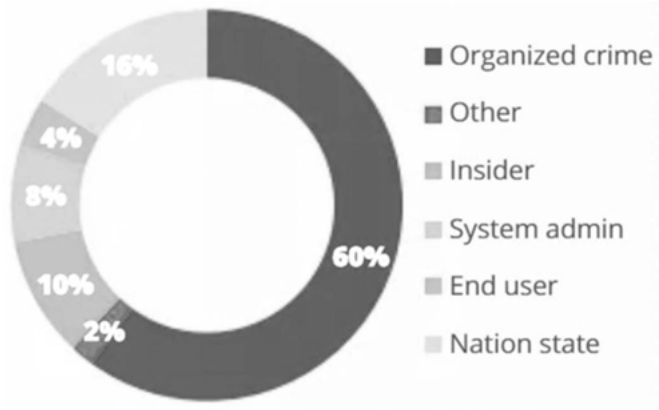
U suočavanju sa novim izazovima i pretnjama, EU je preko svojih institucija i agencija postavila borbu protiv sajber kriminala u sam vrh prioriteta, pored borbe protiv terorizma, zaštite javnih prostora, zaštite kritične infrastrukture i bezbednosti granica. U institucionalnom i operativnom smislu, pored Agencije EU za sajber bezbednost – ENISA, formirane su nove ili dograđene postojeće službe kao što su: Evropska agencija za operativno upravljanje velikim informacionim sistemima u području slobode, bezbednosti i pravde (eu-LISA), Evropske agencije za bezbednost vazdušnog saobraćaja (EASA), Agencije EU za osposobljavanje u području izvršavanja zakonodavstva – (CEPOL) i Regulatorno telo za elektronske komunikacije (BEREC).

Na planu borbe protiv sajber kriminala, EU se oslanja i na brojne politike, a pre svega EMPACT kao ciklus politika usmerenih na suzbijanje krivičnih dela sa kojima se suočava EU iz domena organizovanog kriminala. Tokom 2017. godine, Savet Evrope je ponovo pokrenuo ciklus politika EU-EMPACT, stavljajući u njegovu nadležnost 7 prioriteta i to: sajber kriminal, krijumčarenje narkotika, trgovina ljudima, organizovani imovinski kriminal, proliferacija oružja, ekonomski kriminal, finansijski kriminal, pranje novca i prevare sa dokumentima.

U nedavno objavljenoj Strategiji EU za bezbednosnu uniju, decidno se ističe „da broj sajber napada i dalje raste. Ti su napadi sofisticiraniji nego ikada pre, dolaze iz niza izvora unutar i izvan EU, te su usmereni na područja najveće ranjivosti. U njima često učestvuju državni akteri ili akteri sa podrškom države i usmereni su na kritičnu digitalnu infrastrukturu, kao što su veliki pružaoci klaud usluga.[7]

U nizu dokumenata objavljenih tokom 2020. godine, za vreme trajanja pandemije kovid 19, ENISA je kroz brojne izveštaje i analize, svoje težište rada usmerila na mapiranje i vizuelizaciju pejzaža sajber pretnji, pružajući na taj način uslugu svim donosiocima odluka i politika vezanih za područje sajber bezbednosti, upotrebu sajber prostora, uključujući tu i pretnje koje dolaze iz njega.

[7] Evropska komisija, COM (2020) 605 final, Brisel, str. 8



Izvor: ENISA – Cybersecurity Threat Landscape, 2020[8]

Grafik br. 3: *Procentualna zastupljenost vrsta kriminala*

Analizirajući poslednje događaje vezane za sajber bezbednost u uslovima pandemije, u godišnjem izveštaju ENISA notira 15 eskalirajućih pretnji tokom 2020. godine, uz istovremeno obrazloženje njihove učestalosti, razmera, karakteristika, ciljeva i meta napada, žrtava i štetnih posledica uz navođenje mera za ublažavanje i smanjenje izloženosti tim pretnjama za sve relevantne aktere.

Statistički gledano, broj pretnji svakodnevno raste, dok se obim napada povećava i po broju i po složenosti. U takvom redu veličina, ne samo da raste broj potencijalnih napadača zajedno sa veličinom mreža, nego su i novi alati dostupni potencijalnim napadačima koji su znatno sofisticiraniji u pogledu performansi, efikasniji i delotvorniji. Iz širokog dijapazona evoluirajućih pretnji, težište je usmereno na sledeće:

1. **Malver (Zlonamerni softver) –** je česta vrsta sajber napada čiji je osnovni cilj krađa podataka ili identiteta, špijunaža ili ometanje usluga. U arsenal zlonamernog softvera uključujemo kriptominere, viruse, ransomware, crve i špijunski softver. Tokom 2019. godine, kriptomineri su bili dominantna malwer familija u području pretnji i izazvali su povećane IT troškove, uvećali potrošnju električne energije i istovremeno umanjili produktivnost rada među zaposlenima. Kada su u pitanju empirijski pokazatelji, zvaničnim analizama utvrđeno je preko 400.000 detekcija[9] preinstaliranog spajver i adver softvera na mobilnim uređajima. U periodu od 2019.-2020. godine došlo je do povećanja od 13% malver detekcija vezanih za Windows operativni sistem u poslovnim krugovima na globalnom nivou. U isto vreme 71% organizacija je doživelo malver aktivnost koja se širila od zaposlenog do zaposlenog, tj. putem bočnog širenja unutar korporativne mreže, a ne putem interneta, što je tehnika koja se primenjuje u

[8] https://securityboulevard.com/2020/11/the-enisa-cybersecurity-threat-landscape/

[9] "2020 State of Malware Report". February, 2020. Malware Bytes. https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

