CYBER BEZBJEDNOST- IZAZOVI U RADU STRUKTURA ZA SPROVOĐENJE I ZAŠTITU ZAKONA SA ASPEKTA VISOKOTEHNOLOŠKOG-SAJBER KRIMINALITETA ZA OBLAST: TELEKOMUNIKACIJE / CYBER SECURITY-CHALLENGES IN THE WORK LAW ENFORCEMENT STRUCTURES FROM THE ASPECT OF HIGH- TELECOMMUNICATIONS

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: *Sajber prijetnje (visokotehnološki kiriminalitet-VTK) u našem okruženju su stvarne, a jedini pravi način za uspješno suprostavljanje izazovima je razvoj i implementacija visoko-tehnoloških dostignuća u sistem bezbjednosti i zaštite. Uvažavajući trenutne bezbjednosne izazove sa aspekta trendova u pogledu sajber prijetnji (kriminaliteta) prioritetni zadatak društva u pogledu sistemske bezbjednosti je stvaranje IKT preduslova za efikasan rad struktura za zaštitu zakona. Da bi smo mogli obezbjediti adekvatne preduslove za efikasno otkrivanje i suprostavljanje određenim prijetnjama neophodno je prepoznati svaki vid ugrožavanja kako je navedeno u predhodnom članku u Poglavlju 3. kroz sistematizovanje izazova u radu struktura za zaštitu zakona na sprječavanju VTK u tri oblasti: A. Oblast: Internet (obrađeno u prvom članku), B. Oblast: Telekomunikacije i C. Oblast: Nadzor, geolociranje i enkripcija. Telekomunikacioni sistem je nezaobilazan segment modernog načina komuniciranja u interakciji između subjekata kako unutar jedne društvene zajednice tako i na međunarodnom nivou između pojedinih društvenih zajednica u svim oblastima života i rada. Sa druge strane isti taj sistem je omogućio i određene zloupotrebe od strane kriminogenog dijela društva kako prema pojedincu (fizičko lice) tako i prema kolektivitetu u svim oblicima (pravno lice). U kontekstu navedenog u ovom članku će biti obrađeni izazovi za strukture za zaštitu zakona iz oblasti B.Oblast: Telekomunikacije.*
Ključne riječi: *Sajber prijetnje, izazovi, IKT, telekomunikacije.*
JEL klasifikacija K140, K240, K400, K420

Abstract: *Cyber threats (high-tech criminality-HTC) in our environment are real, and the only real way to successfully confront the challenges is the development and implementation of high-tech achievements in the security and protection system. Taking into account the current security challenges from the aspect of trends in cyber threats (crime), the priority task of society in terms of system security is to create ICT prerequisites for the effective operation of structures for the protection of the law. In order to be able to provide adequate prerequisites for effective detection and countering of certain threats, it is necessary to recognize each type of endangerment as stated in the previous article in Chapter 3 through systematizing the challenges in the work of legal protection structures to prevent HTC in three areas: A. Area: Internet (covered in the first article), B. Area: Telecommunications and C. Area: Surveillance, geolocation and encryption. The telecommunications system is an indispensable segment of the modern way of communicating in the interaction between subjects both within a social community and at the international level between certain social communities in all areas of life and work. On the other hand, the same system also enabled certain abuses by the criminal part of society, both towards the individual (natural person) and towards the collective in all its forms (legal entity). In the context of the above, this article will address the challenges for structures for the protection of laws in the area of B. Area: Telecommunications.*

Keywords: *Cyber threats, challenges, ICT, telecommunications.*

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.[145] 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, geolociranje i enkripcija.

1. B. OBLAST: TELEKOMUNIKACIJE

[145] 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)

1.1. ZAKONITO PRESRETANJE KOMUNIKACJA

Zakonito presretanje komunikacija isključivo se odnosi na legalno odobreno presretanje komunikacija (nadzor) od strane nadležnog suda prema postupajućoj policijskoj strukturi i telekom ili drugom operateru za komunikacije. Potreba da se ostvari uvid u sve vrste komunikacija (telefonske, internet i druge vrste komunikacija u okviru navedenih, aplikacione komunikacije, sms,...) je ključna kada je u pitanju prevencija i sprječavanje kriminalnih aktivnosti za sve agencije-strukture za zaštitu i sprovođenje zakona. Izvršioci krivičnih djela za komunikaciju koriste sva dostupna tehnološka sredstva a svaka komunikacija ostaje ograničen vremenski period zabilježena u uređaju i kod telekom operatera (serveri za pohranu podataka) koji pruža usluge. Od sposobnosti i tehnološkog znanja izvršioca (lice koje sprovodi istragu) zavisit će i režim sprovođenja procesa istrage. U takozvanim standardnim komunikacijam u kojima se koristi klasični telefonski saobraćaj i koji ostavlja vidljive i lako dokumentovane informacije i podatke koji se kod pružaoca usluga i čuva određeni vremenski period, lako se dokumentuju neophodni dokazi. Međutim, u situacijama u kojima izvršioci za komunikaciju koriste neku od aplikacionih platformi za komunikaciju koja koristi internet (viber, WhatsApp, signal, telegram, ili neku platformu za razmjenu fotografija i čatovanje...) konekciju, prikupljanje i dokumentovanje dokaza je mnogo teže, a često i nemoguće bez adekvatnih forenzičkih alata. Korištenje kripto zaštite ili VPN[146] mrežne arhitekture od strane kriminalnih struktura svaku istragu dodatno usložnjava a ponekad i potpuno onemogućava u pogledu pronalaženja i dokumentovanja dokaza. Presretanje bilo koje vrste komunikacija je svakako u istražnom smislu imperativ a od posjedovanja adekvatnih forenzičkih alata zavisiće i mogućnost pronalaženja i dokumentovanje dokaza o krivičnom djelu, aktivnostima i identitetu izvršioca.

