CYBER BEZBJEDNOST- IZAZOVI U RADU STRUKTURA ZA SPROVOĐENJE I ZAŠTITU ZAKONA SA ASPEKTA VISOKOTEHNOLOŠKOG-SAJBER KRIMINALITETA ZA OBLAST: INTERNET / CHALLENGES IN THE OPERATION OF ENFORCEMENT AND PROTECTION STRUCTURESLAW FROM THE ASPECT OF HIGH-TECH-CYBER CRIME FOR THE FIELD: INTERNET

Vlado Jovanić[1], Glavni inspektor, Zamjenik načelnika, Ma Boris Tušinski[2]
[1]Uprava za policijsku podršku, MUP Jug Bogdana 108, 78 000 Banja Luka, Republika Srpska,
[2]OSA/OBA Bosna i Hercegovina,
e- mail: vlado.jovanic@hotmail.com, vlado.jovanic@gmail.com, boris.tusinski@gmail.com

Stručni članak
UDK / UDC 343.2:004.056

Sažetak
Globalizacija društva je neminovno dovela do umrežavanja i povezivanje svih subjekata međunarodnih odnosa u sistemu komunikacija i razmjene informacija na svim nivoima. Putem IKT (informaciono komunikacione tehnologije) svaki pojedinac (fizičko lice) i kolektivitet (pravno lice, država) postali su aktivni učesnici i korisnici neke od društvenih mreža, neke aplikacije ili poslovne platforme. Ovakav proces povezivanja putem Interneta doveo je i do određenih zloupotreba (nastanak novih pojavnih oblika krivičnih djela) koje su rezultirale materijalnom ili nekom drugom vrstom štete kako pojedincu tako i kolektivitetu ili društvenoj zajednici u cjelini. Sa druge strane potreba da se pojedinac, kolektivitet, odnosno društvena zajednica zaštite i da im se omogući bezbjedno okruženje za život i rad, postavila je nove izazove pred zakonodavca i organizacione strukture koje se pod njihovim nadzorom bave sprovođenjem i zaštitom zakona, prava i bezbjednosti građana i društvene zajednice. Da bi se nadležni subjekti uspješno suprostavljali novim izazovima, neophodno je da prate nove trendove prijetnji kao i da se blagovremeno i adekvatno obuče, opreme i ostanu u kontinuitetu trendova. Kako bi ovaj proces bio održiv neophodno je prepoznati glavne izazove u korištenju IKT koji otežavaju rad navedenim subjekatima kroz nove pojavne oblike krivičnih djela.
Ključne riječi: *Internet, IKT, društvene mreže, visokotehnološki kriminalitet, bezbjednost, izazovi.*
JEL klasifikacija K140, K240, K400, K420

Abstract
The globalization of society has inevitably led to the networking and connection of all subjects of international relations in the system of communication and information exchange at all levels. Through ICT (information communication technology), every individual (natural person) and collectivity (legal entity, state) have become active participants and users of some social network, some application or business platform. This process of connecting via the Internet also led to certain abuses (the emergence of new forms of criminal acts) that resulted in material or other types of damage to both the individual and the collective or the social community as a whole. On the other hand, the need to protect the individual, the collective, or the social community and to provide them with a safe environment for life and work, posed new challenges to the legislator and the organizational structures that, under their supervision, deal with the implementation and protection of laws, rights and the safety of citizens. and social communities. In order for competent entities to successfully confront new challenges, it is necessary to follow new trends in threats, as well as to be trained and equipped in a timely manner and to remain in the continuity of trends. In order for this process to be sustainable, it is necessary to recognize the main challenges in the use of ICT that make it difficult for the aforementioned entities to work through new forms of criminal acts
Keywords: *Internet, ICT, social networks, high-tech crime, security, challenges.*

UVOD

Kontinuirani informaciono komunikacioni i tehnološki (IKT) razvoj društveno-ekonomskih odnosa izvršio je i značajan uticaj na nastanak i razvoj društveno štetnih pojava u vidu novih oblika kriminaliteta, ali je takođe omogućio i razvoj novih metoda za suzbijanje kako postojećih, tako i tih novih oblika kriminaliteta. Dakle, kontrolisana (ili nekontrolisana) ekspanzija u razvoju informaciono komunikacionih tehnologija omogućila je i korišćenje tehnologije za dokumentovanje (identifikaciju, pronalaženje, prikuplanje, i čuvanje) tragova i dokaza u novom formatu, odnosno u elektronsko-digitalnoj formi. Sa druge strane, ubrzani razvoj informacionih tehnologija i telekomunikacija uslovio je kontinuiranu pažnju i angažovanje zakonodavca za praćenje trendova (društveno socijalnih promjena) koje se dešavaju, sa stalnom tendencijom prilagođavanja i usklađivanja postojećih zakonodavnih okvira u cilju efikasnog i adekvatnog načina u postupanju sa novim izazovima. Informaciono komunikacione tehnologije kao moćno tehničko sredstvo, našle su svoju dobronamjernu primjenu u svim sferama ljudskog života i biznisa, ali su isto tako postali i moćno sredstvo za izvršenje krivičnih djela. Ovaj novi vid kriminaliteta (visokotehnološki, kompjuterski, cyber kriminalitet) predstavlja kriminalitet čiji izvršioci posjeduju posebne informatičke vještine i znanja, koja permanentno nadograđuju i višestruko multipliciraju. Jedan od problema je u nepostojanju dovoljno efikasnog sistema nadgledanja interneta i telekomunikacija u cilju otkrivanja krivičnih djela visokotehnološkog kriminala, kao i efikasna platforma za prijavljivanje ovih krivičnih djela u *online* režimu. Kao poseban problem se javlja i potreba za boljom saradnjom na bezbjednosnom polju sa naučno-edukativnom zajednicom, nevladininim organizacijama, privatnim sektorom itd. (*Jovanić, 2024*) Zakonito presretanje komunikacija i analiza podataka i informacija koje nastaju u komunikacijskoj interakciji između subjekata u potpunosti zavisi od saradnje telekom operatera i vladinih institucija za sprovođenje i zaštitu zakona. To praktično znači da uspješnost subjekata suprostavljanja novim izazovima u pogledu krivičnih djela zavisi od dostignutog stepena razvoja i implementacije pozitivnih propisa u društveno-ekonomske odnose. Naravno, zakonodavac u predmetnoj društveno ekonomskoj organizaciji-strukturi (državi) mora da vodi i računa o ljudskim pravima i slobodama građana koje štiti. Zato se uvijek postavlja pitanje čemu dati veći značaj, pravima ili bezbjednosti, odnosno kako napraviti idealan kompromis između ova dva osnovna ustavna postulata. Ova dilema je rješena na međunarodnom nivou kroz donošenje Konvencije o ljudskim pravima i slobodama u kojoj je u članu 8. (Pravo na poštovanje privatnog i porodičnog života) omogućeno narušavanje zagarantovanih prava u slučaju kada je to zakonom predviđeno (eksplicitno u posebnim situacijama ugrožavanja) a neophodno je kao mjera u demokratskom društvu i u interesu nacionalne i javne bezbjednosti, ekonomske dobrobiti zemlje, sprječavanja nereda ili kriminaliteta, zaštite zdravlja i morala ili zaštite prava i sloboda drugih.[137] U radu će kroz tri vezana članka biti obrađeni izazovi sa kojima se u svom radu suočavaju strukture za zaštitu zakona (LEA) kroz tri vezane oblasti: A. Oblast: Internet, B. Oblast: Telekomunikacije i C. Oblast: Nadzor i geolociranje kao i preporuka za prevazilaženje problema.

[137] Evropska konvencija o ljudskim pravima, Evropski sud za ljudska prava, Savjet Evrope, Strazbur, strana 10, https://www.ombudsmen.gov.ba/documents/obmudsmen_doc2013041003092706bos.pdf, 26.07.2024., 08.10 h.