napadima na javni sektor kako bi povećala sposobnost naplate većih otkupnina nakon zaključavanja podataka. Preko 46% celokupnog malvera širio se putem e-mail poruka a bio je vezan za .docx tip fajla. Novija istraživanja, takođe, pokazuju povećanje od 50% u domenu malvera projektovanog za krađu ličnih podataka, odnosno malvera projektovanog za proganjanje žrtava, dok je istovremeno 67% malvera[10] isporučeno putem kriptovanih HTTPS konekcija. U svetu sajber kriminala povezanog sa malverom, posebno su zanimljive forme tipa malver kao servis čija prodaja i distribucija potiče iz foruma povezanih sa podzemljem, gde se sajber kriminalcima nude alati i infrastruktura neophodna za izvođenje ciljanih napada. Pružalac i vlasnik malvera kao servisa, sajber kriminalcu pruža usluge koje prate celokupan postupak napada u formi kompleta koji sadrži inicijalni loader, komandni i kontrolni server i tzv. backdoor sistem za preuzimanje kompletne kontrole nad inficiranim računarom. Takođe, povećana je i pojava malvera u oblasti mobilnog bankarstva gde su mobilne aplikacije specifično dizajnirane za krađu podataka, a posebno ličnih podataka, podataka o plaćanjima i iznosu sredstava žrtava koji se nalaze na njihovim bankovnim računima, pa je porast sajber kriminala u ovoj oblasti za period 2019.-2020. godine, uvećan za 50%. Uobičajene forme sajber kriminala u ovoj oblasti bile su bazirane na phishing tehnikama radi pribavljanja poverljivih bankarskih podataka, što se najčešće odigravalo, bilo putem lažnih stranica banke, tzv. klonova, sa log in opcijom, a onda i lažnih mobilnih aplikacija koja izgledaju kao originalne bankarske aplikacije. Međutim, od 2019. godine, sajber kriminalci su postali još kreativniji, pa su kreirali trojanski softver za android operativni sistem koji je u stanju da preuzme kontrolu nad legitimnom bankarskom aplikacijom, zloupotrebivši pristupne funkcije operativnog sistema, kako bi automatizovao maliciozne transakcije. I ova vrsta malicioznog softvera (malvera) kao finansijskog malvera, prodaje se na forumima crnog tržišta, gde se i usavršavaju tehnike izbegavanja bezbednosnih mehanizama. Izuzetna malver inovacija otkrivena je 2019. godine, kroz mogućnost da malver upotrebi senzore pokreta, koji se aktivira samo kada se pametni mobilni telefon kreće, za šta je napravljen trojanac za mobilno bankrstvo koji je sposoban da otkrije „sandboxed environment". Velika inovacija na polju malvera nastala je i kroz zlonamerni softver bez datoteka, tzv. file-less malver, koji iz razloga što ne sadrži izvršni fajl može da izbegne najveći broj uobičajenih sigurnosnih filtera, kao i da zaobiđe tehnike odobravanja po modelu „bele liste". Iz ovog razloga ova malver tehnika je efikasnija i do 10 puta od ostalih tehnika, obzirom da koristi sistem injektiranja malicioznog koda u već instalirani pouzdani softver, bilo da napadač to radi na daljinu, ili putem aktivnog preuzimanja dokumenata koji sadrže maliciozne makroe, odnosno makro naredbe nakon čega se zlonamerni softver integriše u registar Windowsa. Ova vrsta napada je samo u prvoj polovini 2019. godine imala rast od 265%. Prema

[10] "Malware statistics and facts for 2020" July 29, 2020. Comparitech. https://www.comparitech.com/antivirus/malware-statistics-facts/

najnovijim Botnet Threat izveštaju za 2019. godinu, čak 94% od svih vrsta malvera isporučeno je putem e-maila, koji se koristi kao ulazna tačka/vektor kako bi nakon uspešnog napada maliciozni softver bio u mogućnosti da preuzme i dodatni maliciozni softverski kod, koji se onda izvršava u sistemu po principu crva, što mu omogućava bočno i neometano širenje po mreži među svim njenim korisnicima. Među najpoznatijim incidentima u ovoj oblasti, izdvojeni su incident u kompaniji Airbus, gde je došlo do curenja podataka zaposlenih u ovoj kompaniji u Evropi, onda instaliranje malicioznog softvera za obradu kreditnih kartica na sajtu American Medical Collection Agency, što je rezultiralo krađom 12 miliona dosijea sa ličnim podacima pacijenata. Jedan od najvećih pružalaca usluga laboratorijske dijagnostike LifeLabs takođe je postao žrtva ransomware napada koji je rezultirao krađom 15 miliona naloga koji su sadržali rezultate medicinskih testova i brojeve zdravstvenih kartica. Ransomware napad grada Pensacola na Floridi rezultirao je time što je 2GB podataka postalo dostupno online za koje se veruje da su sadržali lične identifikacione podatke građana.

2. **WEB bazirani napadi**[11] **–** predstavljaju atraktivnu metodu kojom generatori pretnje mogu obmanjivati žrtve korišćenjem web sistema i servisa kao vektora pretnje. Najčešći mehanizam je upotreba zlonamernih URL-ova ili zlonamernih skripti sa ciljem preusmeravanja korisnika (žrtve) na željenu web stranicu radi preuzimanja zlonamernog sadržaja ili injektiranja malicioznog koda u pravi ali kompromitovani web sajt radi krađe informacija, protivpravne imovinske koristi, ali i iznuda putem ransomvera.
3. **Fišing** – predstavlja pokušaj prevare radi krađe korisničkih podataka, kao što su log-in podaci, podaci o kreditnim karticama, čak i krađa novca putem korišćenja tehnika socijalnog inženjeringa. I ova vrsta napada se uobičajeno pokreće putem e-mail poruka koje su koncipirane tako da izgledaju kao da su poslate iz kredibilnih izvora, a iza kojih stoji namera da se primalac takve poruke navede da otvori maliciozni prilog ili pokrene maliciozni URL[12]. Ciljani sistem krađa identiteta nazvan „spear phishing" oslanja se na tehniku istraživanja ličnosti i navika žrtve, kako bi prevara izgledala što više prilagođena afinitetima žrtve, što ovu prevaru čini jednom od najuspešnijih kada su u pitanju kompanijske mreže. Ovaj sistem prevare skrojen je na način da izazove emotivnu reakciju žrtve, što je upravo ono što hakeri traže. Iako je ova tehnika od ranije poznata, inventivni hakeri konstantno menjaju modus operandi ove tehnike i na taj način umanjuju stepen uspeha različitih uobičajenih zaštitnih sistema od spam napada. Iako su e-mailovi glavni nosilac ove vrste sajber kriminalne aktivnosti, novija istraživanja ukazuju da se određeni broj ovih aktivnosti polako premešta na polje poruka koje se razmenjuju na društvenim mrežama gde se istovremeno povećava broj

[11] "What is Formjacking and How Does it Work?", Norton. https://us.norton.com/internetsecurity-emerging-threats-what-is-formjacking.html

[12] "What Is Phishing?", Cisco. https://www.cisco.com/c/en/us/products/security/emailsecurity/what-is-phishing.html

ovih i ovakvih napada. Stručnjaci pretpostavljaju da će i metodologija sajber kriminala u ovoj oblasti u skorije vreme biti modifikovana ka novim sofisticiranijim metodama slanja poruka pri čemu će one postati znatno rizičnije zbog upotrebe veštačke inteligencije koja će obavljati pripremu i slanje specijalizovanih i objektno skrojenih poruka da bi iste bile upotrebljene kao vektori za druge pretnje poput nenamernih unutrašnjih pretnji. Ono što je karakteristično za ovu vrstu sajber kriminala, jeste da je istraživanjima utvrđeno da se kovid 19 veoma često koristi kao fišing mamac, putem koga sajber kriminalci iskorišćavaju strah javnosti od kovida 19, sve radi ostvarivanja prethodno pobrojanih kriminalnih ciljeva. Brojni empirijski nalazi pokazuju da su se fišing napadi koji uključuju pominjanje ovog virusa za samo 1 mesec u 2020. godini (februar, mart), uvećali za 667%[13], čime je ova vrsta prevare u ukupnom broju svih prevara dostigla zapaženih 2%, samim tim što su ove tehnike pokazale izuzetne rezultate u korist kriminalaca. Nove verzije prevara sada uključuju specijalno dizajnirane e-mailove koji izgledaju kao da su poslati od strane Američkog Centra za kontrolu bolesti (US-CDC), Svetske zdravstvene organizacije (WHO) ili čak poznatih univerzitetskih medicinskih timova. Komunikacija ovog tipa se vrši sa zlonamernim ciljem da se žrtva navede da prati maliciozni link, pa su iz tog razloga i FBI i WHO nedavno dali upozorenja građanima i zaposlenima, jer veliki broj njih radi na zastarelim bezbednosnim i operativnim sistemima u čemu su sajber kriminalci videli šansu i pokušavaju da iskoriste njihovu ranjivost i izloženost.