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

- Sakupljanje detaljnih zapisa o pozivima (CDR).
- Neprekidnost pretrage sa neograničenim mogućnostima analize podataka, detaljnim upitima i rezultatima kroz naprednu analitiku i sistem kompletnog izvještaja.
- Vođenje istražnih procesa koji su napredni i kojima je moguće ući u trag kriminalnim aktivnostima i otkrivanje virtualnih identiteta.
- Jednostavan multifunkcionalni korisnički interfejs za usmjeravanje toka rada koji je prilagođen potrbama i zahtjevima istrage u svim fazama istrage.
- Geofencing (mogućnost geo lociranja telefona, vozila ili drugog uređaja koji koristi izvršilac-meta).
- Transmission Intercept (presretanje prenosa podataka, video signala...).
- Korisnička identifikacija audio komunikacija.
- Mrežna forenzika.
- Primjena alata na bazi Umjetne inteligencije (AI).

U pogledu planiranja i postavljanja ciljeva u istragama koje koriste mogućnost presretanja komunikacija, neophodno je funkcionalno rasporediti resurse kako bi se olakšala identifikacija izvora i strategija prikupljanja podataka iz svih dostupnih izvora (praćenje i izdvajanje podataka i informacija o zadanoj temi, parametru, događaju ili nekom drugom predmetu interesa u istražnom

[146] Virtuelna privatna mreža (VPN) je mrežna arhitektura za virtuelno proširenje privatne mreže (tj. bilo koje računarske mreže koja nije javni Internet) preko jedne ili više drugih mreža koje su ili nepouzdane (pošto ih ne kontroliše entitet koji želi da implementira VPN) ili ih treba izolovati (na taj način čineći nižu mrežu nevidljivom ili neupotrebljivom).

procesu). Takođe je neophodno metodološki organizovati i provjeriti dobijene podatke kroz kategorizaciju i provjeru kompletne informacije uz osiguravanje tačnosti i relevantnosti. Analiza treba da podrazumijeva ispitivanje i dubinsku provjeru podataka i spajanje u relevantnu informaciju u vidu izvještaja uz mogućnost djeljenja sa zainteresovanim stranama u istrazi u stvarnom vremenu.

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

- Sigurnost logovanja: pristup na osnovu dopuštenja u pogledu ovlaštenja za uvid, potpuna povjerljivost, integritet i dostupnost.
- Mogućnost revizija: Kontrolni zapisnici, logovi i upozorenja.
- Sistem: bezbjednosno kopiranje i mogućnost restitucije.
- Anonimizacija: sveobuhvatan mrežni izvor.
- Hardver: potpuna segregacija (u potpunosti nezavisan i isključen iz sistema drugih uređaja).
- Sistem šifriranja: end to end (od kraja do kraja).
- Mogući napadi i štetne posljedice: sistem oporavka podataka sa centralnim sistemom upravljanja.

1.2. PRESRETANJE I PRAĆENJE SIGNALA MOBILNIH TELEFONA

Podaci o ćelijskoj mreži RF-radiofrekvencijsko skeniranje i snimanje prerdstavlja specijalizovanu djelatnost, a njene tehničke mogućnosti u pogledu određenih podataka i informacija često se koriste tek nakon određenih događaja u krivičnim istragama vezivanjem aktivnosti mobilnog telefona aktera-učesnika (mete) događaja za određenu lokaciju. Kakve informacije (na osnovu obrazloženja-kako, zašto i kada se preduzima RF snimanje i kriterijuma odluke za korištenje RF podataka i informacija) možemo dobiti iz RF podataka, odnosno kako te tehničke podatke i informacije možemo iskoristiti u istrazi korištenih digitalnih medija od strane lica koja su predmet operaivnog interesovanja i istrage:

- Analiza ćelijske lokacije (kretanje i boravak lica na određenim lokacijama-kretanje lica u realnom vremenu-lociranje ili istorija kretanja, pronalazak nestalih lica).
- Format RF podataka ili informacija koji se mogu koristiti u dokaznom pstupku kao zakoniti dokazi pred sudom.

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

- Metodologija RF istraživanja.
- Kriterijumi selekcije RF podataka i informacija.
- Analitika korišćenja ćelijskih podataka (Cell Site).
- Tehnike prikupljanja RF podataka i informacija.
- Korelacija RF podataka i informacija sa drugim izvorima podataka i informacija.
- Kreiranje dokaznih podataka i informacija.
- Mogućnost prenamjene RF podataka.
- Smanjenje kašnjenja podataka i informacija RF saobraćaja.