1.PROBLEMI U RADU POLICIJSKIH STRUKTURA NA OTKRIVANJU, SPRJEČAVANJU I PROCESUIRANJU VTK

Pravna regulativa, metodi i politike kriminalnog progona unutar pojedinih zemalja, kao i međunarodna saradnja, ne prate ubrzanu ekspanziju i razvoj IKT. Mogućnosti praćenja i nadogradnje pravne regulative, metoda i politika kriminalnog progona u skladu sa trenutnim trendovima kriminaliteta su determinisane, prije svega ekonomskim razvojem svake pojedine države. Pored raspoloživih finansijskih, infrastrukturnih i ljudskih resursa, neophodna je i visoko razvijena bezbjednosna svijest svih korisnika IKT. U kontekstu navedenih parametara, trenutno samo nekoliko država poseduje efikasne pravne okvire i mehanizme za sprečavanje (prevenciju) i suprostavljanje (represivni mehanizmi) svim vidovima visokotehnološkog kriminaliteta. Ovakva situacija predpostavlja i zahtijeva maksimalno angažovanje zakonodavaca u kontinuiranoj i brzoj implementaciji svih novonastalih društveno štetnih promjena u ovoj oblasti kriminaliteta u domaće zakonodavstvo kako bi se efikasno razvijali svi potrebni-neophodni kapaciteti za sprečavanje, suprostavljanje, procesuiranje i mađunarodnu saradnju. Sa druge strane, nedostatak proaktivnosti i shvatanje ozbiljnosti ovog novog pojavnog oblika kriminaliteta u njegovom globalnom kontekstu može dovesti do nesagledivih posljedica u zlouptrebi IKT. (*Jovanić, 2024*)

Društveno pravna reakcija na ugroženost visokotehnološkim kriminalitetom sa aspekta pojedinačnih nacionalnih zakonodavstava treba da se kreće u sljedećim okvirima: (*Jovanić, 2024*)

- preduzimanje preventivnih mjera (sprječavanje i ublažavanje posljedica kompjuterskog kriminala i razvoj bezbjednosne svijesti kod korisnika IKT);
- usvajanje i implementacija odgovarajućih zakonodavnih rješenja u oblasti materijalnog i procesnog prava sa aspekta nacionalnih potreba i međunarodnie saradnje (uspostava pravnih mehanizama i instrumenata za otkrivanje i sprječavanje svih oblika visokotehnološkog kriminaliteta);
- razvijanje ljudskih i materijalnih resursa nadležnih policijskih i pravosudnih organa za efikasnu primjenu povjerenih zakonskih ovlašćenja.

Kada je u pitanju međunarodna saradnja u globalnim nastojanjima za otkrivanje i sprječavanje visokotehnološkog kriminaliteta možemo konstatovati da postoje sljedeći problemi u domaćem nacionalnom zakonodavstvu: (*Jovanić, 2024*)

- neusklađenost pravnog definisanja u smislu inkriminacije radnji izvršenja i opsega radnji koje predstavljaju krivično djelo visokotehnološkog kriminala;
- neadekvatna profesionalna obučenost subjekata (policijskih službenika, tužilaca i sudija) koji postupaju i primjenjuju određena zakonska ovlašćenja u predmetima visokotehnološkog kriminala;
- neusklađenost određenih procesnih mehanizama u nacionalnim zakonodavstvima u pogledu istraga krivičnih djela visokotehnološkog kriminala;
- inertnost u praćenju trendova visokotehnološkog kriminaliteta i implementaciji novih procesnih mehanizama u zakonodavstvo (razmjena informacija i dobrih praksi).

U suštini, ova nova vrsta kriminaliteta predstavlja kriminalnu djelatnost koja se u principu odvija u elektronskom-digitalnom okruženju. Ako prihvatimo konstataciju (prema Konvenciji o VTK) da se pod kompjuterskim sistemom podrazumeva svaki uređaj ili više međusobno povezanih različitih uređaja i komponenti koji vrše automatsku obrada određenih podataka (ili neku drugu funkciju koja podrazumijeva obradu ili analizu dostupnih podataka) onda se podrazumijeva da bez tih uređaja, komponenti i kompjuterskih mreža nema ni sajber (Internet kriminal, eKriminal, kriminal visokih tehnologija, mrežni kriminal, kompjuterski, računarski i visokotehnološki

kriminal) kriminala. Ovaj termin je veoma širok i podrazumijeva različite kriminalne aktivnosti usmjerene prema kompjuterima, kompjuterskim sistemima i mrežama, uključujući napade na kompjuterske podatke i sisteme, napade vezane za računare i druge sadržaje u vezi sa računarima. (*Jovanić, 2024*)

Kompjuterska mreža podrazumjeva međusobno povezane kompjutere i druge uređaje koji služe kao mreža i sredstvo za povezivanje, komunikaciju i razmjenu informacija interesno povezanih poslovnih subjekata. Možemo konstatovati da sajber (cyber) kriminal predstavlja oblik kriminalnog ispoljavanja kod kojeg je sajber (cyber) prostor ujedno i okruženje u kojem se kompjuterske mreže pojavljuju kao sredstvo, cilj, dokaz ili okruženje u kojem se odvijaju određena krivična dela. (*Jovanić, 2024*)

Sajber kriminal predstavlja novi pojavni oblik kriminaliteta koji zahtjeva visoku tehničku osposobljenost, opremljenost, samostalnu kvalitetnu i visokotehnološki razvijenu informaciono-komunikacionu infrastrukturu. S obzirom da IKT ima globalnu zastupljenost i dostupnost ona predstavlja svojinu koja nema titulara, u okviru koje paralelno postoje i funkcionišu različite vrste stvarnosti (virtuelna i realna) a komunikacija između subjekata može biti jednostrana, višestrana ili zajednička. Ovakvo teško kontrolisano i bezbjednosno zaštićeno okruženje predstavlja i problem inkriminacije za svako pojedino nacionalno zakonodavstvo u poimanju razmjera ove vrste kriminala i njegovoj društvenoj opasnosti. Ovo je i razlog za stav da je sajber kriminalitet najizrazitiji oblik transnacionalnog kriminala čije otkrivanje, sprečavanje i dokazivanje nije i ne može biti tradicionalno (konvencionalno) upravo iz razloga što društveno-socijalni i ekonomski aspekt ovog kriminala nije isti kao kod klasičnog transnacionalnog kriminaliteta budući da sajber prostor podrazumijeva drugačije procedure i procesna pravila. (*Jovanić, 2024*)

Dokazi koji nastaju prilikom izvršenja krivičnih djela u novonastalom prostoru se nalaze i ispoljavaju u potpuno novom, digitalnom formatu što može da predstavlja određni problem za njihovu upotrebu u sudskom postupku. Transformacija digitalnog dokaza u materijalni (papirni) oblik prihvatljiv za sudski postupak, takođe može predstavljati problem jer ni ovaj postupak nije naveden u značenju izraza i osnovnih pojmova u procesne zakone u RS i BiH. Pored navedenih nedostataka, najveći problem je svakako nedostatak edukovanih kvalifikovanih operativnih radnika, tužilaca i sudija, odnosno operativnih, tužilačkih i pravosudnih specijalizovanih organizacionih struktura. Iz navedenog je očito da je digitalna forenzika kao nauka bitan faktor u istragama vezanim za IKT i da je neophodno da kao takva dobije mjesto u pravnom sistemu u svakom nacionalnom zakonodavstvu. To znači da bi pravnici (policijski službenici, tužioci i sudije) trebali da posjeduju određena informatička znanja za sprovođenje istrage (digitalna istraga), odnosno, da bi mogli koristiti dostupne naučne metode i sredstva (digitalna forenzika) u skladu sa propisanim standardima kako bi prikupljeni dokazi (digitalni dokazi), činjenice i nalazi vještačenja (digitalna forenzika) bili korišteni i prihvaćeni u sudskom postupku. (*Jovanić, 2024*)

Ekspanzija IKT je postavila nove standarde u proizvodnji informaciono komunikacionih uređaja tako da se u svaki novi multimedijalni uređaj ugrađuju komponente, odnosno aplikacije koje omogućavaju konekciju u globalne sisteme i mreže i razmjenu informacija putem takozvane „sporedne ili bočne veze". Praktično su ti novi uređaji, odnosno aplikacije koji se nalaze u pametnim telefonima, automobilima, IOT[138] uređajima ili bilo kom drugom modernom

