# CYBER BEZBJEDNOST- IZAZOVI U RADU STRUKTURA ZA SPROVOĐENJE I ZAŠTITU ZAKONA SA ASPEKTA VISOKOTEHNOLOŠKOG-SAJBER KRIMINALITETA – PREPORUKA ZA PREVAZILAŽENJE PROBLEMA / CYBER SECURITY - CHALLENGES IN THE OPERATION OF LAW ENFORCEMENT AND PROTECTION STRUCTURES FROM THE ASPECT OF HIGH-TECH CYBER CRIMES - RECOMMENDATIONS FOR OVERCOMING THE PROBLEM

Dr 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 004.056.5**

**Sažetak:** *Visokotehnološki-sajber kriminalitet kao novi pojavni oblik kriminaliteta, zbog specifičnog načina ispoljavanja u društveno ekonomskim interakcijama, predstavlja problem strukturama za zaštitu zakona u sprovođenju kriminalističkih i krivičnopravnih aktivnosti i procedura u toku istražnih procesa. Mogućnost i brzina dekriptovanja (enkriptovanih) i obrade prikupljenih i dostupnih podataka u toku istrage može biti presudna na ishod istražnog procesa. Zbog specifičnog načina ispoljavanja u pogledu specifičnosti sredstva izvršenja i posljedice po oštećene subjekte, izvršioci ovih djela često uništavaju ili maskiraju tragove izvršenja kako bi onemogućili ili znatno otežali istragu. Za uspješno suprostavljanje i sprječavanje ove bezbjednosne prijetnje, strukture za zaštitu zakona moraju posjedovati određene resurske kapacitete (ljudske, materijalno-tehničke i infrastrukturne) koji su isti ili na višem nivou u odnosu na počinioce. Sagledavajući navedeno u pogledu brzine, efikasnosti i težine prijetnje, neophodno je u istražni proces uključiti i korišćenje svih dostupnih legalnih resursa u vidu baza podataka, sistema nadzora, evidencija, signalizacije, telekomunikacija, Internet saobraćaj, svih javnih i privatnih subjekata u kontekstu analize podataka iz tih izvora kako bi se došlo do izvršioca ili spriječio napad u fazi planiranja, početka ili u toku trajanja napada. Ovakav pristup zahtijeva uvezivanje navedenih izvora u jedan sveobuhvatan, kompleksan i funkcionalan sistem-platformu za fuziju-spajanje podataka sa mogućnošću veoma brzog pristupa i analize velike količine podataka i informacija u vezi sa metom.*
*JEL klasifikacija K140, K240, K400, K420*

***Ključne riječi:*** *Strukture za zaštitu zakona, dekriptovanje, legalni resursi, fuzija-spajanje podataka.*

***Abstract:*** *High-tech cybercrime as a new emerging form of crime, due to the specific way it manifests itself in socio-economic interactions, represents a problem for law enforcement agencies in the implementation of criminal and criminal law activities and procedures during investigative processes. The possibility and speed of decryption (encrypted) and processing of collected and available data during the investigation can be decisive for the outcome of the investigation process. Due to the specific manner of manifestation in terms of the specificity of the means of execution and the consequences for the injured subjects, the perpetrators of these crimes often destroy or mask the traces of the execution in order to make the investigation impossible or significantly more difficult. To successfully confront and prevent this security threat, law enforcement agencies must have certain resource capacities (human, material-technical and infrastructural) that are the same or at a higher level than the perpetrators. Considering the above in terms of the speed, efficiency and severity of the threat, it is necessary to include in the investigative process the use of all available legal resources in the form of databases, surveillance systems, records, signaling, telecommunications, Internet traffic, all public and private entities in the context of data analysis from of those sources in order to reach the perpetrator or prevent the attack during the planning phase, initiation or during the duration of the attack.*

***Keywords:*** *Law enforcement agencies, decryption, legal resources, data fusion.*

# 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.[159] 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.

[159] 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.ENKRIPCIJA KOMUNIKACIJSKOG SAOBRAĆAJA

Kriminogena lica danas za komunikaciju isključivo koriste OTT[160] aplikacije zasnovane na Internetu. Izazov je, naravno, u tome što ove platforme za razmjenu poruka, audio signala i društvene medije koriste najnoviju, provjerenu i dokazanu tehnologiju šifrovanja što praktično podrazumijeva gotovo nemogućim dešifrovanje ostvarenog mrežnog saobraćaja. Međutim, sa pravim alatima i istražnim tehnikama, strukture za sprovođenje i zaštitu zakona (Law Enforcement Agencies-LEA) i dalje mogu pronaći tragove koji su im potrebni da sprovode istražne procese prema osumnjičenima za krivična djela i mogućnost da prate te tragove dok ne prikupe dovoljno dokaza da identifikuju i uhapse izvršioca ili izvršioce. Strukture za sprovođenje zakona mogu da koriste alate i tehnologiju zasnovane na DPI za legalno presretanje i izolaciju mrežnog saobraćaja zasnovanog na OTT-u i izvođenje metapodataka koji su ključni za njihove istrage.
Neke od smjernica koje treba da ispune izabrana rješenja-alati u pogledu potreba za obradom:

- Kako izdvojiti metapodatke iz šifrovanog saobraćaja?
- Mogućnost forenzike mrežnog saobraćaja da analizira tehnike za utvrđivanje i potvrđivanje osumnjičenih za konkretno djelo.
- Kako generisati VoIP CDR-ove za OTT saobraćaj i korelaciju poziva/komunikacije između osumnjičenih?
- Tehnike za izolovanje naloga društvenih medija na određene uređaje ili korisnike na osnovu forenzičke analize otpremanja signala-podataka.
- Vizuelizacija komunikacione mreže osumnjičenih za razotkrivanje kriminalnih organizacija-struktura ili pronalaženje saučesnika u kriminalnim ili drugim aktivnostima.
- Praćenje osumnjičenih u realnom vremenu tokom operacija i lišenja slobode.