1.3.PRESRETANJE 5G SAOBRAĆAJA

Sistem 5G mreža je privukao pažnju cijelog svijeta, i trenutno se ulažu ogromni napori telekom operatera i vlada da shvate stvarne implikacije i mogućnosti nove mreže. Postoji velika konfuzija oko toga šta je 5G mreža, kako funkcioniše i kakav uticaj i ograničenja predstavlja za

strukture za zaštitu i sprovođenje zakona. Problem je višestruko uvećan stavom operatera da uvedu potpuno novu generaciju mrežne arhitekture za bežične usluge, i mogućnost da mreža može podržavati više vrsta rezličitih pristupa, kao što su Wi-Fi i satelitska komunikacija. Na navedeno, dodatno opterećenje predstavlja koncept po kojem su 5G mreže virtuelizovane i rade u claud (oblak) okruženjima. Neki su zasnovani na privatnim oblacima (claud) u vlasništvu operatera, dok se drugi obraćaju za usluge oblaka javnih provajdera da bi uspostavili svoju kontrolnu i uslužnu infrastrukturu. 5G usluga se trenutno koristi kao spojnica-premosnica na 4G LTE mreže. Ova takozvana „Non-Stand Alone (NSA) arhitektura" koristi 4G (LI-Lawful Interception) interfejse za zakonito presrtanje komunikacija da ispuni zahtjeve identifikacije lokacije, CDR-a i drugih sadržaja neophodnih za rad struktura za zaštitu i sprovođenje zakona (LEA-Law Enforcement Agency) i drugih vladinih bezbjednosnih agencija. Međutim, upotreba „samostalne 5G mreže" trenutno dolazi na tržište u probnom obliku ili u ranoj fazi implementacije. Ove „greenfield" mreže izazivaju mnogo zabrinutosti i postavljaju mnoga pitanja u vezi sa mogućnostima zakonitog presretanja komunikacija (LI). Nove funkcije zaštite privatnosti koje su uvedene implementacijom 5G mreže pružaju mnoge prednosti u zaštiti komunikacija za krajnje korisnike. Međutim, te mogućnosti visokog stepena zaštite privatnosti imaju sa druge strane ogroman uticaj-poteškoće na istražni rad struktura za sprovođenje i zaštitu zakona, a posebno na upotrebu postojeće IMSI opreme za detekciju i presretanje komunikacija. Praktično, problemi se ogledaju u mogućnostima i uslovima korištenja postojeće IMSI i prateće opreme za presretanje komunikacijskog interfejsa u periodu prelaska mobilnih operatera na novu generaciju mreže (5G SA).

Za uspješno sprovođenje kriminalističkih istraga neophodno je da službenici struktura za zaštitu i sprovođenje zakona budu informisani u pogledu određenih mogućnosti 5G mreže:

- Pregled 4G, 5G NSA i stare IMSI Catcher (hvatač) opreme;
- Osnovna poboljšanja privatnosti 5G dizajnirana da onemoguće IMSI opremu i tehnologiju presretanja komunikacijskih interfejsa;
- IMSI oprema i opcije pasivnog presretanja na implementaciji 5G SA;
- API[147] i informacije potrebne od 5G mreže za korelaciju podataka komunikacijskih interfejsa;
- Informacije o tačnosti presretanja 5G, granularnosti, izazovi i problemi u radu.
- Arhitektura i infrastruktura 5G mreže iz ugla posmatranja struktura za zaštitu i sprovođenje zakona.

[147] Aplikacijsko programski interfejs (eng. Application Programming Interface-API) ili interfejs za programiranje aplikacija predstavlja skup određenih pravila i specifikacija koje programeri koriste tako da se mogu služiti uslugama ili resursima operativnog sistema ili nekog drugog složenog programa kao standardne datoteke rutina (funkcija, procedura, metoda), struktura podataka, objekata i protokola. Na primjer, s programskim jezicima kao Java, C i Python dolazi skup osnovnih aplikacijskih programskih interfejsa dok specifični API-ji dolaze s programskim paketima posebne namjene kao što su Google Maps, MySQL, Facebook Platform. Korištenje API omogućava programerima da koriste rad drugih programera štedeći vrijeme i trud koji je potreban da se napiše neki složeni program, pri čemu svi programeri koriste iste standarde. Napretkom u operativnim sistemima, posebno napretkom u grafičkom korisničkom interfejsu API je nezaobilazan u kreiranju novih aplikacija. Umjesto da se pišu potpuno novi programi i od početka, sa API programeri nastavljaju-nadograđuju svoj rad na radu drugih. API su softverski konstrukcijski blokovi koji omogućavaju međusobnu komunikaciju dvije aplikacije. Kad se koristite aplikacije poput Facebooka, kada šaljemo izravnu poruku ili provjeravamo vrijeme na pametnom telefonu, koristimo API. API se obično sastoji od skupa rutina, protokola i alata koji se koriste u izradi softverskih aplikacija. Ukratko, API određuje kako softver treba integrirati i kako taj softver nakon toga funkcionira zajedno. Uz to, API se koriste kao komponente grafičkog korisničkog sučelja (GUI). Dobri API olakšavaju razvoj programa pružajući gotove konstrukcijske blokove. Programer tada postavlja gradivne blokove i API dograđuje podacima iz programa. Omogućuje programu da prikuplja podatke koje API vraćaju na daljnju obradu. https://aws.amazon.com/what-is/api/ 25.11.2024., (12.14 h)

- Uticaje virtuelizovane 5G mrežne arhitekture na zakonito presretanje (uticaj virtuelizovane 5G infrastrukture (NFV, SDN, cloud, openRAN) na LI).
- Koji se protokoli koriste za podršku glasovnih i tekstualnih usluga u virtuelizovanoj osnovnoj 5G mreži i LI interfejsa (npr. IMS, SIP, Diameter).
- Nove usluge i modeli usluga, uključujući ponude kompanija kroz pristup mreži, podršku za internet pristup i dijagnostika uređaja, tipovi 5G mreža, implikacije na LI itd.