[138] IoT (Internet of Things), Internet stvari, uređaji su nestandardni računarski uređaji koji se bežično povezuju na mrežu i imaju mogućnost razmjene podataka. Internet stvari podrazumijevaju proširenje internet konekcije izvan standardnih uređaja, kao što su desktop računari, laptopovi, pametni telefoni i tableti, na bilo koji opseg tradicionalno „glupih" fizičkih uređaja i svakodnevnih objekata bez interneta. Povezani u IK sistem, ovi uređaji mogu da komuniciraju međusobno i/ili preko interneta. Takođe se mogu daljinski nadgledati i kontrolisati. https://www.techtarget.com/iotagenda/definition/IoT-device (02.02.2023., 11.52 h) Primjer IoT uređaja:

informaciono komunikacionom uređaju omogućili da ostvare konekciju direktno (sporedne ili bočne veze) preko Bluetooth, Vi-Fi i V2Ks interfejsa i razmenjuju datoteke, glas, poruke, strimuju podatke ili na drugi način komuniciraju. Sa aspekta agencija za sprovođenje zakona presretanje, odnosno istraga vezanih komunikacija predstavlja veliki problem i izazov u odnosu na standardne komunikacione usluge koje nude ovlašteni telekom i mrežni operateri (mobilni i fiksni) i internet provajderi. U klasičnim istragama oslonac u prikupljanju podataka agencijama za sprovođenje zakona pruža nadležni mrežni operater u vidu određenih metapodataka i/ili komunikacionih sadržaja ciljanih komunikacija preko LIOS interfejsa. U situacijama kada su uređaji „bočno povezani"[139] nema podataka za upit kod mrežnih operatera ili internet provajdera. Ovakve situacije u nedostatku kritičnih podtaka (lokacije, identiteta, metapodataka, komunikacionih sadržaja, obrazaca poziva i drugih podataka), stavlja u veoma nezgodnu poziciju agencije za sprovođenje zakona u konkretnim istragama. Jedan od problema je i airdrop (*eardroop*) usluga koju posjeduju određeni uređaji (Apple) koja onemogućava presretanje komunikacija.

Digitalni podaci su dospjeli na sam vrh liste kao primarni izvor dokaza u istragama, a često su informacije prikupljene sa mobilnih telefona glavni-vodeći izvor dokaza. Zbog rasprostranjenosti mobilnih uređaja koji se koriste u kriminalnim incidentima, forenzički alati za analizu podataka sa mobilnih telefona predstavljaju osnovni zahtjev i potrebu agencija za sprovođenje zakona. Sa druge strane sve agencije treba da razvijaju sposobnost da sami strateški obrađuju mobilne i druge pametne uređaje u smislu potpune akvizicije adekvatnim digitalno-forenzičkim alatima.

Svaka vlada nastoji da zaštiti svoju kritičnu infrastrukturu od svih vrsta ugrožavanja i napada, koji eskaliraju i po obimu i po ozbiljnosti širom svijeta, pri čemu veliki broj administratora bezbjednosti kritične infrastrukture priznaju da su imali najmanje jedan proboj i ugrožavanje operativne tehnologije u posljednje tri godine. Zaštita kritičnih resursa i krivično gonjenje počinilaca takvih napada je ključni prioritet za agencije za sprovođenje zakona i obavještajnih agencija. Međutim, većini nedostaju alati za praćenje napada do njihovog izvora, kao i za akviziciju-prikupljanje forenzičkih digitalnih dokaza potrebnih za identifikaciju i krivično gonjenje napadača-počinilaca.

Zakonito presretanje i nadzor svih vrsta komunikacija u potpunosti zavisi od saradnje telekom i mobilnih operatera sa institucijama za zaštitu i sprovođenje zakona. Sa druge strane, nadzor društvenih mreža i internet saobraćaja putem internet provajdera koji mogu biti i u privatnom vlasništvu zahtijeva i određena-posebna zakonska rješenja u svakoj državi. Međutim, i pod uslovima da su ispunjeni svi zakonski preduslovi i nadležnim agencijama omogućen monitoring i nadzor telefonskog i internet saobraćaja i drugi neophodni poslovi i aktivnosti koji zadiru u privatnost i građanska prava, neophodna je i tehnološka podrška u vidu digitalno-forenzičkih alata kojima se mogu identifikovati i dokumentovati relevantni digitalni incidenti i dokazi. Praktično to

Povezani uređaji su dio IK sistema u kojem svaki uređaj komunicira sa drugim srodnim uređajima u okruženju kako bi razmjenio određene informacije. Ovakvi uređaji se mogu razvrstati u tri grupe: korisničke-potrošačke, poslovne i industrijske. Pod korisničke-potrošački povezane uređaje podrazumijevamo tzv. pametne televizore, pametne zvučnike, igračke, nosive i druge pametne uređaje. U pametnoj kući, na primjer, uređaji su dizajnirani da osjete-detektuju prisustvo lica i reaguju prema predhodno unesenim protokolima. Kada lice stigne autom u blizinu kuće, auto komunicira sa uređajom (smješten u garaži) koji je programiran da otvori garažna vrata. Kada lice uđe u unutrašnjost kuće, termostat je već podešen na željenu temperaturu i uključio je grejne elemente, a osvetljenje se podešava na niži intenzitet i boju, jer podaci koje je centralnoj jedinici poslao pametni sat pokazuju da je dan bio stresan. Ostali pametni kućni uređaji uključuju prskalice koje prilagođavaju količinu vode koja se daje travnjaku na osnovu vremenske prognoze i robotske usisivače koji uče koje dijelove kuće se najčešće moraju čistiti.

[139] Posredno povezivanje putem drugog uređaja na mrežnog operatera ili internet provajdera (telefon preko drugog telefona ili preko mobilnog rutera...).

znači da je neophodna materijalno-tehnička podrška u vidu adekvatnih softvera i hardvera, odnosno materijalnih, infrastrukturnih i ljudskih resursa kako bi se mogle prepoznati, otkriti i otkloniti sve vrste bezbjednosnih prijetnji, krivična djela i identifikovati izvršioci. Iz navedenog je očita tendencija uticaja IKT na rad agencija za sprovođenje i zaštitu zakona i ta veza postaje obrnuto proporcionalna u odnosu na otkrivenost i procesuiranje izvršilaca krivičnih djela (veća implementacija IKT i njenih digitalno-forenzičkih proizvoda u rad agencija za sprovođenje i zaštitu zakona, uticaće i na veću otkrivenost prijetnji i izvršilaca i efikasnost u procesuiranju i presuđivanju). To znači da će veća materijalno finansijaka podrška agencijama omogućiti i njihov efikasniji rad, budući da kriminalci i teroristi koriste komunikacije koje su tehnološki na mnogo višem nivou od tehnoloških mogućnosti agencija koje trebaju da im se suprostavljaju. Takođe je bitan faktor u radu agencija za sprovođenje i zaštitu zakona na vrijeme prepoznati i identifikovati prijetnju, kao i način i mogućnost za njeno sprječavanje, a to znači biti u kontinuitetu i trendu sa proizvodima i uslugama koje se nude na tržištu za efikasno otkrivanje i otklanjanje prijetnji (specijalizovane kompanije za softver i hardver i efikasni alati za dokumentovanje digitalnih dokaza koje nude).