4. **Napadi putem web aplikacija –** Web aplikacije i tehnologije postale su centralni deo interneta time što su uslužno usvojile različite namene i funkcionalnosti. Povećanje broja i kompleksnosti web aplikacija i njihovih široko rasprostranjenih usluga, veliki je izvor bezbednosnih izazova i pretnji koje su različito motivisane počev od narušavanja ugleda pa preko finansijske štete, do krađe važnih ličnih podataka. Kako web usluge i aplikacije uglavnom zavise od baza podataka, bilo da su one namenjene za pohranjivanje ili njihovo isporučivanje, napadi tipa SQL Injection dobro su poznati primer i najčešća pretnja ovim servisima. Napadi na više lokacija tzv. Cross-site Scripting napadi funkcionišu tako što maliciozni akter pronalazi i zloupotrebljava slabosti, kako u formularima, tako i u drugim ulaznim oblicima na web aplikacijama, jer one vode do drugih malicioznih osobina, poput onih za preusmeravanje na zlonamernu web lokaciju. Kako organizacije postaju sve više stručne u poslovima kojima se bave i u tom pravcu razvijaju neophodnu automatizaciju, tokom životnog ciklusa web aplikacije koju koriste, dosledna automatizacija zahteva najviši stepen bezbednosti i predstavlja najvažniji deo njihove ponude i najvažniji parametar pri određivanju poslovnih prioriteta. Na ovaj način su stvorena složena okruženja koja vode do usvajanja novih usluga kao što su programske interfejs aplikacije (APIs) čija je osnovna uloga podizanje nivoa bezbednosti web aplikacije kroz više preventivnih i detek-

[13] "Coronavirus phishing emails: How to protect against COVID-19 scams" 2020. https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

tivnih mera. Približno 80% organizacija[14] je usvojilo ove kontrolne protokole za njihov ulazni saobraćaj.

5. **Spam ili neželjena pošta –** datira od 1978. godine[15] i ima, kako široku rasprostranjenost, tako i veliki uticaj na razvoj i obim sajber kriminala, kao i razne vektorske tehnike njegovog izvođenja. Iako prijem neželjene pošte uglavnom izaziva nelagodnost, istovremeno to predstavlja i priliku da se putem malicioznog softvera nekome ukradu lični podaci ili instalira malver. Neželjena pošta se u principu sastoji od grupnog slanja poruka i smatra se ozbiljnom sajber pretnjom, posebno u slučaju kada predstavlja vektor za distribuciju ili omogućavanje drugih pretnji. Samim tim spam često biva pogrešno percipiran kao fišing kampanja, međutim, glavnu razliku između ove dve maliciozne radnje, predstavlja činjenica da je fišing strogo targetirana akcija koja koristi metode i taktike socijalnog inženjeringa, aktivno ciljajući na krađu korisničkih podataka. Sa druge strane, spam je taktika za slanje velike količine poruka korisnicima koji se nisu prijavili za njihovo primanje. Samim tim, fišing kampanja može koristiti spam taktiku za distribuiranje poruka, dok spam može povezati korisnika sa kompromitovanim web sajtom, kako bi na njegovom računaru mogao biti instaliran malwer radi krađe njegovih ličnih podataka. Tokom 41 godine postojanja spama[16], tokom kojih je došlo do zloupotrebljavanja mnogih popularnih sportskih i društvenih događaja, nikada u istoriji ništa nije omogućila toliko zlonamerne spam aktivnosti kao ona koja je viđena u vreme ovogodišnje kovid 19 pandemije.
6. **DDoS sajber napadi** – su distribuirano uskraćivanje usluge i predstavljaju slučaj kada korisnici sistema ili usluge nisu u mogućnosti da pristupe relevantnim informacijama, servisima ili drugim resursima. Ovaj efekat može biti postignut iscrpljivanjem sistema pružanja usluga ili preopterećenjem mrežnih komponenti ili infrastrukture. Izvođači ovih malicioznih aktivnosti konstantno povećavaju broj napada time što targetiraju nove sektore kroz korišćenje različitih motiva, iako su odbrambeni mehanizmi i strategije vremenom postale znatno robusnije. I maliciozni akteri takođe unapređuju njihove tehničke sposobnosti i dostignuća. To je otišlo dotle da maliciozni akteri unapređuju svoje komercijalne taktike time što u poslednje vreme čak i javno reklamiraju svoje usluge na internetu, iako je ranije ova vrsta usluga bila reklamirana samo na darkweb forumima, sada se taj reklamni mehanizam preselio na društvene medije i kanale, kao što su Youtube

[14] "2020 State of Application Services Report" F5 Networks, 2020. https://www.f5.com/state-of application-services-report

[15] "Email: Click with Caution – How to protect against phishing, fraud, and other scams" June, 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/emailsecurity/email-threat-report.pdf

[16] "Naming the coronavirus disease (COVID-19) and the virus that causes it". 2020. WHO. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it

i Redit.[17] Tokom 2019. godine, primećena je značajna promena na listi zemalja koje generišu DDoS saobraćaj, gde se među najviše plasiranima pojavljuju Hong Kong, Južna Afrika itd. Prošla 2019. godina je donela uvećanu DDoS aktivnost[18] izvedenu preko Botnet mreža i IoT uređaja koji predstavljaju središte Bot mreža. Kada su u pitanju zemlje koje su najviše zaražene Botnet agentima, tu su najzastupljenije Kina, Brazil i Iran, pa se obzirom na razvoj implementaciju i distribuciju 5G mreža, s pravom očekuje eksponencijalni rast u ovoj oblasti, ne samo broja povezanih uređaja, već i širenja Botnet mreža.