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

- Pregled 4G, 5G NSA i 5G mreža;
- Istorija pristupa 5G metapodacima: Kako upravljati filtriranjem nevažnog saobraćaja od saobraćaja od interesa u slovima veoma velikih brzina prenosa podataka (tbps-Tera Bits Per Second-jedinica za brzinu prenosa podataka) mrežama, interfejsima uređaja i backhaul?[148];
- Edge computing[149]: Šta je edge computing?
- Kako operateri koji nude usluge korištenja oblaka-claud aplikacija (Amazon, MSFT, Google i drugi) sarađuju sa mobilnim operaterima i kako se podaci dobijeni od njih mogu analizirati?
- Koje su opcije presretanja sadržaja za nove 5G računarske arhitekture?
- Šifrovanje: Kako iskoristiti u istragama sadržaje OTT[150] aplikacije za razmjenu poruka, vlasničkih sistemskh protokola, e2e (end to end) enkripciju i P2P[151] (peer-to-peer mreža)?

[148] Bežični backhaul je upotreba bežičnih komunikacionih sistema za transport podataka između interneta i podmreža. Može pomoći organizaciji ili mobilnoj mreži da eliminira potrebu za fizičkim kabliranjem. Umjesto da postoji postrojenje-petlja gdje se sva internet čvorišta povezuju putem žica s internetom, veza se odvija bežično koristeći mikrovalne ili radio valove za prijenos signala između bežičnih pristupnih tačaka. Jedan primjer bežičnog backhaul-a je pametni telefon koji se povezuje na internet primanjem podataka sa mobilnog tornja ili druge vrste bazne stanice. Veza između tornja mobilne telefonije i pametnog telefona je bežični backhaul. Bežični backhaul i backhaul nisu ista stvar. U primjeru s pametnim telefonom, veza se odvija bežičnim putem; tako da je to bežični backhaul. Backhaul je sličan jer povezuje uređaj s internetom, ali koristi žice ili kablove. Na primjer, tablet povezan na Wi-Fi ruter preko Ethernet kabla je primjer backhaul sistema. Ruter se povezuje na Internet pomoću podatkovne linije. Ako se korisnik poveže na LTE (Long Term Evolution) ili 5G mrežu, direktno pristupa internetu koristeći bežičnu backhaul vezu.
https://www.techtarget.com/searchmobilecomputing/definition/wireless-backhaul, 25.11.2024., 12.22

[149] Edge computing je distribuirani računarski model koji približava obradu i skladištenje podataka prema izvorima podataka. U širem smislu, odnosi se na bilo koji dizajn koji omogućava jednostavnu obradu prilagođenu korisniku, kako bi se smanjilo kašnjenje u odnosu na vrijeme kada aplikacija radi na centraliziranom centru podataka. Edge computing uključuje pokretanje kompjuterskih programa koji isporučuju brze odgovore korisniku koji je postavio zahtjev za određene podatke.

[150] Over-the-top (OTT) je striming usluga namijenjena direktno gledaocima-korisnicima putem interneta. OTT zaobilaznice su platforme kablovske, zemaljske i Satelitske televizije, kompanije koje tradicionalno djeluju kao kontrolor ili distributer takvog sadržaja. Takođe je korišćen za opisivanje mobilnog uređaja bez nosača, gdje se sva komunikacija naplaćuje kao podaci, izbjegavajući monopolističku konkurenciju ili aplikacije za telefone koji na ovaj način prenose podatke, uključujući i one koji zamjenjuju druge načine poziva i one koji ažuriraju softver.

[151] Peer to peer (eng: *isti s istim* ili *svaki sa svakim*) u računarstvu podrazumijeva:
- koncept umrežavanja računara bez posrednika, gdje je svaki računar inteligentna radna stanica koja pronalazi druge računare putem *broadcast* ethernet paketa i komunicira s njima direktno, bez potrebe autorizacije na nekom centralnom posredniku-serveru. Primjer takve mreže su Microsoftove radne grupe (*Workgroups*), za razliku od domene (*Domain*) gdje se korisnici moraju prijaviti na centralni posrednik-server domene,
- koncept dijeljenja datoteka između većeg broja računra, za razliku od mrežnog posrednika-servera datoteka (*file servera*) koji koristi protokol za dijeljenje datoteka (NFS, SMB/CIFS i sl.).

- Presretanje sadržaja 5G mreže: Šta predstavlja presretanje sadržaja 5G mreže i kako iskoristiti tu tehnologiju u istragama? Koja je LI tačka presretanja?
- Virtuelne mreže i privatni 5G operateri: mogućnost pristupa podacima putem LI, VoIP-om na virtuelnim uređajima i koje LI (zakonito presretanja) barijere predstavlja i postavlja IETF[152]?
- IMSI Catchers: Kako poboljšanja privatnosti 5G jezgra blokiraju IMSI i tehnologije presretanja komunikacijskog bežičnog interfejsa? Koje su opcije IMSI i pasivnog presretanja u odnosu na implementaciju 5G SA? Koji API-ji i informacije su potrebne od 5G jezgra da bi se uskladili podaci bežičnog interfejsa?
- Koji uređaji „sljedeće generacije" se razvijaju i optimizuju za 5G mreže?
- Šta Google, Apple i Facebook rade na optimizaciji svojih usluga za 5G?