Teroristi, sajber napadači, trgovci ljudima i drugi izvršioci krivičnih djela prelaze sa starih modela telekomunikacionih usluga i uređaja na korišćenje novih IKT i sofisticiranih OTT aplikacija za razmjenu poruka i korištenje softvera za šifrovanje kako bi sakrili svoj identitet, komunikacijske i druge aktivnosti na mreži. Za strukture za sprovođenje zakona, odbranu i obaveštajne agencije ovo predstavlja značajne izazove jer tradicionalni (LI) alati i tehnike za presretanje komunikacija ne mogu da prikupe informacije kroz slojeve šifrovanja i aplikacionih tehnologija koje se koriste u savremenim komunikacionim tokovima kao što su Signal, Telegram i neke druge sajber eksploatacije. Fokus navedenih struktura za zaštitu i sprovođenje zakona treba usmjeriti na mogućnosti upoznavanja i korištenja DPI[161] alata (softvera) za prikriveni i sveobuhvatan izvor i upotrebu komunikacijskog sadržaja sa:

[160] Over-the-top (OTT) je streaming usluga usmjerena direktno na korisnike-gledaoce preko interneta. OTT bypass su kablovske, zemaljske i satelitske televizijske platforme, kompanije koje tradicionalno djeluju kao kontrolor ili distributer takvog sadržaja.

[161] Duboka inspekcija paketa (Deep packet inspection DPI) je vrsta obrade podataka koja detaljno provjerava podatke koji se šalju preko računarske mreže i na osnovu utvrđenih nepravilnosti ili prijetnji mreži može pokrenuti određene protokole-radnje kao što su upozorenje, blokiranje, preusmjeravanje ili evidentiranje prijetnji u skladu sa postavljenim protokolima. Duboka inspekcija paketa se često koristi za osnovnu provjeru-ponašanje aplikacija, analizu korištenja mreže, rješavanje problema s performansama mreže, osiguravanje da su podaci u ispravnom formatu, provjeru zlonamjernog koda ili druge vrste prijetnje, presretanje (prisluškivanje) komunikacija i internet cenzuru, kao i druge aktivnosti koje zahtjevaju visok stepen bezbjednosti. Postoji više zaglavlja za IP pakete. Mrežna oprema treba da koristi samo prvo od njih ( IP zaglavlje ) za normalan rad, ali korištenje drugog zaglavlja (kao što je TCP ili UDP ) se obično smatra površinskim pregledom paketa (obično se naziva inspekcija paketa sa stanjem ). Postoji više načina za preuzimanje paketa za dubinsku inspekciju paketa. Korištenje preslikavanja portova (ponekad nazvanog Span Port )

- Naprednim protokolima za šifrovanje;
- Stalno promenljivim protokolima aplikacija;
- Terabit transportne-gbps pristupne brzine; i
- Kako iskoristiti DPI infrastrukturu za uspješno vođenje operacija i istrage.

Ključni izazovi:

- Enkripcija od kraja do kraja (e2e),
- Aplikacije za razmjenu poruka,
- Obim mreže,
- DPI tehnologija,
- DPI pristupi i tehnike prikupljanja metapodataka i dokaza.

Ključni DPI problemi i izazovi:

- Tipovi saobraćaja,
- Presretanje velike brzine,
- Nove mrežne arhitekture,
- Dekodiranje aplikacija i analiza ponašanja - koje aplikacije koriste, kada i gdje?
- Faktori uspjeha i ograničenja,
- Pretvaranje šifrovanog saobraćaja u praktične uvide,
- Razumjevanje podataka nezavisno od šifrovanja,
- Identifikacija ljudi, objekata, lokacija i događaja iz šifrovanih strimova,
- Izvođenje višeciljne analize u svim šifrovanim aplikacijama
- Sajber bezbjednost vođena DPI,
- Dopuna IDS infrastrukture fidovima zasnovanim na DPI,
- Povezivanje saobraćajnih tokova da bi se identifikovao abnomalni saobraćaj i prijetnje
- Aplikacija za sajber bezbjednost za mreže sa više oblaka i hibridne IT/IoT mreže.

DPI uglavnom koriste zaštitni zidovi (Firewall) koji uključuju funkciju sistema za otkrivanje upada i samostalni IDS koji su namijenjeni otkrivanju napada i zaštiti mreže. Može se koristiti u dobronamjerne svrhe kao alat za mrežnu sigurnost za otkrivanje i presretanje virusa, crva, špijunskog softvera i drugih oblika zlonamjernog saobraćaja i pokušaja upada u mrežu. Ali može se koristiti i za nezakonite aktivnosti, poput presretanja-prisluškivanja i cenzure-zabrane emitovanja određenih sadržaja koju sprovodi država. Duboka inspekcija paketa je takođe korisna za upravljanje mrežom i provođenje politike sadržaja kako bi se zaustavilo curenje podataka i pojednostavio ili modifikovao tok mrežnog saobraćaja prema specifičnim slučajevima upotrebe. Na primjer, poruka označena kao visokoprioritetna može se usmjeriti do svog odredišta ispred manje važnih poruka ili paketa manjeg prioriteta. DPI se također može koristiti za zaustavljanje prenosa podataka kako bi se spriječila peer-to-peer zloupotreba i na taj način poboljšale performanse-mogućnosti mreže. Budući da DPI omogućava identifikaciju autora ili primaoca