7. **Krađa identiteta** – predstavlja nedozvoljenu upotrebu ličnih podataka žrtve putem kojih se sajber kriminalac može predstavljati kao osoba čiji su lični podaci ukradeni, kako bi na taj način stekao protivpravnu finansijsku korist, ili druge beneficije. Trend krađe identiteta u uobičajenoj formi najčešće čini povreda privatnosti, koja u periodu od 2018.-2020. godine beleži porast od 54% i to usled 4,1 milijarde evidentiranih slučajeva u ovom periodu[19].
8. **Povreda tajnosti podataka** – Povreda tajnosti podataka predstavlja sajber bezbednosni incident u kome se informacijama jednog dela ili celog informacionog sistema neovlašćeno pristupa, najčešće sa zlonamernim ciljevima ili namerama, što dovodi do potencijalnog gubitka ili zloupotreba takvih informacija. Ovakvi incidenti veoma često podrazumevaju posledicu ljudske greške, bilo da se ona dešava prilikom konfiguracije sistema ili uspostavljanja određenih usluga baziranih na sistemu, u kom slučaju može doći do nenamernog izlaganja podataka. Praksa je pokazala da je najčešće potrebno oko 206 dana[20] da bi bilo utvrđeno kršenje tajnosti podataka u organizaciji, što jasno pokazuje odsustvo ili kašnjenje kod preventivnih i detektivnih mera vezanih za informacioni sistem, a time nastaje i značajno kašnjenje i u primeni korektivnih mehanizama. Nova saznanja sugerišu da nakon kršenja tajnosti podataka, odnosno nakon njenog otkrivanja, finansijske posledice po organizaciju mogu trajati i dve godine nakon inicijalnog incidenta. Prema dostupnoj statistici, 71% kršenja tajnosti podataka finansijski je motivisano, dok 32% uključuje fišing aktivnosti. Takođe, 52% slučajeva u ovoj oblasti uključuje hakovanje kao bezbednosni problem, dok u 70% slučajeva dolazi do od incidenata vezanih za kompromitovanje podataka putem e-mail servisa.
9. **Insajderska pretnja** – predstavlja radnju koja može rezultirati incidentom, a koju vrši pojedinac ili grupa ljudi povezanih sa žrtvom. Najčešće takve radnje

[17] Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS attacks in Q1 2019" May 21, 2019. Kaspersky. https://securelist.com/ddos-report-q1-2019/90792/

[18] Tomer Shani. "Updated: This DDoS Attack Unleashed the Most Packets Per Second Ever. Here's Why That's Important." April 30, 2019. Imperva. https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/

[19] "$19 million worth of iPhones stolen in massive identity theft scam" June 15, 2019. 9To5Mac. https://9to5mac.com/2019/06/05/19-million-worth-of-iphones/

[20] "Cost of Data Breach Report." 2019. IBM Security, Ponemon Institute. https://www.ibm.com/security/data-breach

potiču od zloupotreba privilegija kada insajderski element nedozvoljeno sarađuje sa eksternim faktorima koji putem takve aktivnosti ostvaruju neovlašćeni pristup određenom informatičkom dobru ili imovini. Takođe, do istog ili sličnog štetnog efekta može doći i posredstvom nenamernih insajderskih grešaka do kojih dolazi usled neodgovornosti ili nebrige, ali i neznanja. Samim tim, postoji 5 insajderskih pretnji[21] koje mogu biti definisane prema njihovim karakteristikama i ciljevima i to: neoprezni insajderi koji nepravilno rukuju podacima, krše bezbednosne politike i neovlašćeno instaliraju aplikacije; insajderski agenti koji kradu informacije u korist trećih lica; nezadovoljni zaposleni koji žele naneti štetu organizaciji u kojoj rade; zlonamerni insajderi koji zloupotrebljavaju važeće privilegije za krađu informacija zarad lične koristi; i neodgovorna treća lica koja ugrožavaju bezbednost putem obaveštajnog rada, zloupotrebe i zlonamernog pristupa ili korišćenja sredstava organizacije.

10. **Botnet mreže** – su mreže povezanih uređaja zaraženih bot malverom. Ovako inficirane uređaje, maliciozni akteri najčešće koriste za sprovođenje distribuiranih napada za uskraćivanje usluge (DDoS). Najčešće funkcionišu po sistemu P2P (peer to peer)[22] pod kontrolom određenog komandnog ili kontrolnog centra sa udaljene lokacije, kako bi zlonamerni akter njima sinhronizovano upravljao radi ostvarivanja unapred ciljanog malicioznog rezultata. Najveća opasnost u ovoj oblasti preti iz domena interneta stvari podržanog 5G tehnologijom, koja je drastično povećala mogućnosti i kapacitete komunikacije mašina sa mašinama (M2M). Botnet mreže često predstavljaju vektor za sajber kriminalce kako bi oni, pored ostalog, pokretali različite operacije koje se kreću od elektronskog bankarstva, prevara sa ransomverom, rudarenjem kriptovaluta i DdoS napadima. Jedan od najpoznatijih i najrazornijih botnet incidenata povezuje se sa Mirai botnet virusom koji je od svog puštanja u opticaj nastavio da „živi" u raznim inoviranim varijantama, obzirom da je njegov izvorni kod bio dostupan na internetu.
11. **Fizičke manipulacije, oštećenja, krađe i gubici –** Fizička ometanja, oštećenja, krađe i gubici doživeli su značajne promene poslednjih godina. Integritet uređaja postao je ključni faktor da bi jedna tehnologija postala mobilna, a uz to i primenjiva u oblasti interneta stvari (IoT).[23] IoT je pružio mogućnost poboljšanju fizičke bezbednosti posredstvom primene veoma složenih i naprednih rešenja. Na ovim osnovama kreirani su IP sistemi koji poseduju pametne senzore, wi-fi kamere, pametno sigurnosno osvetljenje, dronove i elektronske brave, koje su u stanju pružiti sistem nadzora koji prikuplja podatke sa senzora i iste isporučuje

[21] "Insider Threat Report", 2019. Verizon. https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf

[22] 2. Monnappa K A. "Learning Malware Analysis." June 2018. O'reilly. https://www.oreilly.com/library/view/learning-malware-analysis/9781788392501/17a1735d9583-4d86-9d1e-8b2735af5168.xhtml

[23] 1. "Physical Security Guide". Kisi. https://pages.getkisi.com/physical-security-guide

sistemu sa veštačkom inteligencijom (AI) i sposobnošću mašinskog učenja (ML), kako bi putem analize ovih podataka analitički sistemi mogli prepoznati postojanje pretnje i kreirati odgovarajući odgovor uz minimalno kašnjenje i maksimalnu preciznost. Uprkos postojanju ovakvog bezbednosnog sistema, činjenica je da objekti kao što su inteligentne zgrade, ali i mobilni uređaji i pametni nosivi uređaji i dalje mogu biti upotrebljeni za zaobilaženje fizičkih bezbednosnih mera, što potvrđuju napadi povezani sa ATM mašinama[24] i POS terminalima koji su se događali širom Evrope i sveta tokom 2019. godine.