2.GLAVNI IZAZOVI U RADU KOMPANIJA-ORGANIZACIJA KOJE KORISTE IKT

Digitalizacija na globalnom nivou i međusobna mrežna povezanost, nametnula je i potrebu za uvođenje novih naučnih metoda i disciplina u vidu digitalne forenzike za identifikaciju, prevenciju i sprječavanje sajber prijetnji, posebno u korporativnim okruženjima. Prije nekoliko godina zbog COVID pandemije, organizacije-kompanije su bile primorane na uvođenje rada od kuće i na novi vid organizacije rada kroz korištenja udaljene radne snage. Prihvatajući ovu novu realnost deperimetrizovanosti mreže (izlazak iz bezbjednosno kontrolisanog okruženja organizacije-kompanije), vladine agencije i organizacije privatnog sektora usvojile su „Princip nultog povjerenja" u nastojanju da se osmisli nova sajber bezbjednosna (paradigma) teorija i praksa. Sa druge strane i okruženje prijetnji je takođe evoluirao. Kako sajber prijetnje postaju sofisticiranije, organizacije-kompanije moraju biti spremne da u realnom vremenu (*online*) istraže i na brz i efikasan način reaguju i spriječavaju, odnosno rješavaju nastale incidente. Problemi se manifestuju uglavnom u dijelu mreže između servera i uređaja organizacije-kompanije i udaljenog-dislociranog službenika koji koristi računar ili drugu opremu na udaljenoj lokaciji-kod kuće. Ovakvi problemi su doveli i do razvijanja novih tehnoloških rješenja u digitalnoj forenzici, odnosno do nastanka „daljinske digitalne forenzike" a koja podrazumijeva ispitivanje-akviziciju digitalnih uređaja i podataka sa daljine omogućavajući istražiteljima ili drugim ovlaštenim autoritetima da reaguju na svaki vid narušavanja bezbjednosti a da nisu fizički prisutni na samom mjestu događaja. Kako bi se postigao sveobuhvatan uvid i pregled metodologija, alata i najboljih praksi uključenih u sprovođenje digitalnih forenzičkih istraga na daljinu neophodno je usvojiti i određena znanja i vještine za navigaciju-upravljanje ovim složenim procesima, a prije svega prepoznati prijetnje kako bi se uspostavilo otporno bezbjednosno okruženje. Novouspostavljeni sistem daljinske digitalno forenzičke istrage je opstao i nakon završetka pandemije iako se prema istraživanjima sistem rada približno vratio na stari način i nivo rada, ipak je evidentna tendencija rada na daljinu koja je opstala i koja je u odnosu na rad prije pandemije nekoliko puta veća. U kontekstu navedenog i korporativna mrežna struktura se prilagođavala novonastalim uslovima i evoluirala. Nema više potpuno „tvrdih" parametara a zaposleni na radnom mjestu često koriste pametne telefone i uređaje, laptopove i druge urđaje i van mreže i off-VPN. Ovakav pristup je uslovio i novi pristup kompanija-

organizacija u pogledu sajber bezbjednosti i rizika kako unutar tako i izvan perimetara sopstvenih mreža sa imperativom da se svaka prijetnja identifikuje, istražuje i na najbrži i najefikasniji način otkloni bez obzira kad i gdje se pojavi. Glavni rizici za sajber bezbjednost kompanija-organizacija uključuju:

- Malvere i ransomvere,
- Evidencije protokola pristupa i konekcija,
- Malverzacije zaposlenih-insajderski napadi,
- Industrijska špijunaža,
- Vanjske penetracije u mrežu.

Predhodne IKT politike u vidu fizičkih pristupa uređajima u kancelarijama gdje se nalaze ili fizičko dostavljanje uređaja u namjenske prostorije za ažuriranja, zakrpe i popravke, nisu održive u okviru savremenih pristupa u vidu poslovanja putem udaljenih radnih mjesta. Troškovi slanja ili fizičkog dostavljanja uređaja na specijalizovane destinacije za ažuriranje i popravke su uvijek visoki, posebno s obzirom na izgubljenu produktivnost kada se moraju obustaviti poslovi kako bi se sačekale popravke napadnutog ili oštećenog uređaja. Ove politike su se pokazale kao potpuno nepraktične posebno kada se radi o potencijalnoj insajderskoj prijetnji, jer daje insajderu mogućnost „sterilizacije" uređaja, odnosno mogućnost uništavanja određenih ili svih dokaza o upadu-napadu. Način da se spriječi svaki mogući rizik od sajber napada, odnosno da se stanje sajber bezbjednosti kompanije-oragnizacije dovede u nivo „bezbjedno za rad" neophodna je permanentna prostorno-vremenska zaštita svih uređaja i mrežne infrastrukture, kao i razvijanje neophodnog nivoa personalne bezbjednosne svijesti i kulture.

3. GLAVNI IZAZOVI U RADU POLICIJSKIH STRUKTURA NA SPREČAVANJU VISOKOTEHNOLOŠKOG KRIMINALITETA

Statistike trendova pokazuju da je trenutno najveći rizik-rijetnja po bezbjednost svakog društva u cjelini sajber (visokotehnološki-kompjuterski) kriminalitet. Ekspanzija IKT i Umjetna inteligencija (AI) preoblikuju okruženje sajber-cyber bezbjednosti velikom brzinom. Sa druge strane, odbrambeni alati-softveri vođeni Umjetnom inteligencijom pomažu korisnicima (fizičkim i pravnim licima) da otkriju svaku prijetnju brže nego u predhodnom periodu. Međutim, i sajber-cyber kriminalci takođe koriste umjetnu inteligenciju za automatizaciju svojih sofisticiranih napada. Od dubokih zlonamjernih (deepfake phishing) shema prevara do zlonamjernog softvera koji pokreće umjetna inteligencija, jasno je da će strukture za sajber-cyber bezbjednost morati usvojiti i implementirati nove i kompleksne alate poboljšane Umjetnom inteligencijom kako bi u eskalirajućoj situaciji-borbi sa kriminalom i kriminalnim strukturama ostali ispred njih. Nove tehnologije koje se ubrzano razvijaju donose i nove izazove koji zahtijevaju brzo i napredno razmišljanje kao i bezuslovnu saradnju struktura za zaštitu zakona. Razvoj IKT uslovio je i potrebu za snažnim i efikasnim odbrambenim strategijama i sistemima koje pokreće umjetna inteligencija kako bi se suprotstavili novim sajber prijetnjama. Da bi se određena tehnologija kvalifikovala kao bezbjedna po dizajnu, mjere zaštite podataka i bezbjednosti moraju biti integrisane u štićeni sistem od samog početka, a ne kao dodatak ili naknadno razmišljanje o zaštiti. Tehnologije sa ovom sposobnošću daju prioritet vitalnim sigurnosnim karakteristikama kao što su end-to-end enkripcija, kontrola pristupa, mehanizmi provjere autentičnosti i stalna sigurnosna ažuriranja. Ugrađivanjem ovog nivoa sigurnosti u osnovu dizajniranih tehnoloških rješenja, organizacije mogu uspostaviti mnogo jaču i efikasniju osnovu za zaštitu svojih podataka u okviru sigurnosnog okruženja usmjerenog na konkretne podatke. Više razvijena bezbjednosna svijest i sistem zaštite u obradi i

razmjeni podataka među subjektima pooslovne ili bilo koje druge zakonite interakcije (fizičkih i pravnih lica) omogućit će i lakše i efikasnije postupanje policisjkih i drugih bezbjednosnih i pravosudnih struktura u istragama u kojima je došlo do narušavanja bezbjednosti i štete (nekim kriminalnim aktivnostima) po napadnuti subjekt i otkrivanje počinioca ili više počinilaca. U navedenom kontekstu osam najvećih izazova u korištenju mrežnih komunikacija (IKT) sa kojima se suočavaju strukture za zaštitu i sprovođenje zakona i obavještajna zajednica u svom radu mogu se podjeliti u tri oblasti:

A. Oblast: Internet

1. Praćenje i istraga društvenih mreža i medija
2. Prepoznavanje i otkrivanje sajber prijetnji u realnom vremenu (*online*)
3. Crno tržište (Dark Market) i praćenje mogućih zloupotreba kriptovaluta

B. Oblast: Telekomunikacije

1. Zakonito presretanje komunikacija
2. Presretanje i praćenje signala mobilnih telefona
3. Presretanje 5G saobraćaja

4. Oblast: Nadzor i geolociranje

1. Elektronski nadzor
2. Geolociranje i geolokacijske istrage

4.A. OBLAST: INTERNET

4.1.PRAĆENJE I ISTRAGA DRUŠTVENIH MREŽA I MEDIJA

Internet zbog svoje globalne zastupljenosti predstavlja neograničen i neiscrpan izvor informacija, koji sadrži podatke o pojedincima, lokacijama i društvenim mrežama, čineći ga nezamjenjivim za policijeske i obavještajne strukture koje su u neprestanom traženju informacija o osumnjičenima, mogućim teroristima i drugim kriminogenim licima. Navigacija, odnosno pretraga pedstavlja veliki problem upravo zbog neograničenog broja dostupnih informacija koje treba selektovati i staviti u okvire zahtjevanih potreba. Problemi se ogledaju kroz sljedeće parametre:

- Beskonačan broj i izvor podataka.
- Višestruki sistem aplikacija u vidu različitih društvenih mreža.
- Stalno angažovanje resursa i intezivan rad za pretragu i pregled.
- Virtualizacija aplikacija.
- Mogućnost izrade lažnih i zlonamjernih profila.
- Upotreba AI (vještačke inteligencije) za zloupotrebe u kreiranju zlonamjernih aplikacija.
- Jednostavnost pristupa mrežama.
- Mogućnost strateške nazavisnosti.