je vrlo uobičajen način, kao i fizičko umetanje mrežnog tapa koji duplira i usmjerava tok podataka u alat za analizu na pregled. Duboka inspekcija paketa (i filtriranje) omogućava napredno upravljanje mrežom, korisničku uslugu i sigurnosne funkcije, kao i internetsko rudarenje podataka, prisluškivanje i internet cenzuru. DPI se koristi u širokom spektru aplikacija, na takozvanom nivou „struktura" (korporacije i veće institucije), u pružaocima telekomunikacijskih usluga i u vladama.

sadržaja koji sadrži određene pakete, to je izazvalo zabrinutost među zagovornicima privatnosti i protivnicima neutralnosti i bezbjednosti mreže.

Duboka inspekcija paketa ima tri značajna ograničenja:

1. Može stvoriti nove ranjivosti u mreži, čak i kada pruža zaštitu od postojećih ranjivosti. Iako je efikasan protiv napada prekoračenja bafera, napada uskraćivanja usluge i određenih vrsta zlonamjernog softvera, DPI se također može iskoristiti za olakšavanje napada u istim kategorijama.
2. DPI doprinosi složenosti i glomaznoj prirodi postojećih zaštitnih zidova (Firewall) i drugog softvera koji se odnosi na sigurnost. Da bi ostao optimalno efikasan, DPI zahtijeva periodična ažuriranja i revizije, što može povećati administrativni teret za bezbjednosne timove.
3. DPI može smanjiti brzinu i mogućnosti mreže jer stvara uska grla-mjest u mreži i povećava opterećenje za firewall procesore za dešifriranje podataka i unutrašnju inspekciju.

Uprkos navedenim ograničenjima, mnogi mrežni administratori su prihvatili tehnologiju dubinske inspekcije paketa (DPI) kako bi se uspješno suprostavili povećanju obima, složenosti i učestalosti prijetnji povezanih sa Internetom.

Tehnike dubinske inspekcije paketa:

1. Podudaranje uzorka ili potpisa (IDS). Firewall sa IDS[162] mogućnošću analizira svaki paket u odnosu na bazu podataka poznatih mrežnih napada. Traži određene obrasce za koje se zna da su zlonamjerni i blokira saobraćaj ako pronađe takav obrazac. Nedostatak ovog pristupa je što njegova efikasnost zavisi od redovnog ažuriranja potpisa. Ova metoda radi samo protiv poznatih prijetnji ili napada. Kako se svakodnevno otkrivaju nove prijetnje, stalna ažuriranja potpisa su kritična kako bi se osiguralo da zaštitni zid može otkriti prijetnje i nastaviti štititi mrežu.
2. Anomalija protokola. Metoda anomalije protokola, koju koriste zaštitni zidovi sa IDS nema inherentnu slabost metode podudaranja šablona/potpisa jer jednostavno zaustavlja cjelokupan sadržaj koji se ne podudara sa bazom podataka potpisa. Umjesto toga, slijedi standardni pristup odbijanja. Zaštitni zid određuje koji sadržaj/saobraćaj treba dozvoliti na osnovu definicija protokola. Dakle, za razliku od podudaranja potpisa, ova metoda također štiti mrežu od nepoznatih napada.
3. Sistem za sprječavanje upada (IPS). IPS rješenja mogu blokirati otkrivene napade u realnom vremenu sprječavajući isporuku zlonamjernih paketa na osnovu njihovog sadržaja. Stoga, ako određeni paket predstavlja poznatu bezbjednosnu prijetnju, IPS će proaktivno uskratiti mrežni saobraćaj na osnovu definisanog skupa pravila-protokola. Jedna od mana

[162] Sistemi za otkrivanje upada (Intrusion Detection Systems-IDS) i sistemi za prevenciju upada (Intrusion Prevention Systems- IPS) neprestano nadgledaju mrežu, identifikuju moguće incidente i evidentiraju informacije o njima, zaustavljaju incidente i prijavljuju ih bezbjednosnim administratorima. Pored toga, neke mreže koriste IDS/IPS za identifikaciju problema sa bezbjednosnim politikama i odvraćanje pojedinaca od kršenja bezbjednosnih politika. IDS/IPS su postali neophodan dodatak bezbjednosnoj infrastrukturi većine organizacija, upravo zato što mogu zaustaviti napadače dok prikupljaju informacije o ciljanoj mreži.

IPS je to što se baza podataka o sajber-cyber prijetnjama mora redovno ažurirati informacijama o novim prijetnjama. Rizik od lažnih pozitivnih rezultata je također visok, ali se može ublažiti uspostavljanjem odgovarajućeg osnovnog ponašanja za mrežne komponente, kreiranjem konzervativnih politika i prilagođenih pragova, kao i redovnim pregledom upozorenja i evidentiranih incidenata kako bi se poboljšao nadzor i upozorenje.