2. C. OBLAST: NADZOR, GEOLOCIRANJE I ENKRIPCIJA

2.1.ELEKTRONSKI NADZOR

Nadzor (elektronski ili bilo koji drugi) predstavlja praćenje ponašanja, različitih interesantnih ili svih aktivnosti ili društveno-socijalnih tokova određenog društva u svrhu prikupljanja informacija, uticaja, upravljanja ili usmjeravanja aktivnosti i društvenih tokova. (*Lyon, 2001*) Ova aktivnost može uključivati posmatranje sa daljine pomoću elektronske opreme (elektronski nadzor), kao što je televizija zatvorenog kruga (CCTV), ili presretanje elektronski prenošenih informacija kao što je Internet ili drugi komunikacijski sadržaj-saobraćaj. Takođe može uključivati jednostavne tehničke metode, kao što su prikupljanje obavještajnih podataka (od strane određenih lica) ili poštansko presretanje pošiljki. Pored navedenih razloga određene društvene zajednice i pojedinci koriste nadzor za zaštitu svojih naselja, lične imovine, proizvodnih ili nekih drugih procesa i aktivnosti. Vlade ga naširoko koriste za prikupljanje obavještajnih podataka, uključujući špijunažu, sprječavanje krivičnih djela, zaštitu bezbjednosnih procesa, lica, grupa ili objekta, ili istragu krivičnih i drugih društveno štetnih aktivnosti. Elektronski nadzor, takođe koriste i kriminalne organizacije i strukture za planiranje i izvršenje krivičnih djela. Strukture za sprovođenje i zaštitu zakona elektronski nadzor koriste za prikupljanje obavještajnih podataka o kriminalcima, njihovim konkurentima, dobavljačima ili kupcima. Neželjeni produkt svakog nadzora je to što može neopravdano narušiti i privatnost građana koji nisu predmet interesovanja u pogledu kriminalnih ili drugih društveno štetnih aktivnosti i često je takva aktivnost predmet kritike aktivista za građanske slobode. (*Stallman, 2013*) Određena društva imaju zakone koji nastoje da ograniče vladinu-režimsku-državnu i privatnu upotrebu svih vrsta nadzora, dok autoritarne i nedemokratske vlade rijetko imaju takve zakone i prihvataju svaku vrstu ograničenja građanskih prava u pogledu nadzora. Špijunaža je po definiciji prikrivena i tipično protivzakonita prema pravilima posmatrane strane, dok je većina vidova nadzora otvorena i državni organi ih smatraju legalnim ili legitimnim. Smatra se da je međunarodna špijunaža uobičajena među svim tipovima zemalja (bez obzira na društveno uređenje). Elektronski nadzor podrazumijeva: video nadzor, audio nadzor, nadzor saobraćaja fotografija, nadzor dronovima i druge vidove nadzora. Video

Peer to peer programi su postali popularni pojavom Napstera i masovnim uvođenjem širokopojasnog interneta. Koncept je ispirirao nove strukture i filozofske pristupe u mnogim područjima ljudske interakcije. Peer-to-peer mreže nisu ograničene na tehnologiju; takođe pokrivaju i društvene procese koji imaju peer-to-peer tip odnosa. U tom smislu, društveni peer-to-peer procesi trenutno rastu na popularnosti.

[152] Internet Engineering Task Force (IETF) je organizacija za standarde za Internet i odgovorna je za tehničke standarde koji čine paket internetskih protokola (TCP/IP). Nema formalni spisak članstva ili uslove i svi njegovi učesnici su volonteri. Njihov rad obično finansiraju poslodavci ili drugi sponzori.

nadzor je sistem koji se sastoji od kamera za video nadzor kao i uređaja (storage-memoriske jedinice, serveri) koji skladište snimljeni materijal sa kamera ili drugih uređaja koji vrše određene aktivnosti u pogledu nadzora. Potreba za ovakvim sistemima je u naglom porastu i očekuje se još veća potražnja zbog Internet of Things (IOT) fenomena, gde će svi uređaji biti spojeni na internet i njima će moći lako da se upravlja. Dakle, video nadzor je sistem koji se sastoji od jedne ili više nadzornih kamera-jedinica koje su povezane sa centralnim uređajem koji vrši obradu dolaznih signala sa tih nadzornih jedinica-kamera. Pregled materijala sa sistema se može vršiti putem Interneta ili smart-pametnih mobilnih telefona i drugih uređaja. U savremeno doba, doba informatike i savremene komunikacione tehnologije, video nadzor je postao normalna pojava na svakom javnom mjestu. Svuda se mogu vidjeti kamere i ponekad, kada se zamislimo, imamo osećaj kao da smo uvijek pod nečijem („budnim okom") nadzorom. U praksi postoji mnogo varijacija na temu video nadzora, jer sistem može biti u sprezi i sa alarmnim sistemom ili posjedovati mikrofone za snimanje zvuka. Uspješno vođenje istraga podrazumijeva da službenici struktura za zaštitu zakona mogu koristiti dostupne informacije video zapisa svih video nadzora koji su relevantni za istragu. Praktično to podrazumijeva saradnju struktura za zaštitu zakona i svih fizičkih i pravnih lica koja posjeduju bilo kakav elektronski nadzor na javnom mjestu ili u objektima koji su u njihovom vlasništvu a kojim je snimljeno izvršenje krivičnog djela ili nekog drugog relevantnog događaja, da ustupe snimljeni materijal postupajućoj strukturi za zaštitu zakona. Informacije koje elektronski nadzor strukturama za zaštitu zakona može da pruži u istragama:

- Mjesto i vrijeme određenog događaja,
- Identitet lica koja su učestvovala u događaju,
- Identitet oštećenih lica i žrtava,
- Aktivnosti lica na mjestu događaja,
- Vozila i registarske oznake vozila i identitet vlasnika,
- Tonski zapisi,
- Potvrđivanje ili odbacivanje alibija,
- Kvalifikacija mogućeg krivičnog djela,
- Verifikacija dokaza za prezentaciju i odbranu na sudu.