Informaciono komunilacione tehnologije (IKT) kroz aplikacije otvorenog koda-tipa su značajno evoluirale, omogućavajući brzo i efikasno prikupljanje, sistematizovanje i analizu ogromne količine informacija, ali i pored toga ipak ne pružaju potpuno sveobuhvatna i efikasna rješenja tako da i dalje ostaju određeni izazovi u pogledu potreba krajnjih korisnika (policijskih, obavještajnih, tužilačkih i sudskih struktura) za određenim tipom podataka i informacija koje treba prepoznati, sistematizovati i analizirati iz mase metapodataka. Društvene mreže se kroz nove aplikacije i mogućnosti neprestano poboljšavaju i onemogućavaju jednostavno i brzo

prepoznavanje pravih i lažnih identiteta, što usložnjava i komplikuje upravljanje sigurnim i tajnim virtuelnim operacijama. Teroristi, kriminalci i drugi zlonamjerni subjekti iskorištavaju ove internetske mogućnosti za obavljanje nezakonitih aktivnosti i predstavljaju realnu i moguću prijetnju nacionalnoj i globalnoj bezbjednosti.

Baš kao i glavne platforme društvenih medija, i alternativni sajtovi društvenih medija su evoluirali, privlačeći više kriminalnih aktivnosti i stvarajući nove izazove strukturama za sprovođenje i zaštitu zakona i obaveštajnoj zajednici. Neprekidna evolucija društvenih medija privukla je i ekstremiste (radikalne pojedince i organizacije) stvarajući kontinuirane i stalno promjenljive prijetnje svim vladinim agencijama, organizacijama i privatnim kompanijama. Kako bi se na vrijeme pripremili i zaštitili od svih vrsta prijetnji i ugrožavanja neophodno je pratiti razvoj društvenih platformi mreža i medija kao i mainstream društvenih medija i predvidjeti njihovu evoluciju u kontekstu budućih mogućih prijetnji, kao i rješenje za njihovo sprječavanje i praćenje. Pored navedenog neophodno je identifikovati ekstremističke korisnike i sam sadržaj plasirane dezinformacije.

Pristupiti beskonačnoj količini i vrstama izvora, obraditi beskonačne količine i vrste podataka i sve u jednom sveobuhvatno dizajniranom rješenju (softver) koje podržava projektovani (zahtjevani) ciklus istraživanja i ispunjava sve operativne potrebe u pojednostavljenom upravljanju sigurnim i tajnim virtuelnim operacijama otvorenih izvora, web aplikacija i virtualnih HUMINT[140] rješenja zaista bi predstavljao veliki doprinos u radu svih struktura za sprovođenje i zaštitu zakona i obavještajnoj zajednici. Na tržištu postoje proizvodi koji zadovoljavaju iskazane potrebe samo ih treba prepoznati u kontekstu svojih zahtjeva i potreba.

Neke od smjernica koje treba da ispune izabrana rješenja-alati u pogledu potreba za obradom:

- **Globalni podaci:**
  Sveobuhvatan pregled i analiza svih dostupnih otvorenih izvora u kontekstu mogućih prijetnji i izazova.
- **Ciljani podaci:**
  Analiza i profiliranje u stvarnom vremenu i izdvajanje iz ogromnih izvora podataka ciljanih podataka u pogledu uvida sa minimalnim unosom traženih podataka.
- **Globalni sakupljač (kolektor) podataka:**
  Omogućuje masovno prikupljanje, stalno praćenje i detaljnu analizu bilo koje informacije, teme, događaja, podatka ili predmeta interesa na bilo kojoj platformi otvorenih izvora (otvorenom webu).

[140] U obavještajnim podacima koje prikupljaju vladine agencije, nalazi se i ljudska obavještajna aktivnost (HUMINT), koja se prikuplja iz ljudskih izvora. Kancelarija direktora za nacionalnu bezbjednost SAD (ODNI-Office of the Director of National Intelligence) prepoznaje ljudsku obavještajnu aktivnost kao najstariji način prikupljanja informacija i vitalni je dio obavještajnog ciklusa. Prema Federaciji američkih naučnika, obavještajni ciklus ima pet koraka: 1. Planiranje, 2. Prikupljanje, 3. Obrada, 4. Analiza izvora i izvještaj, 5. Disribucija i razmjena. Prikupljanje obavještajnih informacija putem neposrednih aktivnosti pojedinaca-operativaca odnosi se na drugi korak. Dakle, obavještajne infoirmacije kao rezultat aktivnosti operativca-pojedinca se mogu prikupljati i iz izvora u toku intervjua i/ili ispitivanja nekog lica ili više lica. HUMINT se također može prikupiti putem drugih obavještajnih aktivnosti kao što je tajna operacija ili infiltracija. Discipline unutar zajednice prikupljanja obavještajnih podataka razlikuju se u zavisnosti od sigurnosnih prijetnji, ali podaci prikupljeni obavještajnim radom operativaca koriste se za identifikaciju prijetnji prije napada. Međutim, sirovi podaci se takođe upoređuju i sa drugim informacijama prikupljenim putem drugih operacija prikupljanja i iz više različitih izvora.
Jarrod Sadulski: What is HUMINT and How Is It Used in The Intelligence Field?, American Public University, Digital Learning for Real Life, https://www.apu.apus.edu/area-of-study/intelligence/resources/what-is-humint-and-how-is-it-used-in-the-intelligence-field/ 21.08.2024., 07.45

- **Dark Web (nelegalne internet platforme):**
  Jedinstveni pogled na skrivene i nezakonite (crne-dark) web izvore, mogućnost tajno praćenja-nadgledanja i analizu podataka, kako bi se detektovale-otkrile i spriječile ilegalne aktivnosti i druge zlonamjerne radnje.
- **Avatar alati:**
  Operativni avatari-virtelni alati za borbu-navigaciju sa predhodno definisanim potrebama i ciljevima. Nevidljivo i sigurno end-to-end upravljanje avatarom i operativnim okruženjem.
- **WebCrawler**[141]**-** web meta-vizuelni pretraživači:
  Ovo rješenje predstavlja indeksiranje informacija bez koda koje omogućuje jednostavan pristup i odabir podataka s web stranica, foruma ili mreža i mrežnih sredstava. Alat treba da omogući operateru procjenu autentičnosti naloga, bilo da ga je generisao čovjek ili bot. Alat treba da ima mogućnost brzog pretraživanja baza podataka na osnovu naziva, adrese, telefonskog broja, e-pošte, lozinke kako bi detektovao i izolovao čvorište sa kojeg dolazi do odliva podataka i vizuelno analiziranje za prepoznavanje veza, obrazaca i logovanja. Definisanje popisa za uvid, sa detektorima upozorenja putem ključne riječi, lokacije, entiteta i medija.
- **Uvid u ciljane informacije:**
  Mogućnost selektoanja pristupa informacijama s obzirom na nivo rada i hijerarhije u strukturi i u pogledu predmeta rada.
- **Analitički filteri:**
  Omogućavanje brzog filtriranja visokog nivoa prema sadržaju, medijima, društvenim mrežama, predmetu i cilju.
- **Odliv podataka:**
  Sistem zaštite, detekcije i traženja kritičnih čvorišta za moguće napade i sprečavanje upada za odliv podataka i informacija preko alata za navigaciju-tražilica, automatska dijagnostika sistema sa upozorenjem i blokiranjem odliva.
- **Izvještavanje:**
  Izvještaji treba da budu bazirani na postavljenim filterima, potpuno automatizirani i konfigurabilni za specifične zahtjeve i potrebe korisnika i u formatu prihvatljivom za sud.