U mreži, svaki paket podataka dolazi sa zaglavljem koje pruža osnovne informacije o njegovom pošiljaocu, namjeravanom-krajnjem primaocu i vremenu kada je otpremljen. Konvencionalno filtriranje paketa može samo čitati ove informacije. Ovo je tradicionalni pristup koji koriste stariji zaštitni zidovi budući da nisu bili u stanju da obrađuju druge vrste podataka dovoljno brzo da izbjegnu negativan utjecaj na mogućnosti i karakteristike mreže. Sa dubokom inspekcijom paketa, zaštitni zidovi mogu prevazići te nedostatke za sveobuhvatniju inspekciju paketa u realnom vremenu. Ovo im omogućava da ekstrahuju ili filtriraju informacije izvan zaglavlja paketa za proaktivnije i naprednije praćenje i zaštitu mreže. Unutar okruženja cyber prijetnji koje se stalno širi, DPI je moćan aspekt ekosistema mrežne bezbjednosti. Efikasno istraživanje otvorenog koda na internetu zahtjeva da istražitelji posjeduju specifičan skup vještina kako bi prevazišli ograničenja kao što su izbrisani podaci nakon nezakonitih aktivnosti, skriveno prisustvo i šifrovani-tajni profili na mreži. Pored navedenih vještina neophodno je i poznavanje postupka zakonitog bezbjednog i skrivenog pregledavanja, snimanja i analize ciljanih podataka i informacija na mreži. Ovi procesi moraju ostati potpuno skriveni u odnosu na sve korisnike i u zakonskim okvirima. Uobičajen je stav da je kriptografija teorijski veoma komplikovana i teška za razumevanje, a toliko tehnički uslovljena da se teško može razbiti-dešifrovati bez ogromnog truda i tehničkog znanja koji se mogu naći samo u određenim državnim bezbjednosnim strukturama. Ova konstatacija i stav nisu sasvim utemeljeni i tačni jer postoje mnogi kriptografski problemi sa kojima se istražitelji rutinski susreću u istragama i za koje se sa primjenom sistematske kriptografske analize, mogu da rješe i prevaziđu i uz skroman rad i adekvatne softverske alate. Dakle, pitanje je kako sistematski pristupiti kriptografiji kroz fokusiranje na četiri uobičajena slučaja upotrebe sa kojima se suočavaju istražitelji struktura za zaštitu zakona u svom radu na prikupljanju informacija sa mreža na internetu (teorijska i praktična primjena kriptografije):

1. Kako izvući lozinke iz tragova mrežnih paketa?
2. Kako povratiti izbrisane tajne podatke sa nosača medija?
3. Kako analizirati sigurnost kriptografske aplikacije?
4. Koji su elementi dizajna bezbjednog kriptografskog protokola?

Sveobuhvatan i sistematski pristup u pogledu na probleme u kriptografiji daju dublji uvid u neophodne kriptografske alate za svaki konkretan slučaj-potrebu u vidu oporavak kriptografskih ključeva, otklanjanja nastale štete u pojedinim djelovima koji su predmet napada kao i razvoj perspektiva bezbjednog dizajna i alata koji će olakšati dešifrovanje ciljanih sadržaja. Jedan od efikasnih internet protokola za anonimnost koji se koristi već dugo vremena za hostovanje crnih-mračnih tržišta (ilegalni sajtovi) i skrivanje raznih ilegalnih aktivnosti je Tor[163]. Međutim, postoje

[163] Tor je slobodan softver za omogućavanje anonimne komunikacije. Ime je akronim dobijen iz originalnog imena projekta (engl. *The Onion Router)*. Tor rutira Internet saobraćaj kroz slobodnu, svjetsku (emgl. *world wide),* volontersku mrežu sastavljenu od više od šest hiljada štafeta-posrednika kako bi prikrili korisnikovu lokaciju i upotrebu od strane bilo koga ko nadgleda mrežu, ili vrši kontrolu saobraćaja na mreži. Korišćenje Tora čini mnogo teže određivanje putanje do korisnika koristeći Internet aktivnosti korisnika. Ovo uključuje „posjetu Internet stranicama,

tehnike koje strukture za sprovođenje zakona mogu da koriste kako bi otkrili stvarne identitete pravog korisnika i vlasnika naloga koje uključuju:

- Pregled nezakonitih-kriminalnih aktivnosti zasnovanih na Tor-u (npr. droga, zloupotreba, trgovina ljudima, pranje novca);
- Pravci crnih-mračnih tržišta: novi modeli i kako operateri-kreatori njima stiču protivpranu korist;
- Uputstva o kriptovalutama/plaćanjima;
- Umnožavanje i nastajanje manjih i lokalizovanih tržišta;
- Razumevanje paketa Tor protokola (npr. Tor V3.0), ključnih ažuriranja i pozadine zajednice koja razvija-podržava Tor;
- Profil i sofisticiranost tipičnih operatera i korisnika Tor tržišta;
- Uobičajene tehnike za blokiranje Tor operatera i demaskiranje IP-ova (npr. otisak prsta na sajtu, eksploatacije Tor-a, eksploatacije ranjivosti pretraživača, pronalaženje pogrešnih konfiguracija, navođenje Tor-a da propušta IP-ove i još mnogo toga);
- Tor protivmjere, liste blokiranja i dezinformacije na koje treba obratiti pažnju;
- Najbolje prakse, zamke i „što treba i ne treba" tokom istraga Tor-a;
- Crno tržište i velike zapljene: Šta dalje u pogledu prikupljanja dokaza, demaskiranja korisnika i prikupljanja korisničkih podataka;
- Budući pravac istražnih tehnika, proizvoda i usluga (npr. tehnologije potpomognute veštačkom inteligencijom, automatizacija).