12. **Curenje informacija** – Povreda podataka predstavlja bezbednosni incident, do koga dolazi kada podaci za koje je organizacija odgovorna, usled bezbednosnog incidenta bivaju kompromitovani i time dođe do kršenja njihove poverljivosti, dostupnosti ili integriteta[25]. Ova povreda najčešće uzrokuje curenje informacija i obično obuhvata spektar, od ugrožavanja ličnih podataka i informacija, preko finansijskih podataka pohranjenih u IT infrastrukturi, pa sve do ličnih podataka iz domena zdravstva koji se čuvaju u repozitorijumu pružalaca zdravstvenih usluga. Do ovakvih incidenata najčešće dolazi usled neodgovorne ili zlonamerne radnje pojedinca ili neuspeha primenjenog organizacionog procesa u organizaciji.
13. **Ransomver** – predstavlja vrstu malvera čiji je zadatak da se na prevarni način infiltrira u sistem, nakon čega kriptuje, odnosno zaključava fajlove računara žrtve i pokreće proces iznude kako bi žrtva platila traženu otkupninu napadaču, ali bez garancije da će zaključani materijali biti vraćeni u prvobitno stanje. Samim tim, ovaj oblik sajber kriminala postao je veoma popularno oružje za nanošenje štete vladama, kompanijama i pojedincima. Iako bezbednosne politike u ovoj oblasti suštinski datiraju još od početka 2000. godine,[26] one ni nakon 20 godina nisu dale jasan odgovor na ovu vrstu sajber pretnje, osim što je u poslednjih nekoliko godina došlo do povećanog interesovanja za osiguranje od ovakvih šteta, pa se troškovi iznude pokrivaju ugovorima sa osiguravajućim društvima. Obzirom da je ovaj trend u oblasti osiguranja poznat u sajberkriminalnim krugovima, samim tim je u istim stvoreno uverenje da će im nakon ransomver napada biti plaćena zahtevana suma od strane osiguravača, pa se u praksi neretko dešava da osiguravači plate zahtevanu sumu kako bi ublažili efekte nastale štete i sačuvali ugled žrtve u javnosti. Iako ovakvi slučajevi mogu predstavljati trenutno i relativno bezbolno rešenje za određene žrtve ransomver napada, jer su sa jedne strane i povratili podatke i sačuvali javni ugled, u

[24] Jovi Umawing. "Everything you need to know about ATM attacks and fraud: Part 1." May 29, 2019. Malwarebytes Labs. https://blog.malwarebytes.com/101/2019/05/everything-you-need-to-know-about-atm-attacks-and-fraud-part-1/

[25] "What is a data breach and what do we have to do in case of a data breach?" European Commission. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

[26] "What you – and your company – should know about cyber insurance", August 20, 2019. Talos. https://blog.talosintelligence.com/2019/08/cyber-insurance-FAQs.html

globalu ovakav trend samo podstiče sajber kriminalnu zajednicu da nastavi sa ovim delovanjem, a to na dugi rok ne doprinosi ni osiguranju žrtve od ponavljanja ovakvih incidenata, niti očuvanju ili održanju njenog ugleda. Tome u prilog govori da su procenjeni troškovi iznuda po ovom osnovu već dostigli 10,1 milijardu evra, odnosno 3,3 milijarde više nego 2018. godine, pa ovaj kriminal time beleži porast od 365%,[27] dok je 45% napadnutih organizacija u 2019. godini platilo ovakav otkup.

14. **Sajber špijunaža** – predstavlja specifičan fenomen, jer se smatra i pretnjom i motivom iz domena sajber kriminala.[28] Uobičajena definicija za ovu vrstu sajber kriminala je da se radi o upotrebi računarskih mreža za ostvarivanje nezakonitog pristupa poverljivim informacijama, koje uobičajeno predstavljaju vlasništvo vlada ili drugih važnih organizacija. Tokom 2019. godine rađene su brojne analize koje su prikazale da globalne organizacije sajber špijunažu ili špijunažu sponzorisanu od strane nacionalnih država tokom vremena vide kao sve veću pretnju, tj. pretnju koja utiče na skoro sve industrijske sektore, kritičku i strateškу infrastrukturu širom sveta, uključujući tu i ministrarstva, železnice, telekomunikacione provajdere, energetske sisteme, bolnice i banke. Sajber špijunaža je, stoga, najčešće fokusirana na geopolitičko polje, obzirom da je ona pretežno usmerena na krađu poslovnih tajni, intelektualne svojine i drugih zaštićenih informacija iz strateških oblasti. Ova vrsta sajber kriminala često mobiliše privredne i industrijske aktere, ali i strane obaveštajne službe, odnosno lica angažovana da rade u njihovo ime. I ova oblast sajber kriminala u 2019. godini beleži rast, posebno u domenu napada sponzorisanih od strane države, ali i napada na industrijske sisteme interneta stvari, najčešće u oblastima nafte i gasa, javnim postrojenjima i proizvodnim sektorima. Sajber napadi izvršeni putem naprednih upornih pretnji (APT) sada već jasno pokazuju da su finansijski napadi veoma često motivisani špijunažom.
15. **Kriptorudarenje** – predstavlja neovlašćeno korišćenje resursa uređaja za rudarenje kriptovaluta.[29] Mete ove vrste sajber kriminala uključuju svaki povezani uređaj, uključujući i kompjutere i mobilne telefone. Trendovi pokazuju, da sajber kriminalci u poslednje vreme sve više targetiraju infrastrukturu oblaka, međutim, iako je to tako, takva dešavanja nisu privukla značajniju pažnju ni zakonodavaca, ni agencija za sprovođenje zakona. Jedan od glavnih razloga za to je što se ovakvi slučajevi retko prijavljuju, pretežno iz razloga manjeg obima negativnih posledica. U svakom slučaju, najčešće posledice za organizacije obuhvataju

[27] 22. "BDO's Fall 2019 Cyber Threat Report: Focus on Healthcare". October 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber-threat-report-focus-on-health

[28] "Cyber Threatscape Report. 2019." IDefense – Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

[29] Sergiu Gatlan. "Cryptominers Still Top Threat In March Despite Coinhive Demise." April 9, 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/cryptominers-still-top threat-in-march-despite-coinhive-demise/

uvećane troškove u IT sektoru, degradiranje računarskih komponenti, uvećanu potrošnju električne energije, ali i umanjenje produktivnosti zaposlenih usled usporenog funkcionisanja radnih stanica.

5. Višedimenzionalne konvergencije i novi trendovi u sajber bezbednosti

Dramatičan razvoj industrije 4.0, u čijem središtu se nalazi razvoj i upotreba nano/bio/informacionih tehnologija u kombinaciji sa AI, robotikom, minijaturizacijom internet stvari i pametnih uređaja, imaju širok uticaj, ne samo na ekonomiju i društvo, već i na područje bezbednosti. Konvergencija, kako se ističe u stručnoj literaturi javlja se, po pravilu, uvek tamo gde se naučne discipline i ključne tehnologije kombinuju, umrežavaju i prepliću sa drugim disciplinama i tehnologijama, koje omogućavaju ili perspektivno nude novu ili dodatnu vrednost izvan sinergije. Dakle, konvergencija je daleko više od kombinacije različitih disciplina i tehnologija, jer pored sinergije generiše i novu i veću dodatnu vrednost.