4.2. PREPOZNAVANJE I OTKRIVANJE SAJBER PRIJETNJI U REALNOM VREMENU (*ONLINE*)

[141] WebCrawler je pretraživač i jedan od najstarijih preživjelih pretraživača na webu danas. Dugi niz godina je radio kao metapretraživačka mašina . WebCrawler je bio prvi web pretraživač koji je omogućio pretraživanje cijelog teksta. Metapretraživač je online alat za pronalaženje informacija koji koristi podatke web tražilice da bi proizveo vlastite rezultate-tražene informacije**.** Metatražilice na osnovu unosa traženog zahtjeva od korisnika odmah pristupaju traženju informacija koje transformišu u tražene rezultate. Prikupljaju se zahtjevani podaci, sortiraju se, rangiraju i prezentuje korisnicima.

Države, vladine organizacije i agencije za sprovođenje zakona su permanentno potencijalne mete visoke vrijednosti za napredne trajne prijetnje (APT)[142]. Motivi ovih napada variraju od sajber i industrijske špijunaže, terorizma, izazivanja ekonomske štete i uništavanja i zloupotrebe baza podataka. Obično se napadi otkrivaju naknadno, kada je napadač već započeo sa protivzakonitim štetnim radnjama. Ono što je organima za sprovođenje zakona i vladinim agencijama neophodno potrebno jesu obavještajni podaci na osnovu kojih mogu da otkriju prijetnje u toku pripremne faze napada-planiranja ili u toku samog napada, a ne poslije njega. Zbog povećane upotrebe informaciono komunikacnionih tehnologija (IKT) od strane kriminalaca i korištenja pametnih uređaja i telefona, tokom posljednjih nekoliko godina, Internet je preplavljen različitim tekstovima, slikama i video podacima u vezi sa određenim kriminalnim djelatnostima. Ovo je primoralo strukture za sprovođenje i zaštitu zakona da preko svojih pripadnika u fizičkom pogledu provode većinu vremena slušajući, čitajući, gledajući i pregledavajući te podatke sa ciljem pronalaska i najmanjeg dijela relevantne informacije i njeno postavljanje u kontekst razumijevanja kako bi se uklopila u širu sliku i kako bi se omogućila obrada u istražnim i obavještajnim procesima, a imajući u vidu da postoji više od stotinu mogućnosti za svaku prikupljenu informaciju. Ovaj posao je iscrpljujući i predstavlja opterećenje za bezbjednosne strukture jer se radi o ponavljajućim radnjama koje se mogu u potpunosti automatizovati putem određenih alata-softvera koji se nude na tržištu na principu detekcije „ključne riječi, ili više riječi". Automatizacija *online* praćenja sajber prijetnji omogućila bi bezbjednosnim strukturama, analitičarima i istražiteljima da uštede vrijeme, omogućavajući im prebacivanje fokusa na druge poslove koji bi omogućili veću efikasnost u radu.

Neke od smjernica koje treba da ispune izabrana rješenja-alati u pogledu potreba za obradom:

- Integralno istraživanje podataka da bi se došlo do ključnih informacija o eventualnoj prijetnji i napadu,
- Usklađivanje racionalizacije vremena i ljudskih resursa za efikasnu prevenciju i razrješavanje kriminalnih aktivnosti,
- Stvaranje efikasne i sigurne saradnje između struktura za sprovođenje zakona,
- Vizuelizacija informacija sa detaljima koji su važni za istragu,
- Garantovanje interoperabilnosti uz visok nivo bezbjednosti, kontrole i privatnosti,
- Mogućnost otkrivanja i istrage potencijalnih izvršilaca, ciljanih: meta, grupa, tema, ključnih riječi i drugih podataka i informaija o sajber kriminalu ,
- Mogućnost vođenja istrage o sajber kriminalu „odozdo" prema „gore" i „odozgo" prema „dole":
    - Istraga uživo o (BI licu) licu od interesa.
    - Kako pristupiti izvorima sajber kriminala, kao što su forumi o sajber kriminalu, Telegram grupe, botnet tržišta i drugo, bez otkrivanja identiteta i obima.
- Kako da se iskoriste sajber obavještajni podaci i informacije za otkrivanje prijetnji prije nego što potencijalni napadači pokrenu svoje aktivnosti (zlonamerni softver ili neki drugi vid napada),
- Kako prikupiti blagovremene i djelotvorne obavještajne podatke za podršku istragama koordinisanih napada sa posebnim osvrtom na:

[142] APT - Napredna trajna pretnja (Advanced Persistent Threat-APT), je skup skrivenih i trajnih hakerskih procesa, često orkestriranih od strane pojedinaca i uperenih prema određenom entitetu. APT najčešće cilja organizacije i/ili nacije iz poslovnih ili političkih motiva. APT procesi zahtevaju visok nivo prikrivenosti u dužem vremenskom periodu.

- Status reaktivnih sajber sistema,
- Pregled antivirusnih programa i zašto i da li su oni dovoljni,
- Razumijevanje komandnih i kontrolnih servera - zajednički elementi APT napada,
- Pristup, identifikovanje i razumijevanje prijetnji prije nego što se pojave,
- Promjena paradigme sa reaktivnog na proaktivno otkrivanje prijetnji,
- Uspostava sistema odbrane da bi se predvidjeli i spriječili napadi,
- Prikupljanje svih relevantnih dokaza o napadima na vladine i druge institucije,
- Kako verifikovati prikupljene dokaze i
- Zaštitita od APT grupa prije nego što su već u pripremnoj fazi napada.

4.3.Crno tržište (Dark Market) i praćenje mogućih zloupotreba kriptovaluta

Uobičajena je zabluda zloupotrebljivača kriptovalute (kao što je Bitcoin) da aplikacije koje koriste nude potpunu anonimnost za svoje korisnike. Na početku oni su samo pseudonimni, što znači da su anonimni i to samo dok neko ne otkrije ko stvarno stoji iza pseudonima koji koriste. Upravo to i predstavlja problem. Obično istražioci moraju da sačekaju dok vlasnik pseudonimne adrese kriptovalute koja je uključena u transakciju od interesa za istragu stupi u interakciju sa drugim pseudonimnim entitetom, (u cilju razmjene putem aplikacije), prije nego što mogu da otkriju njihove značajne i stvarne identifikacione podatke. Pored navedenog načina postoji i drugi način za deanonimizaciju transakcija. Korisnici kriptovaluta (misli se na zloupotrebljavače) moraju da komuniciraju sa bitkoin mrežom (putem aplikacija), rudarima i drugim klijentima da bi zabilježili i sproveli svoje transakcije. Pri tome stalno ostavljaju mrežne tragove-otiske (digitalni dokazi) i upravo se ta komunikacija može koristiti za otkrivanje stvarnog identiteta lica koje stoji iza transakcija u realnom vremenu.