## 2.PLATFORME ZA UVEZIVANJE I PRAĆENJE FUZIJE PODATAKA

Jedan od najvećih problema u radu policijskih i obavještajnih struktura predstavlja analiza prikupljenih podataka i informacija i brzo utvrđivanje činjeničnog stanja u cilju usmjeravanja i vođenja istražnih procesa. Proces identifikacije lica i predmeta i verifikacija-potvrđivanje tačnosti izvršenih provjera u određenim situacijama zahtijeva hitnost u postupanju što sa druge strane predstavlja problem u tehničkom pogledu, jer treba obraditi veliku količinu informacija-metapodataka u kratkom vremenskom roku. Praktično je potrebno izvršiti provjere u različitim bazama podataka, registrima, serverskim-data i provajder centrima, elektronskim nadzororima, senzorskim sistemima, kao i Telekom i Internet provajder operaterima ali i u svim drugim

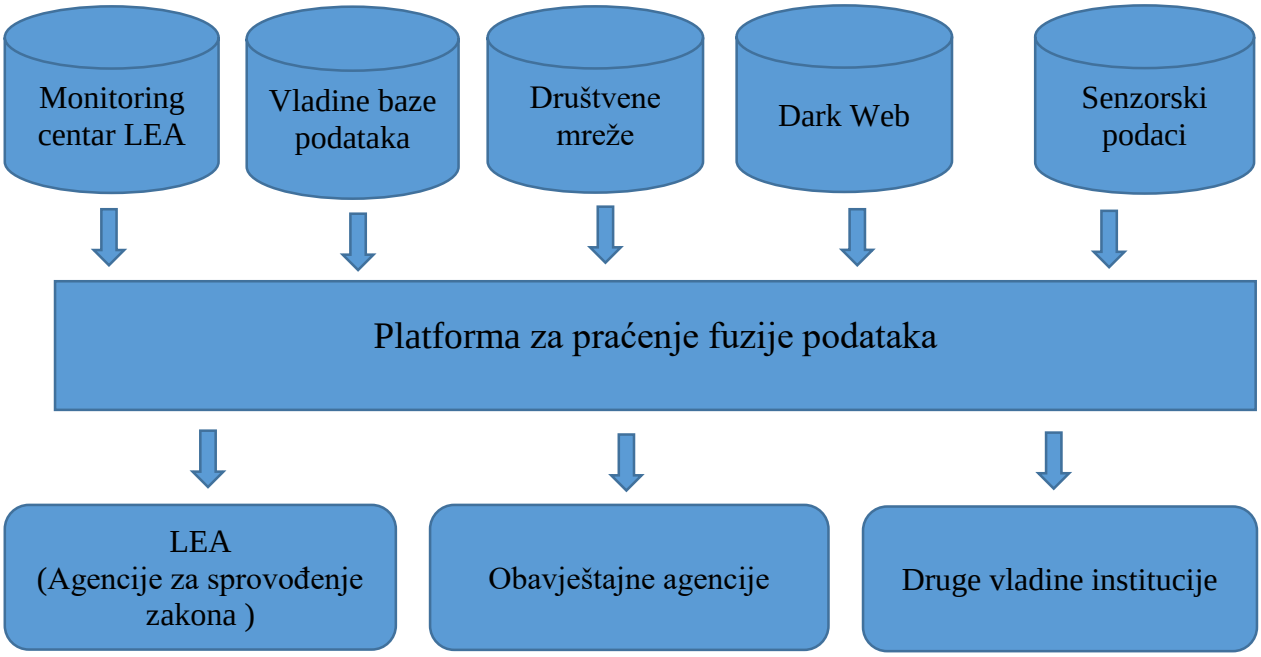
postove na mreži, instant poruke i ostale vidove komunikacije". Tor je namijenjen za zaštitu privatnih podataka korisnika, kao i njihove slobode i mogućnosti da sprovodi povjerljivu komunikaciju držeći njihove Internet aktivnosti izvan mogućnosti da budu praćene. NSA je karakterisao Tor kao „Kralja visoke sigurnosti, niske latentnosti Internet anonimnosti" i da „nema takmičara za tron", i (engl. *POST*) smatra se, sa otprilike 2,5 miliona korisnika dnevno, „daleko najpopularnijim anonimnim internet komunikacionim sistemom". Onion rutiranje je implementirano enkripcijom u aplikacijskom sloju komunikacijonog protokola, ugniježđenog kao sloj luka, korišćeno da anonimira komunikaciju. Tor enkriptuje originalne podatke, uključujući i IP adresu, više puta i šalje kroz virtuelno kolo koje obuhvata uzastopne, slučajno izabrane Tor etape. Svaka etapa dekriptuje sloj enkripcije da bi razotkrila samo sljedeću etapu u kolu u redu i tako ostatak enkriptovanih podataka. Konačna etapa dekriptuje najdublji sloj enkripcije i šalje originalne podatke do destinacije bez otkrivanja, ili čak znanja, izvora IP adrese. Zato što je rutiranje komunikacije djelimično prikriveno na svakom koraku u Tor kolu, ovaj metod eliminiše svaku pojedinačnu tačku gdje komunikacija može biti otkrivena (deanonimizirana) kroz prismotru. Protivnik nije u mogućnosti da porazi jaku anonimnost koju Tor obezbjeđuje. Jedan od načina da ovo bude omogućeno je iskorištavanje ranjivog softvera na klijentovom računaru. NSA ima tehniku koja cilja na zastarele Fajerfoks brauzere pod kodnim imenom (engl. *Egotistical Giraffe*). Napadi protiv Tora su aktivna područja akademskih istraživanja, što je dobro prihvaćeno i od strane samog Tor projekta.