U postojećem ambijentu, pogođenom virusom sa vektorom širenja, više nego jasno se može uočiti da između pandemije i sajber bezbednosti postoje čvrste konvergentne veze i odnosi. Nesporna je činjenica da pandemija kao kriza, nije za sada došla do svoje silazne putanje, usled čega produkuje celu jednu panoramu uticaja, štetnih posledica i manifestnih efekata. Jednom rečju, ona je sama po sebi izazov i konkretna pretnja širem okruženju, pa i globalnom. Sa druge strane, sajber prostor tokom poslednjih godina, sve više se tretira kao peta dimenzija ratovanja i sve se više koristi kao arena vojnog, bezbednosnog, obaveštajnog, izviđačkog i informacionog ratovanja između globalnih sila.

Brojne države izdvajaju rastuća budžetska sredstva za vođenje sukoba u sajber prostoru, razvijaju organizacione kapacitete za izvođenje operacija i usvajaju savremene doktrine, strategije i vojne recepture.[30] Teroristi su poslednjih godina počeli intenzivnije da koriste prednosti sajber prostora, brzinu komunikacije, lakoću, skrivanja, smanjenu mogućnost presretanja komunikacije i kontrole novčanih tokova u kripto valutama od strane policijskih ili bezbednosnih službi.[31]

Istovremeno, sajber prostor poslednjih godina, usled geostrateškog preslaganja i resetovanja odnosa među globalnim silama, koristi se sve više kao prostor za pripremu i izvođenje ofanzivnih modela hibridnog rata, u koje spada i sajber kriminal, koji je indukovan od državnih, ali često nedržavnih aktera i struktura. Sajber kriminal je, takođe, velika opasnost i izazov za većinu modernih država sveta zbog njihove izražene digitalne i ključne infrastrukture.

[30] Više o tome: Mladenović D., Multidisciplinarni aspekti sajber ratovanja, doktorska disertacija, Fakultet organizacionih nauka, Univerzitet u Beogradu, 2016

[31] Opširnije: Putnik N., Sajber prostor i bezbednosni izazovi, monografija, Fakultet bezbednosti, Univerzitet u Beogradu, 2009

Suština konvergentne veze i odnosa koji se uspostavlja između pandemije i sajber kriminala, nije samo u sinergiji štetnih efekata, povećanja ranjivosti, već u generisanju potpuno novih, pre aktuelne situacije nepoznatih i nedovoljno istraženih sajber izazova, vektora napada, konkretnih pretnji i evoluirajućih rizika koji svojim multipliciranjem i kaskadnim razvojem mogu dovesti pojedince, društvo, državu i druge subnacionalne strukture u neodrživu situaciju sa čitavim spektrom nadolazećih faktora, štetnih efekata, nepodnošljivih gubitaka i nenadoknadive štete.

Drugim rečima, u takvoj kombinatorici faktora, nastupaju, po pravilu, ireverzibilne promene koje jednostavno ne dozvoljavaju uspostavljanje prethodnog stanja. Suština te veze ili odnosa, ogleda se u tome da pandemija svojim uticajem generiše povoljnu klimu za porast međusobnih malicioznih veza i interakcija koje daju dejstvujuće efekte u formi kvantnih skokova, stvarajući tako čitav niz različitih scenarija od kojih nijedan nije potpuno povoljan i poželjan usled njihove stalno cirkularne konvegencije.

Jedna od vodećih globalnih istraživačkih i konsalting kompanija koja se inače bavi tehnološkim pitanjima, uključujući i sajber bezbednost, privatnost i upravljanje rizicima, identifikovala je 9 novih trendova u ovim oblastima za 2020-2021, koji će, kako to ističu stručnjaci, dugoročno uticati na kreatore politike, kompanije, operatere kritičnih usluga, kao i državne institucije[32].

Za razliku od nekih drugih relevantnih sajber aktera, Gartner određuje vrhunske trendove kao tekuće strateške korake u bezbednosnom sajber okruženju, koji još uvek nisu široko prepoznati, ali će zbog svoje učestalosti i zamaha imati sasvim izvesno širok industrijski uticaj i značajan potencijal za disrupciju. Među najvažnije trendove, Gartner ubraja:

- Nastaju nove mogućnosti pokrivanja i reagovanja na sajber pretnje i incidente, kako bi se poboljšala tačnosti produktivnost;
- Postepeno se uvodi automatizacija bezbednosnih procesa i receptura radi uklanjanja ponavljajućih zadataka;
- Veštačka inteligencija (AI) stvara nove bezbednosne odgovornosti za zaštitu digitalnih poslovnih inicijativa;
- Uvode se glavni bezbednosni službenici na nivou kompanija koji okupljaju više silosa usmerenih na bezbednost;
- Privatnost postaje samodisciplina;
- Novi timovi „digitalnog poverenja i bezbednosti“ fokusirani su na održavanje integriteta u kome potrošači komuniciraju sa drugim učesnicima;
- Bezbednost mreže prelazi sa fokusa na modele uređaja baziranih na LAN tehnologiji u tehnologije sigurnog pristupa;
- Pristup celovitom životnom ciklusu za zaštitu dinamičkih zahteva aplikacija u oblaku;

[32] https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020/

- Tehnologija mrežnog pristupa bez poverenja, počinje menjati VPN-ove.[33]

Prilikom istraživanja novih pojava i procesa u sajber domenu, koji su uslovljeni pandemijom kovid 19, analitičari ENISA-e najavljuju početak nove dekade sa potpuno novim normama, dubokim promenama u fizičkim i digitalnim sistemima koji opredeljujuće utiču na fizionomiju i konfiguraciju savremenih sajber pretnji i rizika, uključujući tu i njihov evolucioni kontekst.

Primenjujući inoviranu metodologiju za procenu rizika u sajber okruženju, ENISA najpre određuje fundamentalne izazove u sajber bezbednosti, a tek nakon toga, uz pomoć metoda dedukcije definiše i osnovne trendove. Rezimirajući udarne tačke relevantnih nalaza iz napred navedenih razmatranja, prema iznetoj metodologiji, ENISA utvrđuje 10 izazova u sajber bezbednosti i to:
- suočavanje sa sistemskim i složenim rizicima;
- široko rasprostranjena primena AI;
- smanjenje nenamernih grešaka, a time i opšte ranjivosti digitalnih sistema;
- uspostavljanje diversifikovanog lanca snabdevanja i pretnji trećih strana;
- bezbednosna automatizacija i instrumentacija;
- redukovanje lažno pozitivnih rezultata;
- bezbednosne strategije bez poverenja;
- greške prilikom migracije poslovnih podataka u oblak;
- hibridne pretnje i novi modus operandi u domenu virtuelnih pretnji fizičkom svetu sa hibridnim dimenzijama;
- veće oslanjanje na javnu infrastrukturu u oblaku.