Neke od smjernica koje treba da ispune izabrana rješenja-alati u pogledu potreba za obradom:

- Tehnike istraživanja zasnovane na mreži koje se mogu koristiti za prepoznavanje-izdvajanje i analizu mrežnih komunikacija između klijenata kriptovaluta, interesno povezanih lica, rudara i drugih komponenti;
- Kako pratiti korisnike kriptovaluta i njihove aktivnosti na slojevima mreže;
- Vrste korišćenih mrežnih, enkripcionih i komunikacionih protokola;
- Geolokacija transakcije - kako povezati izvršenu transakciju kriptovaluta sa IP adresom;
- Kako poboljšati blockchain podatke sa OSINT[143] i HUMINT;

[143] OSINT (Open Source Intelligence-otvoreni obavještajni izvori). Neke od definicija OSINT koje se koriste su: „Informacija s potencijalom mogućeg značaja za obavještajne službe koja je dostupna javnosti", „Informacija koja je pružena od bilo koje osobe ili grupe bez očekivanja da ona ima određenu privatnost, odnosno, informacija koja nije zaštićena od javnog izlaganja". Open source intelligence (OSINT) - je neklasificirana informacija koja je s namjerom otkrivena, diskriminirana i prikazana odabranoj publici kako bi odgovorila na specifična pitanja. Prilikom sistemske primjene, OSINT proizvodi mogu smanjiti zahtjeve prema klasificiranim zbirkama obavještajne službe na način da se ograniče zahtjevi za informacijama samo na ona pitanja na koja se ne može odgovoriti putem otvorenih izvora. Javno dostupne informacije - su informacije objavljene i prikazane za javnu upotrebu, informacija koja je zakonito pregledana od strane običnog promatrača ili je omogućena dostupnost široj javnosti. Informacija koja je učinjena javno dostupnom može doći u bilo kojem formatu. Provjeren OSINT (OSINT-V) - informacija sa visokim stepenom točnosti. To su informacije dobijene od strane obavještajnih profesionalaca sa pristupom provjerenom materijalu ili provjerenim izvorima. OSINT je u praksi korišten od strane velikog broja različitih pojedinaca i organizacija, ali prvi koji je usmjerio pažnju i shvatio njegov značaj je Robert David Steel. On je bivši pripadnik US Marine Corps and Intelligence-

Izvršioci svih vrsta krivičnih djela koriste blokčejn (kriptovalute) kako bi oprali sredstva stečena nezakonitim aktivnostima. Kriminal povezan sa kriptovalutama dostigao je najviši nivo u istoriji 2021. godine sa ilegalnim adresama koje su putem transakcija imale promet od 14 milijardi dolara širom svieta - u odnosu na 7,8 milijardi dolara u 2020. godini. Pored izvršioca krivičnih djela i određene državne i privatne strukture koriste kriptovalute da izbjegnu sankcije, finansiraju terorizam, vrše zlonamjerni uticaj ili nabavljaju nedozvoljene robe i predmete. Međutim, sve aktivnosti koje se obavljaju putem računara i računarskih mreža ostavljaju digitalni potpis-trag u vidu podataka o logovanju (digitalni dokazi) tako da javni blokčejn čuva nepromjenljivu evidenciju transakcija koju strukture za sprovođenje i zaštitu zakona u svojim istragama mogu da prate - samo ih treba znati pročitati na pravi način i uz adekvatne softverske alate kojima bi se moglo pristupiti kriminalnim finansijskim mrežama, pratiti kriminalne aktivnosti i sprovoditi istraga uz mogućnost blokiranja i oduzimanja sredstava uključujući borbu protiv terorizma i kontraobaviještajnih aktivnosti.

Neke od smjernica koje treba da ispune izabrana rješenja-alati u pogledu potreba za obradom:

- Alati za analizu blokčejnova koji imaju mogućnost da povežu transakcije kriptovaluta sa stvarnim entitetima-fizičkim ili pravnim licima.
- Korišćenje naprednih tehnika eksploatacije podataka i praćenja za identifikaciju nezakonitih aktivnosti na blokčejnu.
- Prikupljanje i praćenje dokaza.

Ove transakcije se uglavnom otkrivaju nakon izvršenja, odnosno prekasno u istražnom procesu. Da bi bili korak ispred izvršilaca organizovanog kriminala i maksimalno iskoristili mogućnost blokiranja i oduzimanja nelegalne kripto imovine, strukture za sprovođenje i zaštitu zakona moraju da pojednostave svoj radni-istražni proces i na najbrži način povežu tačke od interesa kada istražuju poznate ili sumljive kriminalne aktivnosti.

a u kojem je proveo 20 godina. Smatraju ga kreatorom i osnivačem OSINT-a (Open Source Intelligence). Steel je 1992. godine objavio članak pod nazivom E3i (Ethics, Ecology, Evolution, and Intelligence). U radu je predstavio tadašnje poglede i stavove prema alternativnim paradigmama nacionalnih obavještajnih službi, one koje naglašavaju dijeljenje-ustupanje informacija i otvorene izvore umjesto tradicionalne jednostrane tajnosti. Između 1993. i 2001. sprovedena su razna ispitivanja i komisije koje su provjeravale stanje američke obavještajne službe i kako one mogu efikasno zaštiti Ameriku od raznih vanjskih ali i unutrašnjih prijetnji. Steel je prisustvovao tim ispitivanjima i uvidio je veliki značaj OSINT-a u svemu tome. Na osnovu provedenog istraživanja između Steel-a i CIA-e i ostalih, još postoji rasprava u krugovima profesionalaca iz obavještajnih službi o važnosti OSINT-a. Generalno se svi slažu kako su otvoreni izvori informacija (iako su ne klasifikovani) korisni i kako treba vršiti njihovo prikupljanje i analiziranje, isto kao i one kod klasifikovanih izvora. Neslaganja nastaju kod relativne važnosti OSINT informacija kada se uporede sa onim tajnim informacijama pribavljenih tajnim metodama. Ono što je sporno jesu vrijeme i resursi koji su uloženi u prikupljanje i analiziranje otvorenih izvora. Smatra se kako postoje 3 pogleda na OSINT i njegovo značenje.

- Prvi pogled podrazumijeva politiku koja preferira stavu da više informacija pružaju tajno prikupljenje informacije u odnosu na OSINT. Troškovi i procesi koji se koriste kod prikupljanja takvih informacija znače i njihovu veću pouzdanost, dok OSINT može poslužiti samo kao potvrda tih informacija. Sa OSINT-om nije moguće ući u „suštinu" promatranog podatka, odnosno događaja.
- Drugi pogled podrazumijeva da bi se OSINT trebao posmatrati ne samo kao dopuna i dodatak klasifikovanim podacima i informacijama, već i kao izvor važećih-postojećih informacija.
- Treći pogled predstavlja kombinaciju prva dva. Treći pogled podrazumijeva veoma bitan značaj OSINT-a, koji ne može pružiti baš sve odgovore, ali može pomoći da se usmjere resursi i sredstva prema onom što bi trebalo pronaći tajnim putem. U navedenom kontekstu možemo reći da se ovdje OSINT smatra prvim filterom za dalje postupanje.

https://security.foi.hr/wiki/index.php/OSINT_-_Open_Source_Intelligence.html, 16.09.2024.(09.40)

Neke od smjernica koje treba da ispune izabrana rješenja-alati u pogledu potreba za obradom:

- Mogućnost da se ispita veze između kriminalnih aktivnosti i van lanca (kriminalne aktivnosti kod kojih zarada nije u početku izvedena u kriptovaluti) i kripto kriminalnih aktivnosti.
- Mogućnost pregleda koraka koji su uključeni u identifikaciju i praćenje nezakonitih sredstava pomoću blockčein analitike.
- Mogućnost za izolovanje i deanonimizaciju transakcija povezanih sa sumljivim aktivnostima i licima.

Konverzije kriptovaluta imaju ključnu ulogu u ekosistemu kriptovaluta jer korisnici uglavnom konvertuju svoja sredstva virtualne valute (kao što su bitkoin, eterijum, NFT, tokeni, itd.) u fiat[144] valutu. Kao takve, konverzije-razmjene pružaju kritičnu vezu-informacije strukturama za zaštitu zakona kako bi mogli izvršiti utvrđivanje stvarnog identiteta entiteta (fizičkog ili pravnog lica) koji stoji iza ideentiteta entiteta koji kontroliše adrese virtuelne valute uključene isključivo u kriminalne aktivnosti (treba razlikovati legalne aktivnosti u konverzijama). Međutim, da bi uspješno pronašli i pribavili ove informacije, pripadnici struktura za sprečavanje i istrage sajber kriminala i finansijski istražitelji moraju da razumiju osnovne istražne tehnike koje uključuju konverziju-razmjenu. Konkretno, oni moraju da znaju koje su informacije dostupne, kada su dostupne, šta da traže, kako da traže, gdje da traže, itd. Pored navedenog kada su u pitanju istrage u vezi sa kriminalnim aktivnostima u pogledu kriptovaluta neophodna je određena saradnja sa operaterima koji obavljaju konverzije-razmjene (Binace-najveća svjetska berza kriptovaluta).
Specifični zahtjevi prema operateru koji obavlja konverziju-razmjenu kriptovaluta uključuju:

- Šta je, odnosno šta nije zabilježeno u blokčejnu?
- Otvoreni kod-pristup (deanonimizacija uz pomoć komercijalnih alata).
- Razumjevanje uloge razmjene kriptovaluta i informacija koje su u vezi s tim dostupne.
- Mjere usklađenosti u Binance-u (saradnja i ustupanje informacija).
- Šta očekivati od Binance-a u pogledu zahtjeva za blokiranje i/ili oduzimanje sredstava?