dostupnim otvorenim izvorima informacija (Internet). Ovo je veliki problem jer se prepliću privatna i društvena-državna nadležnost-vlasništvo nad određenim izvorima informacija što dodatno uslovljava problem u radu. U zavisnosti od političke volje i stava nosilaca vlasti u velikoj mjeri će zavisiti i efikasnost struktura za zhaštitu zakona (policijskih i obavještajnih) u otkrivanju, sprječavanju i dokumentovanju izvršrnih krivičnih djela i identifikaciji izvršilaca.

To znači da je neophodno usaglašavanje svih subjekata u sistemu vlasti u pogledu omogućavanja potpune fuzije-spajanja svih izvora podataka i informacija (civilni i svi drugi registri podataka građana, baze podataka, elektronski nadzor, senzorski sistemi...-vladini i privatni), za nesmetan rad struktura za sprovođenje i zaštitu zakona (LEA-Law Enforcement Agencies). Potpuni konsenzus svih subjekata bi omogućio upravljanje zakonito presretnutim metapodacima i sadržajima kroz proces fuzije-spajanja (nova platforma-softversko i hardversko rješenje) sa svim postojećim bazama podataka i evidencijama-registrima bez obzira na titulara. Ovaj pristup podrazumijeva specifične izazove u pogledu više izvora, više formata podataka i njihovo filtriranje kroz novu platformu fuzije-spajanja podataka. Naravno, podrazumijeva se da će u korištenju ovih mogućnosti biti uspostavljena i adekvatna institucionalna kontrola kako bi se spriječile moguće zloupotrebe.

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

1. Prikupljanje i spajanje metapodataka:
- CDR-ovi mobilnog telefona (zapisi podataka o pozivima, eng.: Col Detail Record),
- IPDR-ovi, (zapisi o internet protokol podacima, eng.:Internet Protocol Detail Record)
- SS7 zapisi (sistem signalizacije broj 7, eng.: Signaling Sistem No. 7)....
2. Ekstrahovanje-izdvajanje ciljnih metapodataka:
- Podaci i informacije u oblaku (Claud),
- Web stranice,
- Informacije i podaci telekom operatera (tekst, chat, e-mail, itd.).
3. Presretanje metapodataka:
- Veće brzine prenosa podataka
- Filtriranje metapodataka
- Pohranjivanje metapodataka.
4. Presretanje metapodataka društvenih mreža i medija...




**Šema 2.** Platforma za fuziju-spajanje podataka

Pored navedenih smjernica izabrani alati platforme za fuziju-spajanje podataka (softver i hardver) bi trebali da posjeduju i mogućnosti:

- Video analizu snimljenog materijala iz video nadzora (identifikacija lica i objekata, prepoznavanje ciljanih boja i vozila).
- Prikazivanje podatke sa pametnih kamera u realnom vremenu, mogućnost video reprodukcije i naprednu analizu (biometrijski nadzor za prepoznavanje lica i analizu ljudskog ponašanja).
- Platforma za fuziju-spajanje podataka trebala bi da omogući i prepoznavanje lica upoređivanjem slika koje su preuzete sa interneta, uključujući i slike sa društvenih mreža sa kojih se prikupljaju podaci.
- Mogućnost korištenja slabosti mobilnih sistema u cilju praćenja poziva, poruka i lokacija telefona, bez potrebe hakovanja uređaja.
- Mogućnost za hakovanje računara tako što se meti pošalje video link putem mejla, nakon aktiviranja linka softver se instalira bez znanja mete i prikuplja sve podatke sa uređaja.
- Mogućnost zakonitog presretanja komunikacijskog saobraćaja preko specijalizovanih monitoring centara (telefonskih poziva, SMS poruka i cjelokunog internet saobraćaja), uz mogućnost za efikasnu obradu i analizu velike količine podataka.
- Mogućnost korištenja bezbjednosnih propusta prilikom ažuriranja softvera (na ciljnom uređaju mete) kako bi se „napao" ciljani uređaj. Instalirani softver-program, prikuplja sve podatke, telefonske pozive i prati lokaciju mete i omogućava pristup kameri i mikrofonu.
- Mogućnost softvera da bez bilo kakve interakcije inficira ciljani uređaj ili sistem.