Kroz izradu najnovije izveštaja pod nazivom „Procena pretnji organizovanog sajber kriminala“ SOCTA 2020[34], pored razrade i akceptiranja krajolika savremenih pretnji iz domena sajber kriminala, isticanja ili razrade ranjivosti internet platformi, određivanja najugroženijih sektora – meta napada, određeno je 5 novih trendova koji su u odnosu na ranije izveštaje i period prilično modifikovani i usklađeni sa aktuelnim promenama izazvanih pandemijom kovid 19[35]. U 5 trendova koji obeležavaju aktuelne sajber pretnje ubrajamo:
- nadogradnja zlonamernog softvera;
- pretnje postaju sve mobilnije;
- kriminalni akteri koriste nove vrste datoteka za širenje zlonamernog softvera (ISO, IMG, DOC, ZIP i XLS);
- rast ciljanog i koordinisanog ransomver napada;

[33] Isto

[34] EUROPOL, Procena pretnji organizovanog sajber kriminala 2020, Hag, Holandija

[35] Durbin, Steve, "The Future's Biggest Cybercrime Threat May Already Be Here", https://www.darkreading.com/vulnerabilities---threats/the-fu-tures-biggest-cybercrime-threat-may-already-be-here/a/d-id/1338439, 2020

- rast broja napada automatskim injektiranjem ukradenih korisničkih imena i kombinacija lozinki putem velikog broja automatizovanih login zahteva usmerenih na web aplikacije.

Izvlačenje dubljih normativnih supstanci iz svega navedenog, podrazumeva daleko šire sagledavanje konteksta pandemije i svih propratnih pojava i nus efekata koje ona sa sobom neizbežno nosi, što predstavlja polaznu osnovu i fundamentalnu poziciju za sve političke aktere, specijalizovane i profesionalne službe, proizvođače savremenih tehnoloških sredstava i uređaja, vlasnika i operatora kritičnih infrastruktura, kao i samih korisnika/potrošača da značajno unaprede svest, znanje i potrebu zaštite od navedenih pretnji i ranjivosti, kao i razvijanje sposobnosti za prepoznavanje, preveniranje i saniranje svih izazova, pretnji, rizika i eventualnih šteta. Osnov za jedan takav poduhvat leži u formalizovanju adekvatne politike sajber bezbednosti kao integralnog dela nacionalne politike bezbednosti i dizajniranje fleksibilnog sistema i mehanizama zaštite po opšteprihvaćenim evropskim i svetskim standardima.

Zaključak

Za razliku od prethodnih kriza i katastrofalnih događaja, pandemija kovid 19 u širokom luku i različitim intenzitetom pogađa pojedince, kompanije, javne službe, operatere kritičnih usluga, državne strukture, najpre izazivajući osećaj trajne ranjivosti, kao i permanentnog stanja ugroženosti, stvarajući promenljivo strateško okruženje u kome dominira tržište straha gde se većina građana ne oseća dovoljno bezbedno i zaštićeno.

Kovid 19 u velikoj meri ubrzava i produbljuje konfiguraciju rizičnog okruženja u kome se sistemski i evoluirajući rizici uzrokovani pandemijom susreću, umrežavaju i prožimaju zajedno sa vektorima i strateškim varijablama u domenu sajber kriminala, pri čemu dolazi do konvergencije između njih, a to praktično znači stvaranje novih hibridiziranih pretnji i rizika koji pogađaju i privredu i javni sektor i pojedince, bez razlike.

Globalna pandemija kovid 19, predstavlja, ne samo ozbiljnu zdravstvenu krizu, već i značajan rizik i vektor sajber bezbednosti. Naime, kriminalni akteri su veoma brzo shvatili potencijal globalne zdravstvene krize i prelaska svih aktivnosti iz fizičke u digitalnu sferu, što je značajno umnožilo mogućnosti za uspešnu kriminalnu aktivnost, kako po obimu, tako i po visini štete koju mogu da proizvedu.

U praksi je stvorena jedna fundamentalna asimetrija: rast i šira digitalizacija donose brojne prednosti, dobrobiti, beneficije i sl., dok se istovremeno registruje i povećanje pretnji, rizika i šteta iz sajber prostora, a naročito u domenu sajber kriminala, što potvrđuju brojne zvanične statistike na svim meridijanima.

Najnovija istraživanja, rezolutno pokazuju da se svet u globalu suočava sa rapidnim i raznovrsnim rastom sajber kriminala uz korišćenje savremenih tehnika i mehanizama. Prema istim nalazima, očekuje se masovna primena inovativnih tehnika sajber napada u kojima će se koristiti alati poput automatizovanog hakovanja sa primenom veštačke inteligencije, kao i sve veće učešće botnet mreža i interneta stvari kao vektora ranjivosti širokog spektra.

Sve češća primena interneta stvari, pametnih uređaja i veštačke inteligencije i sve veća dostupnost istih različitim akterima, uključujući i one zlonamerne, može imati takve razmere da kriminalni akteri mogu bez većih teškoća uspostaviti nove nivoe neovlašćenog nadzora građana, privrede i državnih organa, povrede privatnosti i sl., čime se otvara put za radikalno i nekontrolisano prelivanje moći između pojedinaca, korporacija i država, ali i kriminalnih aktera.

U tom kontekstu posebno zabrinjavaju statistički podaci o kretanju sajber kriminala i njegovog sve izraženijeg ubrzanja i disperzije, kao i trendova njegovog daljeg razvoja. Stručnjaci predviđaju da će sajber kriminal samo u 2021. godini pričiniti finansijsku štetu od 6 triliona američkih dolara, dok će do 2025. godine taj iznos porasti do 10,5 triliona dolara. **Taj iznos je daleko veći od štete nanete prirodnim katastrofama u svetu u isto vreme, ali i daleko nadmašuje iznose od globalne trgovine svim narkotičkim sredstvima zajedno.**

Uvažavajući sve napred navedeno, proizilazi jasan i vrlo uverljiv zaključak: svaki dalji korak u razvoju i primeni tehnoloških sredstava i dostignuća, usko je vezan sa širenjem skale rizika od njihove primene. Navedeno implicira stav, da ukoliko se nastavi ovaj trend štetnih posledica vezanih za primenu tehnoloških sredstava i dostignuća, bez adekvatnog operativnog odgovora, mora se postaviti pitanje svrsishodnosti i racionalnosti daljeg nekontrolisanog širenja digitalizacije i njene dostupnosti zlonamernim akterima, ako se prethodno ne razreše pitanja u vezi uspostave adekvatnog međunarodnog pravnog okvira u cilju sankcionisanja takvih aktivnosti, kao i definisanje savremene politika sajber bezbednosti i najzad, dizajnira efikasan i institucionalizovan sistem sajber bezbednosti sa svim pratećim elementima vezanim za organizaciju, logistiku, planiranje i operativne kapacitete.

Pandemije globalnih razmera, ukoliko su aktivno povezane sa drugim kriznim stanjima, po pravilu, su izuzetno komplikovan objekat usmeravanja, regulisanja i upravljanja. Drugim rečima, stepen upravljivosti je jako nizak, bez obzira na obuhvat, alokaciju resursa i preduzete radnje.