Istraživanja mračnih tržišta su sama po sebi komplikovana i teška zbog velikog broja kombinacija anonimizirajućih komunikacionih protokola (TOR), enkripcije i neograničenih mogućnosi prikrivanja tragova transakcija kriptovaluta. Ali, korištenjem sofisticirane heuristike (softver, metode, tehnike...) moguće je analizirati aktivnosti mračnog tržišta i povezati kupovine sa blokčejn transakcijama. Upravo iz navedenih razloga neophodno je da istražioci koji rade na ovim istragama budu informisani o aktuelnim tehnikama i opcijama istraživanja za praćenje korisnika mračnih tržišta, a posebno:

- Pregled gradivnih-konstrukcijskih blokova bilo kog mračnog tržišta - TOR, PGP, kriptovaluta;
- Kategorizacija mračnih tržišta prema njihovom poslovnom modelu i koja tržišta dozvoljavaju direktan prenos sredstava kriptovalute između prodavca i kupca;
- Kompleti alata-softvera i hardvera za praćenje i prikupljanje podataka o (meta) korisnicima mračnih tržišta;

[144] Fiat novac je državna valuta koja nije podržana fizičkom robom kao što je zlato ili srebro. Podržava ga vlada koja ga izdaje. Vrijednost fiat novca je izvedena iz odnosa između ponude i potražnje i stabilnosti vlade koja izdaje novac, a ne iz vrijednosti robe koja ga podržava. Većina modernih papirnih valuta su fiat valute, uključujući američki dolar, euro i druge glavne globalne valute. Pojednostavljeno rečeno, fiat novac vrijedi zato što središnja banka i država kažu da vrijedi. Sve današnje svjetske valute spadaju pod fiat novac.

- Tehnike analize i heuristike koje mogu povezati aktivnosti/metapodatke mračnog tržišta u vezi sa oglasima i kupovinama kod kupaca i prodavaca.
- Trenutno stanje dostupnih alata-softvera i hardvera, baza podataka i metodologija, i
- Studije slučaja/primjeri o tome kako su pripadnici struktura za sprovođenje i zaštitu ztakona (LEA) koristile dostupne alate-softvere za procjenu specifičnih mračnih tržišta i razotkrili uključene akter-korisnike.

ZAKLJUČAK

Sa informatičkom globalizacijom došlo je i do evolucije-transformacije postojećih krivičnih djela u pogledu sredstva izvršenja i nastanka novih pojavnih oblika krivičnih djela (visokotehnološki-kompjuterski-sajber (cyber) kriminalitet) koja su rezultat zloupotrebe IKT. Korištenje novih tehnoloških mogućnosti i uvezivanje svih oblika ljudske djelatnosti u zajednički sistem (A. Oblast: Internet) kroz različite informaciono-komunikacione platforme a u cilju olakšavanja rada i komunikacija, stvorillo je i nove pojavne oblike ugrožavanja bezbjednosti (sajber-cyber bezbjednost) kako pojedinca tako i svih oblika kolektiviteta sa jednog mjesta (poznatog ili nepoznatog) prema bilo kojem mjestu ili pojedincu na planeti. Specifičnost krivičnih djela izvršenih putem Interneta u odnosu na do sada poznate i proučene forme krivičnih djela jeste u tome da je za sticanje neophodnih znanja za izvršenje ovih djela potrebno veoma kratko vrijeme, mali ili neznatni materijalni i ljudski potencijali u odnosu na štetu i nastalu protivpravnu korist kao i izostanak fizičkog prisustva na licu mjesta izvršenja samog djela. *(Jovanić, 2024)* Trenutni pokazatelji kretanja trendova kriminaliteta upravo i ukazuju da je najveći rizik po bezbjednost društva na globalnom nivou, sajber (visokotehnološki-kompjuterski) kriminalitet. U skladu sa navedenom konstatacijom fokus struktura za zaštitu zakona (LEA) u bezbjednosnom smislu mora se preusmjeriti na aktivno poboljšavanje sajber otpornosti uspostavom sistema bezbjednosti koji će moći blagovremeno i adekvatno da odgovori na svaki napad (A. Oblast: Internet: Praćenje i istraga društvenih mreža i medija, Prepoznavanje i otkrivanje sajber prijetnji u realnom vremenu (*online*), Crno tržište (Dark Market) i praćenje mogućih zloupotreba kriptovaluta). Najčešći vidovi ugrožavanja ovim novim bezbjednosnim prijetnjama, sajber kriminalitetom, uključuju svako oštećenje i uništavanje podataka; pranje novca; sprječavanje odvijanja proizvodnih ili drugih procesa; ugrožavanje ili smanjenje produktivnosti; krađu intelektualne svojine, ličnih i finansijskih podataka; pronevjeru; prevaru; ometanje normalnog toka poslovanja nakon napada kao i sve druge oblike protivpravnog djelovanja gdje se kao način, sredstvo ili cilj izvršenja koristi kompjuter, kompjuterski sistem, mreža (Internet) ili uređaji vezani za IKT. Kako bi se na vrijeme spriječile ove prijetnje, odnosno kad se dese otkrile i identifikovale putem nastalih tragova i dokaza i identifikovali izvršioci napada, neophodno je sprovođenje forenzičke ili neke druge istrage od strane ovlaštenih i nadležnih struktura uz korištenje adekvatnih alata za istražni proces i obradu.

LITERATURA

[1] Jovanić, V. (2024): *Kriminalistički i krivičnopravni aspekti visokotehnološkog-Sajber (Cyber) kriminaliteta,* Doktorska disertacija, Travnik, 2024.
[2] Lyon, David (2001). *Surveillance Society: Monitoring in Everyday Life*. Philadelphia: Open University Press.
[3] Sadulski, J.: What is HUMINT and How Is It Used in The Intelligence Field?, American Public University Digital Learning for Real Life, https://www.apu.apus.edu/area-of-study/intelligence/resources/what-is-humint-and-how-is-it-used-in-the-intelligence-field/ 21.08.2024., (07.45 h)
[4] Stallman, Richard M. (2013): How Much Survelliance Can Democracy Withstand?, Wired, https://www.wired.com/2013/10/a-necessary-evil-what-it-takes-for-democracy-to-survive-surveillance/, 25.11.2024., (10.52 h)

Internet sajtovi

[1] https://www.techtarget.com/iotagenda/definition/IoT-device, 02.02.2023., (11.52 h)
[2] https://security.foi.hr/wiki/index.php/OSINT_-_Open_Source_Intelligence.html, 16.09.2024., (09.40 h)
[3] https://aws.amazon.com/what-is/api/, 25.11.2024., (12.14 h)
[4] https://www.techtarget.com/searchmobilecomputing/definition/wireless-backhaul, 25.11.2024., (12.22 h)
[5] https://portalcripto.com.br/hr/rje%C4%8Dnik/%C5%A1to-je-web-scraping-kako-funkcionira-definicija-i-koristi/, 04.11.2024., (11.22 h)

Pravni akti

[1] Evropska konvencija o ljudskim pravima, Evropski sud za ljudska prava, Savjet Evrope, Strazbur, strana 10, https://www.ombudsmen.gov.ba/documents/obmudsmen_doc2013041003092706bos.pdf, 26.07.2024., (08.10 h).