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

- Hardverska i softverska rješenja i podrška za istrage,
- Mogućnost korišćenje AI tehnologije sa fokusom na audio i video analizu,
- Potvrđivanje autentičnosti video i audio zapisa,
- Mogućnost analize i selekcije metapodataka i makroblokova, (spaja, analizira i vizualizuje veliki broj različitih skupova podataka u cilju pronalaska relevantnih informacija i obrazaca ponašanja),
- Mogućnosti da se kroz istraživanje baza podataka napravi vizuelni prikaz povezanosti žrtve sa drugim licima, zatim kreiranje mapa i grafikona ali i praćenje online aktivnosti meta,
- Mogućnost prepoznavanja lica, (upoređuje i povezuje prikupljene podatke sa drugim podacima u bazama podataka i na Internetu),
- Prikupljanje i analiziranje podataka sa Interneta i društvenih mreža (u odnosu na video snimak),
- Prepoznavanje glasa,
- Mogućnost da pronađe-prepozna identitet osobe-lica sa slike-video snimka i tačno sa kojim ljudima je ta osoba povezana i kakva je priroda tog odnosa koristeći softvere za prepoznavanje lica i analizu društvenih mreža,

- Mogućnost identifikacije lica-vlasnika vozila na osnovu registarskih oznaka vozila,
- Mogućnost za automatsko izvlačenje podataka sa veb stranica tzv. „veb skrejping"[153]
- Kompatibilnost tehnologija sa kamerama pametnih telefona i aplikacija za strimovanje[154] medija,
- Precizno pozicioniranja lica i predmeta na snimkama u cilju potrebnih analiza,
- Povezivanje informacija iz analiza sa drugim informacijama iz dostupnih baza podataka,
- Povezivanje snimljenog materijala sa jedne lokacije sa snimcima sa drugih lokacija,
- Objedinjavanje i centralizacija informacija dobijenih analizom,
- Izvještaj u formatu prihvatljivom za prezentaciju i odbranu pred sudom,
- Razvoj neophodnih vještina za izvršioce-obuka.

2.2.GEOLOCIRANJE I GEOLOKACIJSKE ISTRAGE

Geolociranje predstavlja utvrđivanje (identifikaciju) gegrafsko-topografske lokacije određenog uređaja (objekta) koji posjeduje softver za geolociranje (GPS), odnosno koji koristi neku od platformi za komunikaciju i razmjenu podataka. Geolokacijska identifikacija putem interneta podrazumijeva prepoznavanje (utvrđivanje) IP adrese, identifikaciju države, grada, odnosno korisnika (fizičko ili pravno lice) kojem je dodjeljena određena IP adresa. Pored navedenog načina identifikacije uređaja (odnosno lica koje posjeduje uređaj), identifikaciju je moguće utvrditi i putem MAC[155] adrese, metapodataka ili biometrijskih informacija o ciljanom licu. Navedeni podaci, sistematizovani u određene baze podataka sadrže i podatke o IP adresama. Ovi podaci mogu da se koriste u automatskim sistemima kod kojih je geolokacija osnovni parametar za identifikaciju (sistemi elektronske pošte, veb stranice, oglasni serveri). Alternativa za identifikaciju poštanskog koda države za ciljanu IP adresu je DNSBL[156] pretraživanje putem

[153] Web scraping je tehnika prikupljanja podataka koja se koristi za izvlačenje informacija s web stranice. To je automatizirani postupak koji uključuje korištenje web skrapera, softvera koji je dizajniran za pristup web stranici, izdvajanje relevantnih informacija i njihovo pohranjivanje u formatu kojem se može lako pristupiti i koristiti. Web scraper može pristupiti web stranici i izvući informacije na mnogo različitih načina. Može pretraživati izvorni kod web-mjesta za određene informacije ili može koristiti tehnike raščlanjivanja za prepoznavanje i izdvajanje informacija iz tablica i drugih podatkovnih elemenata. Nakon što su informacije izdvojene, obično se formatiraju u format koji se može lako čitati i koristiti. To može uključivati pretvaranje informacija u format obrađene-proračunske tablice kao što je Excel ili može uključivati stvaranje tekstualne datoteke koja se može jednostavno uvesti u drugu aplikaciju. Web scraping moćna je tehnika koja se može koristiti za prikupljanje informacija s raznih web stranica. Međutim, važno je napomenuti da zlouporaba web skrapinga može biti nezakonita i može dovesti do pravnih problema. Stoga je važno pažljivo koristiti web scraping i pridržavati se svih primjenjivih zakona i propisa.
https://portalcripto.com.br/hr/rje%C4%8Dnik/%C5%A1to-je-web-scraping-kako-funkcionira-definicija-i-koristi/
04.11.2024. (11.22 h)

[154] Strimovanje (Streaming-engl.) metoda odašiljanja ili primanja podataka (posebno video i audio materijala) preko računarske mreže kao stalan, kontinuirani tok, omogućavajući početak reprodukcije dok se ostali podaci još uvijek primaju.