Suptilnija analitička razlaganja dala bi mnogo čvršću podlogu za ocenu da je situacija u vezi pandemije jedan nedovoljno upravljiv i za usmeravanje nepogodan objekt, kako u domenu formulisanja, tako i u domenu implementacije političkih mera, aktivnosti i operativnih postupaka, posebno u području sajber bezbednosti.

Literatura:

- "$19 million worth of iPhones stolen in massive identity theft scam" June 15, (2019). 9To5Mac.
- "2020 State of Application Services Report" F5 Networks, (2020). https://www.f5.com/state-of
- "2020 State of Malware Report". February, 2020. Malware Bytes.
- "BDO's Fall 2019 Cyber Threat Report: Focus on Healthcare" (October 2019). BDO.
- "Coronavirus phishing emails: How to protect against COVID-19 scams" (2020).
- "Cost of Data Breach Report." (2019). IBM Security, Ponemon Institute.
- "Cyber Threatscape Report. (2019)." IDefense – Accenture.
- "Email: Click with Caution – How to protect against phishing, fraud, and other scams" June,
- "Insider Threat Report", (2019). Verizon.
- "Malware statistics and facts for 2020" July 29, (2020). Comparitech.
- "Naming the coronavirus disease (COVID-19) and the virus that causes it" (2020). WHO.
- "Physical Security Guide". Kisi. https://pages.getkisi.com/physical-security-guide
- "What is a data breach and what do we have to do in case of a data breach?" European Commission. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military intelligence-service-exposed.
- "What is Formjacking and How Does it Work?", Norton. https://us.norton.com/internetsecurity
- "What Is Phishing?". Cisco. https://www.cisco.com/c/en/us/products/security/email
- "What you – and your company – should know about cyber insurance", August 20, 2019.
- 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email
- 2019. Kaspersky. https://securelist.com/ddos-report-q1-2019/90792/9583-4d86-9d1e-8b2735af5168.xhtml
- Bleeping Computer. https://www.bleepingcomputer.com/news/security/cryptominers-still-top
- Durbin, Steve, (2020). "The Future's Biggest Cybercrime Threat May Already Be Here", https://www.darkreading.com/vulnerabilities-threats/the-futures-biggest-cybercrime-threat-may-already-be-here/a/d-id/1338439
- EUROPOL, Procena pretnji organizovanog sajber kriminala 2020, Hag, Holandija
- Evropska komisija, COM (2020). 605 final, Brisel, str. 8

- Fox Business, White House confirms cyberattack report on U.S. Treasury by foreign goverment, www.foxbusiness.com
- Harjinder, S.L., Lynsay A.,S., Jason R.C.N., Arnau, E., Gregory, E., Carsten M. & Xavier, B. (2020). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic, str. 1-2
- Herbert, S. (2016). Complexity, Systemic Risks and Converging Technologies, http://www.herbert.saurugg.net/2016/blog/vernetzung-und-komplexitaet/complexity-systemic-risks-and-converging-technologies
- Izveštaj Europola o sajber kriminalu za 2020. godinu. https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime
- https://9to5mac.com/2019/06/05/19-million-worth-of-iphones/
- https://blog.malwarebytes.com/101/2019/05/everything-you-need-toknow-about-atm-attacks-and-fraud-part-1/
- https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf
- https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
- https://securityboulevard.com/2020/11/the-enisa-cybersecurity-threat-landscape/
- https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html
- https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf
- https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber
- https://www.comparitech.com/antivirus/malware-statistics-facts/
- https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020/
- https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020/
- https://www.ibm.com/security/data-breach
- https://www.oreilly.com/library/view/learning-malware-analysis/9781788392501/17a1735d
- https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming
- Jovi, U. (2019). "Everything you need to know about ATM attacks and fraud: Part 1." May 29, (2019). Malwarebytes Labs.
- Mark, L. & Daniel, P. (2018). Securitization and the global politics of cybersecurity, Global Discourse: An interdisciplinary journal of current affairs, Volume 8, Number 1, January, Bristol, Engleska, 2020, pp. 100-115
- Mladenović D. (2016). Multidisciplinarni aspekti sajber ratovanja, doktorska disertacija, Fakultet organizacionih nauka, Univerzitet u Beogradu

- Monnappa, K.A. (2018). "Learning Malware Analysis." June 2018. O'reilly.
- Oleg, K., Ekaterina, B. & Alexander, G. (2019). "DDoS attacks in Q1 2019" May 21,
- Putnik N. (2009). Sajber prostor i bezbednosni izazovi, monografija, Fakultet bezbednosti, Univerzitet u Beogradu
- Sergiu, G. (2019). "Cryptominers Still Top Threat In March Despite Coinhive Demise." April 9, 2019.
- Talos. https://blog.talosintelligence.com/2019/08/cyber-insurance-FAQs.html
- Tomer, S. (2019). "Updated: This DDoS Attack Unleashed the Most Packets Per Second Ever. Here's Why That's Important." April 30, (2019). Imperva. https://www.imperva.com/blog/this-ddos-attack unleashed-the-most-packets-per-second-ever-heres-why-thats-important/
- The European Union External Action Service (EEAS) (2020). "A Europe that Protects: Countering Hybrid Threats", https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en accessed 27 July 2020.
- The European Union External Action Service (EEAS) (2020). "A Europe that Protects: Countering Hybrid Threats", https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en accessed 27 July 2020

Petar Čelik
Miodrag Komarčević
Milovan Dimić

UDC 343.53:[616.98:578.834
343.533::004

DOI: 10.5937/MegRev2004049C
Review Scientific Article
Received 28.04.2020.
Approved 20.06.2020.

CONVERGENCE OF THE KOVID 19 AND CYBER CRIME PANDEMIC: CONTEXT AND SCOPE

Summary: *The deep and widespread global crisis caused by the coronavirus pandemic has directly or indirectly generated numerous and different phenomena and processes that have completely changed the perception and way of life and work and thus established a new context, radically changing the security configuration and landscape. At the same time, the current crisis has become the main accelerator of several important trends and transformations in the field of cybersecurity: first initiations, then support for the processes of privatization, militarization, and securitization of this area. In the strategic environment, two completely different, by their effects and mode of action, recent processes coincided, resulting in a fundamental asymmetry: increasing intensity, dynamics, and frequency of cyberattacks, while drastically reducing the operational capabilities of the state and other actors on the plan of their prevention and suppression.*
The main goal of the research is, first, to consider and then determine the global context that produces different and very complex interrelationships, interactions, conditionality between the spread of a pandemic on the one hand, and the expansion of hybrid threats, especially cybercrime, on the other forms, modalities, narratives, and goals.
Due to the complexity, multidimensionality, and relevance of the problem-subject set, standard methodological tools were applied during the research, based on DESK methods. In the concluding section, the conversational meaning and hybrid nature of cyber threats emphasize the importance and need to innovate existing public policies and security agendas in creating a combined hybrid response with pronounced synergistic effects.

Keywords: *Pandemic, Cybersecurity, Hybrid threats, Disruptive technologies*