Platforma za fuziju-spajanje podataka treba da implementacijom inovativnih, pametnih informacionih rješenja u skladu sa najmodernijim tehnološkim trendovima omogući efikasno suprostavljanje svim vrstama ugrožavanja, a prije svega prijetnjama i izazovima hibridnog ugrožavanja. Sistem treba da bude sveobuhvatan sa mogućnostima brzog i jednostavnog prilagođavanja potrebama i mogućnostima struktura za zaštitu zakona (LEA) u kontekstu njihovog rasta-širenja uz potpunu bezbjednost i integritet. Uspješno pružanje usluga platforme treba da kroz optimizaciju dostupnosti podataka iz različitih izvora, nadograđujući te podatke kroz analizu, selektuje bitne informacije na osnovu kojih je moguće pokrenuti i voditi aktivnosti za ostvarivanje kritičnih ciljeva i ishoda istražnih procesa. Dakle, platforma za fuziju-spajanje podataka mora omogućiti korištenje i upravljanje masom internih i eksternih složenih podataka koji postoje, osiguravajući tačan, blagovremen i pouzdan prenos-transfer informacija. Neki od problema se odnose na podatke koji su vezani za Dark Web (mračni podaci), odnosno informacije za koje strukture za zaštitu zakona ili na znaju da ih posjeduju ili im ne mogu pristupiti. Takođe jedan od problema je i nesklad između velikih količina složenih podataka (metapodataka) i sposobnosti organizacije za analizu i izdvajanje-izvlačenje vrijednosti iz tih podataka što ponekad rezultira izgubljenom prilikom. Upravo rješenje ovakvih problema predstavlja robusna, jedinstvena, multisenzorna platforma za fuziju-spajanje podataka u realnom vremenu uz omogućnost korištenja složenih podataka-metapodataka sigurno, precizno, podižući sposobnost i efikasnost kako struktura za zaštitu zakona, tako i drugih struktura koje mogu da koriste platformu, u donošenju odluka, upravljanju rizicima, otkrivanju problema i ublažavanju posljedica.

Platforma za fuziju-spajanje podataka podrazumijeva uvezivanje svih segmenata-sistema koji evidentiraju i prikupljaju podatke i informacije unutar kolektiviteta po bilo kojem osnovu:

1. Sistem senzorskog upravljanja i signalizacije:
- Tjelesna kamera (kod pripadnika struktura za zaštitu zakona), LPR, CCTV, Kontrola pristupa, Analiza glasa, Biometrija, Facebook prepoznavanje
2. Sve agencije i strukture koje evidentiraju i kontrolišu podatke i informacije (javne i privatne strukture)
- Granični prelazi, kaznene evidencije, kreditne kartice, baze vlasnika oružja i automobila, letovi.
3. Baze podataka (javne i privatne)
- Spark, Cassandra, PCAP, File, SYNBASE, [Un] Structured, Dokumenti, Couch, Dato, PST, Postgres SQL, Text File, Mango, Plugin, Oracle, Elasticsearch, Neo4, MySQL, Import, SQLite, Cellebrite, Oracle.
4. Otvoreni izvori
- Darknet, Facebook, Forumi, Telegram, Instagram, Deep Web, Twitter, Clearnet...

Platforma za fuziju-spajanje podataka treba da bude softverski i hardverski konmfigurisana tako da obuhvata:

- Platformu Umjetne (Vještačke) inteligencije (AI) i mašinsko učenje kroz analize i vizualno prepoznavanje podataka i informacija u kombinaciji s tehnologijom analize velikih količina podataka,
- Mogućnost ubrzavanja protoka podataka,
- Fuzijski kapacitet (višenamjensko uvezivanje neograničenog broja izvora),

- Mogućnosti konzistentnije, tačnije i korisnije obrađene informacije u odnosu na bilo koji drugi izvor obrade podataka,
- Automatski uvidi na osnovu parametara prioriteta u pretragama:
    - Unificirana pretraga podataka,
    - Unificirano GEO upravljanje,
    - Centralno spojeni podaci,
    - Podaci o terenskim istraživanjima,
    - Istražni procesi i procedure,
    - Eksterni pristup bazama podataka.
- Omogućavanje uvezivanja svih sistema senzora i senzorskog upravljanja, mogućnosti multisenzorne fuzije:
    - Inteligentni senzori i komponente,
    - IP presretanje,
    - GSM presretanje,
    - WIFI presretanje,
    - GEO lokacija (SS7, CDR),
    - IMSI senzori,
    - Sigurnosni senzori,
    - OSINT,
    - CDR monitoring,
    - DarkNet Monitoring,
    - WEBINT,
    - ADINT,
    - Aktivni sistemi.
- Pojednostavljeno pretraživanje po bilo kojem zadanom-ciljnom parametru,
- Mogućnost uvida-pristupa u realnom vremanu. Jedinstven mehanizam pravila bez kodiranja koji omogućava kreiranje korisničkih naloga i skupova pravila za donošenje odluka i modela upravljanja informacijama.
- Mogućnost generisanja mjerača-indikatora rizika - zasnovan na sofisticiranom mehanizmu bodovanja koji je dizajniran za okruženja u stvarnom vremenu
- Prediktivna analiza,
- Mogućnost dvosmjerne softverske kontrole,
- Upravljanje sistemskim entitetima (saobraćaj, rasvjta...), prilagođavanje jedinstvenim potrebama, u različitim sektorima uz osnaživanje digitalne transformacije i potpunu integraciju sa postojećim sistemima (Komponente vanjskih senzora):
    - Baze podataka privatnih agencija,
    - Vladine agencije,
    - Oružane snage,
    - Transportna uprava,
    - Nacionalna ministarstva,
    - Agencije za sprovođenje zakona (LEA).
- Analiza sistema veza,

- Sveobuhvatna anonimizacija izvora mreže, potpuna hardverska segregacija, end-to-end enkripcija,
- Sistem poveznica unutar platforme,
- Sigurnost i integritet.