[155] MAC adresa (Adresa kontrole pristupa medijima) je jedinstveni broj koji se koristi za identifikaciju uređaja/sučelja na lokalnoj LAN mreži. Ovo je adresa sloja veze OSI referentnog modela, predstavljena sa 6 bajtova, obično u heksadecimalnoj notaciji.

[156] Blok lista sistema imena domena, lista crnih rupa zasnovana na sistemu imena domena, crna lista sistema imena domena (DNSBL) ili lista crnih rupa u realnom vremenu (RBL) je usluga za rad servera pošte za obavljanje provjere putem sistema imena domena (DNS) upitati da li je IP adresa hosta koji šalje na crnoj listi za neželjenu e-poštu. Većina softvera mail servera može se konfigurirati da provjerava takve liste, obično odbijajući ili označavajući poruke sa takvih lokacija. DNSBL je softverski mehanizam, a ne specifična lista ili politika. Postoje desetine DNSBL-ova. Oni koriste široku lepezu kriterijuma za uvrštavanje i brisanje adresa. To može uključivati navođenje adresa zombi

udaljenog servera. Preciznost dobijenih informacija varira, ali je moguće na osnovu upoređivanja sa više izvora različitih baza podataka dobiti precizne rezultate. Regionalni internet registri IP adresa predstavljaju primarne izvore u kojima se geolokacijski podaci alociraju i distribuiraju korisnicima koji imaju sjedište na području regionalnog registra. Pored ovog izvora postoje i sekundarni izvori informacija neophodnih za geolociranje:

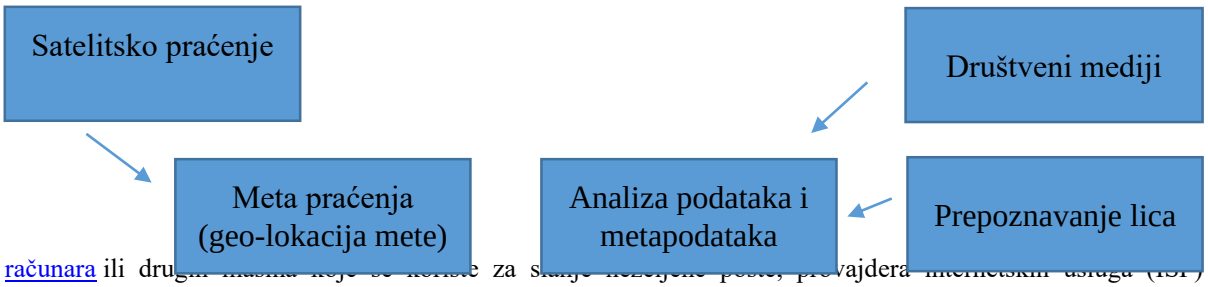
- Analiza dostupnih odataka o uređaju, geolokacijski podaci koje uređaj dostavlja serveru kroz korištenje određenih informacija sa besplatnih komercijalnih aplikacija (korištenje mape, vremenska prognoza, pristup internetu, signalizacija baznih stanica u komunikacionom saobraćaju, provjera i uparivanje IP adrese korisnika sa adresom koja je navedena u njegovom nalogu...),
- Podaci i informacije internet provajdera,
- Inforacija o korištenju baza podataka.

Na preciznost u identifikaciji geolokacije uređaja utiču:

- Analiza i selekcija podataka i otkrivanje anomalija,
- Statistička analiza podataka sa uređaja korisnika,
- Aplikacije za testiranje uređaja.

Korisnicima uređaja koji imaju mogućnost identifikacije geolokacije u određenim situacijama može biti i korisna, a sa druge strane u cilju zaštite privatnosti (ili iz nekog drugog razloga) uređaj omogućava i isključenje opcije identifikacije geolokacije. Pored navedene opcije postoje i druge tehničke mjere koje omogućavaju uslovnu anonimnost. Takve mogućnosti koriste proxy serveri[157] kojima se zaobilaze mogućnosti, odnosno ograničavaju geolokacijski softveri. Određeni veb sajtovi identifikuju korišćenje proksi servera ili anonymizer[158] i imaju mogućnost da blokiraju uslugu, odnosno da obezbjede nelokalizovan sadržaj u odgovoru.

Mogućnosti uvezivanja podataka o geolokaciji meta sa drugim podacima iz različitih izvora za potrebe istrage kroz dostupne opcije geolociranja predstavljena je u Šemi 1.

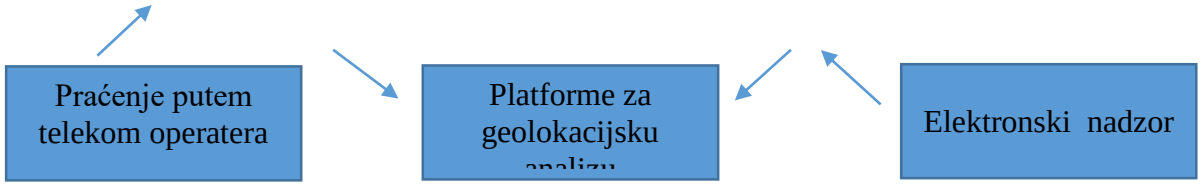


računara ili drugih klasa koje se koriste za slanje neželjene pošte, provajdera internetskih usluga (ISP) koji dobrovoljno ugošćuju spamere ili onih koji su poslali neželjenu poštu na sistem za poštu.

[157] Proxy server je serverska aplikacija koja djeluje kao posrednik između klijenta koji traži resurs i servera koji taj resurs daje. Poboljšava privatnost, sigurnost i moguće performanse u procesu. Otvoreni proxy je proxy server za prosljeđivanje koji je dostupan svakom korisniku Interneta. Na Internetu koriste „stotine hiljada" otvorenih proxy servera:

- Anonimni proxy : otkriva svoj identitet kao proxy server, ali ne otkriva izvornu IP adresu klijenta. Iako se ovaj tip servera može lako otkriti, nekim korisnicima može biti od koristi jer skriva izvornu IP adresu.
- Transparentni proxy: Ovaj server ne samo da se identifikuje kao proxy server, već uz podršku HTTP polja zaglavlja kao što je `X-Forwarded-For`, može se preuzeti i izvorna IP adresa. Glavna prednost korištenja ovog tipa servera je njegova sposobnost keširanja web stranice radi bržeg preuzimanja.

[158] Anonymizer, Inc. je kompanija za zaštitu privatnosti na Internetu. Nudi razne usluge sigurnosti informacija za potrošače, uključujući VPN za višeprotokolni proxy, klijentski softver za iPhone i iPad, proxy server za anonimizaciju, usluge šifrirane e-pošte, anti-špijunski softver, anti-phishing, anti-pharming i konkurentan u poslovnoj klasi obavještajni alati.



Šama 1.: Geolokacijska istraga

Navedena šema oslikava potrebe struktura za zaštitu zakona u vezi sa informacijama koje treba da pruži geolocijsko pozicioniranje mete istrage. Dakle, imamo dvije mogućnosti utvrđivanja tačne geolokacije mete (putem satelitskog praćenja i putem nadležnih telekom operatera) i na osnovu dobijenih podataka možemo izvršiti određene analize kako bismo došli do informacija koje nam mogu pomoći u sprovođenju istrage. Na osnovu geolokacije možemo dobiti i mnoge druge informacije koje nam mogu upotpuniti identitet i kretanje mete (kontakte sa drugima, korištenje određenih uređaja i konekciju na internet, identifikaciju aplikacija i društvenih mreža na kojima je meta boravila).

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

- Korištenje Vještačke inteligencije (AI) za geolokacijsko pozicioniranje i identifikaciju meta, prepoznavanje lica, registarskih oznaka vozila i uvezivanje pribavljenih informacija u sistem-platformu za analizu,
- Uvezanost geolokacije mete sa svim oblicima elektronskog nadzora putem analize podataka,
- Tumačenje geolokacijskih podataka i mogućnost online praćenja,
- Mogućnost korištenja biometrijskih podataka za geolociranje,
- Geolociranje u realnom vremenu i analiza van mreže uz predstavljanje analize položaja meta putem mapa,
- Uvezivanje geolokacije više meta istovremeno,
- Automatsko generisanje i predstavljanje ciljeva u virtuelnom formatu i otkrivanje anomalija.
- Eliminacija rizika u identifikaciji ciljeva-meta,
- Mogućnost automatske podrške u realnom vremenu za donosioce odluka kako bi mogli da odmah identifikuju anomalije u aktivnostima ciljeva-meta i usmjere fokus na sumnjive ciljeve-mete ignorišući ostalo-nepotrebno za obradu,
- Potpuna geolokacijska pokrivenost teritorije nadležnosti za postupanje.

ZAKLJUČAK

U vremensko prostornom okruženju koje karakteriše digitalna i tehnološka dominacija, zaštita građana, društva i društveno ekonomskih odnosa, dostignutog stepena ekonomskog razvoja i fiskalna stabilnost (poreski sistem), su najvažnija i najbitnija pitanja za bezbjednosne i pravosudne strukture u svakom uređenom društvenom sistemu. Podaci i informacije predstavljaju izuzetno vrijedan resurs, a u određenim slučajevima i situacijama, mogu biti i efikasno oružje. Tempo života i biznisa su nametnuli i nove načine komunikacije između subjekata društvene i poslovne interakcije, a sa druge strane je i dio društva koji se bavi nezakonitim djelovanjem (kriminalnom aktivnossću) dobio mogućnost da na brz i efikasan način razmjeni informacije od značaja za svoje

aktivnosti putem nekog od ponuđenih sistema komunikacije (mobilni, satelitski, kablovski sistem). Mogućnost praćenja komunikacija online ili naknadno preslušavanjem evidentiranih komunikacija (obrađeno u B. Oblast: Telekomunikacije: Zakonito presretanje komunikacija, Presretanje i praćenje signala mobilnih telefona, Presretanje 5G saobraćaja) predstavlja trajni izvor informacija i podatak o ostvarenom komunikacijskom saobraćaju između ciljanih subjekata (ovdje se isključivo misli na kriminogena lica i njihove kriminalne aktivnosti) koji se mogu koristiti u istražnom procesu za otkrivanje, dokumentovanje i u dokaznom postupku (u zakonski prihvatljivom formatu) prezentovati pred nadležnim sudom. Budući da sajber prijetnje u kontinuitetu evoluiraju u pogledu ugrožavanja i pojedinaca-građana (fizička lica) i „najsigurnijih" struktura (pravnih lica), bez obzira na stav ili nivo uspostavljene lične ili sistemske zaštite, svi moraju biti svjesni važnosti ulaganja u informaciono komunikacione tehnologije (softverski i hardverski alati) koje su neophodne bezbjednosnim strukturama kako bi mogle efikasno da se suprostavljaju kako novim, tako i svim drugim bezbjednosnim ugrožavanjima i izazovima.

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).