Ovako zadana i koncipirana Platforma za fuziju-spajanje podataka iz svih izvora trebala bi da omogući određene pozitivne rezultate-korist u vidu rasterećenja u pogledu:

- Eliminisanje potrebe za velikim serverskim sistemima za evidentiranje-pohranjivanje podataka (snimačima podataka).
- Povećavanje operativne efikasnosti uz eliminaciju zastoja u radu.
- Mogućnost korištenja veoma složenih podataka i informacija za efikasno rješavanje problema koji se odnose na naslijeđene izvore podataka i sisteme.
- Mogućnost lakog i jednostavnog prilagođavanje parametrara mehanizma pravila u realnom vremenu kako bi se uskladili s novim protokolima.
- Mogućnost uvezivanja više izvora i struktura za izvještavanje.
- Mogućnost definisanja opcija širenja u skladu s potrebama korisnika.
- Manji urošak vremena na prilagođavanje i pripremu neobrađenih podataka i više vremena na analizu i stvaranje visokovrijednih rezultata.
- Vidljivost podataka u realnom vremenu uz pravovremenu komunikaciju u razmjeni informacija prema korisnicima i olakšavanje donošenja kritičnih odluka i djelovanja.
- Ojačavanje deskriptivne, prediktivne i preskriptivne sposobnosti uz minimiziranje troškova obrade velikih količina podataka i analitike.

Pored koristi za vođenje ciljanih istraga i analizu dostupnih podataka i informacija fuzijska platforma treba da omogući i visok stepen bezbjednosti u radu kroz:

- Zagarantovana povjerljivost, integritet i pristupačnost.
- Pristup zasnovan na nivou, ulozi i dozvolama-logovanje sa automatskim evidencijama i provjerom u vidu verifikovanja traženog pristupa.
- Revizija i kontrola evidencija-upozorenja.
- Bezbjednosna kopija (Backup copy) i oporavak sistema.
- Zaštita sistema od elementarnih ili drugih katastrofa (rezervna serverska stanica).
- Potpuna i sveobuhvatna anonimizacija izvora u mreži.
- Potpuna hardverska segregacija.
- End-to-end šifriranje podataka.
- Bezbjedna komunikacija.
- Centralni sistem za upravljanje evidencijom i upozorenje.

# ZAKLJUČAK

Cilj autora ovog članka je upravo bio da se identifikuju glavni izazovi u radu struktura za zaštitu zakona i na osnovu ličnog i dostupnih iskustava drugih, objasni i predloži najbolji način za prevenciju i suprostavljanje svakom pojedinačnom izazovu konkretizujući zahtjeve u pogledu potreba i mogućnosti koje treba da pruže neophodni forenzički alati (softver i hardver) za sprovođenje istrage i istražnih procesa. Identifikovani izazovi u radu bezbjednosnih struktura za zaštitu zakona su metodološki sistematizovani kroz tri oblasti ugrožavanja: A. Internet, B. Telekomunikacije i C. Nadzor i geolociranje. Svaka od identifikovanih oblasti ima i svoje karakteristično ispoljavanje kroz određene aktivnosti koje su identifikovane kao najopasniji izazovi. Da bi se uspješno suprostavljali navedenim izazovima, neophodno je određeno finansijsko ulaganje i podrška u pogledu opremanja, edukacije i uspostave specijalizovanih organizacionih cjelina unutar struktura za zaštitu zakona kroz definisanje i implementaciju određenih tehnoloških rješenja i projekata. Trenutno se na tržištu putem kompanija za IKT nude djelimična, modularna ili potpuna softversko-hardverska rješenja za prevenciju i sprječavanje navedenih prijetnji-izazova. Izbor adekvatne opreme i projektnog rješenja je veoma bitno pitanje jer treba da uspostavi balans između potreba i mogućnosti kroz analizu trenutnog stanja i vizije u pogledu budućih kretanja i ciljeva. Da bi se ovaj kompromis mogao održati neophodno je u kontinuitetu pratiti trendove kako u pogledu novih pojavnih oblika kriminaliteta i ugrožavanja tako i u pogledu trendova tehničko-tehnoloških rješenja koja se nude na tržištu u vidu softvera i hardvera. Kroz platformu za fuziju-spajanje podataka iz svih dostupnih izvora (javnih i privatnih) ponuđeno je moguće rješenje za efikasno vođenje istražnih procesa kao i mogućnost blagovremenog otkrivanja i sprječavanje određenih bezbjednosnih izazova koji se neprestano u kontinuitetu ispoljavaju u društvu. Procesi kojima bi pripadnici struktura za zaštitu zakona mogli na brz i efikasan način da dođu ili obrade velike količine operativnih saznanja i informacija putem ponuđene platforme koja automatizovano radi, omogućila bi potpuno novi pristup u načinu organizovanja, usmjeravanja i rasporeda raspoloživih resursa (materijalnih, tehničkih i ljudskih) u postupanju u konkretnim situacijama. Novi pristup u planiranju i korištenju raspoloživih resursa svakako bi doveo i do velikih finansijskih ušteda jer bi se vrijeme potrebno za rad na konkretnim predmetima znatno redukovao a ostvarene finansijke uštede bi se mogle preusmjeriti u nabavku adekvatne opreme, edukaciju i razvijanje novih projekata. Praktično to podrazumijeva da pripadnici struktura za zaštitu zakona treba da budu fizički prisutni na svim tehničko-tehnološkim sajmovima i konferencijama na kojima se izlažu i nude određena IKT oprema, rješenja i obuke najpoznatijih kompanija za IKT. Najprestižniji takav događaj u Evropi je svakako ISS World Konference koja se održava svake godine u Pragu i na kojoj svoja rješenja i opremu (softver i hardver) nudi preko 120 različitih kompanija iz preko 100 različitih država svijeta.

# 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 Surveliance 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).