



Nemzeti Közszerológati Egyetem
Hadtudományi és Honvédtisztképző Kar
Intézményi Tudományos Diákköri Konferencia

A nyílt forrású információszerzés katonai aspektusai

Készítette: Vattai Eszter hallgató zászlós

Intézmény: Nemzeti Közszerológati Egyetem

Kar: Hadtudományi és Honvédtisztképző Kar

Szakirány: Katonai üzemeltetés, Híradó specializáció

Konzulens neve, beosztása: Dr. Tóth András őrnagy, egyetemi docens

Neptun kód: SF66RC

2022.

Tartalom

I.	Bevezetés	2
1)	Téma aktualitása.....	2
2)	Tudományos probléma megfogalmazása	2
3)	Kutatási célkitűzések.....	3
4)	Hipotézisek.....	3
5)	Kutatási módszertan	4
II.	Téma kifejtése	4
1)	A nyílt forrású információszerezésről részletesen	4
1.1	A nyílt forrású információszerezés fogalma, adatok típusai, a keletkezésükkel való összefüggések	4
1.2	Előnyök és hátrányok.....	8
1.3	Keresőmotorok, internetes weboldalak.....	8
1.4	OSINT eszközök, azoknak funkciói, rendeltetése	14
2)	A kibertér és a nyílt forrású információszerezés kapcsolata.....	17
2.1	Az etikus hackelés.....	17
2.2	Közösségi média szerepe a nyílt forrású információszerezésben.....	19
2.3	A nyílt forrású információszerezés szerepe a kibertámadásokban	21
2.4	Geolokációs információgyűjtés	23
3)	A nyílt forrású információszerezés kapcsolata a hadsereggel	27
3.1	Az OSINT szerepe a nemzetbiztonsági szervezeteknél.....	27
3.2	Az orosz-ukrán háború OSINT vonatkozásai	30
3.3	A katonai felsővezetőkkel végzett interjúk összefoglalója.....	33
3.4	A kérdőíves felmérés kiértékelése, elemzése.....	36
III.	Összegzés.....	44
IV.	Felhasznált irodalmak, folyóiratok	46

I. Bevezetés¹

1) Téma aktualitása

Az infokommunikációs technológiák és az azokkal szoros kapcsolatban lévő közösségi média platformok napjaink egyik leggyorsabban változó és fejlődő területei. A kérdéskör mentén egyik oldalról a nemzetközi, a másik oldalról a hazai fejlesztéseket venném alapul, ezen belül is az egyes hadseregekben alkalmazott technikai és technológiai megoldásokat, mivel magam is híradó katona vagyok.

Mindezek mellett az infokommunikációs technológiák és a biztonság összefüggéseit kívánom bemutatni, hiszen amellett, hogy a korszerű eszközök számos módon jobbá teszik életünket, számos veszélyt is hordozhatnak.

Fő témám pedig a nyílt forrású információszerzésre (továbbiakban: OSINT) szegeződik, amellyel szorosan összefügg az előbb említett témakör. A jelenben, ha egy képet megosztunk, ha egy posztot kiírunk, vagy elfogadjuk azokat a bizonyos „cookie” beállításokat, minden mozdulatunk és érdeklődési körünk lekövethető. A technológia fejlődése megteremtette azt a különleges helyzetet, hogy a felelőtlen, nem biztonságtudatos felhasználók nagyon könnyen lekövethetővé és lehallgathatóvá váltak.

2) Tudományos probléma megfogalmazása

A katonai műveletek egyik alapjellemezője, hogy azt az a fél nyeri, aki több releváns információval rendelkezik. Ezeknek az információknak az összegyűjtése komoly kihívást jelent a parancsnokoknak, így a területet folyamatosan fejlesztik és egyre hatékonyabb módszereket igyekeznek kidolgozni. Ezeknek a fejlesztéseknek az egyik eredménye a nyílt forrású információszerzés, amely számos olyan információhoz juttathatja a parancsnokokat és törzseket, amelyek támogathatják a döntéshozatali folyamatokat és az információs fölény megszerzését.

Azonban komoly problémát jelentenek azok az esetek, amikor a saját katonáink osztanak meg a saját szervezetükkel, csapataikkal, felszereléseikkel vagy csapatmozgásaikkal kapcsolatos információkat, mivel ezeket az ellenséges OSINT tevékenységet végző csoportok könnyedén megszerezhetik és elemezhetik.

Nem szabad azonban figyelmen kívül hagyni a dezinformáció, illetve az álhírek területét sem, amelyek alapvető célja a megtévesztés. Ennek megfelelően kiemelt figyelmet kell fordítani az

¹ A dolgozat az Innovációs és Technológiai Minisztérium ÚNKP-22-1-I-NKE-34 kódszámú Új Nemzeti Kiválósági Programjának szakmai támogatásával készült

OSINT tevékenységek során a megszerzett információk hitelességének vizsgálatára, valamint a több forrásból történő megerősítésre.

3) Kutatási célkitűzések

Kutatásom célja, az OSINT eszközök és az infokommunikációs technológiák komplex vizsgálata katonai aspektusokban. Jelenleg csak nagyon szűk körben vizsgált terület hazánkban a nyílt forrású információszerzés, ennek megfelelően ez ösztönzött arra, hogy ezzel a területtel foglalkozzak. Az előzetes elemzéseim alapján (jellemzően nemzetközi szakirodalmak vizsgálatával) arra a következtetésre jutottam, hogy az OSINT tevékenységeknek egyre nagyobb hatása lesz a katonai műveletekre, így kiemelten fontosnak tartom egy ilyen irányú kutató-elemző munka végrehajtását. Remélem, hogy a munkám több emberhez elér majd, és betekintést nyerhetnek a nyílt forrású információszerzés katonai lehetőségeibe.

4) Hipotézisek

A kutatásom kezdetén a következő kutatási kérdéseket fogalmaztam meg:

- Milyen új megoldásokat és kihívásokat jelent a katonai műveletekben a nyílt forrású információszerzés szélesebb körben történő elterjedése?
- Melyek azok az OSINT alkalmazások és szolgáltatások, amelyek segíthetik a parancsnokokat a döntéshozatali folyamatok során?
- Rendelkeznek-e azokkal az alapvető biztonságtudatos kompetenciákkal a magyar hivatásos és szerződéses katonák, amelyekkel csökkenthetik digitális lábnyomukat?

Ezek alapján a következő hipotéziseket fogalmaztam meg:

1. Véleményem szerint a nyílt forrású információszerzés felgyorsíthatja a műveleti információk gyűjtését, amely gyorsíthatja a döntéshozatali folyamatokat, valamint az információs fölény megszerzését.
2. Az orosz-ukrán konfliktusban megjelent OSINT technikák nagymértékben támogatják a szembenálló feleket az ellenséges csapatok helyének, mozgásának azonosításában.
3. Véleményem szerint a katonák jellemzően nem rendelkeznek megfelelő biztonságtudatossággal, nem ismerik azokat a megoldásokat, amelyekkel megelőzhetik, hogy illetéktelenek hozzáférjenek az adataikhoz.

5) Kutatási módszertan

A releváns hazai és nemzetközi szakirodalmak elemzését követően a következő kutatási módszereket szeretném alkalmazni:

- Kérdőíves felmérés a közösségi média használat és digitális higiénia kérdéskörökben a magyar szerződéses és hivatásos katonák körében;
- Interjú készítése a Magyar Honvédség felsővezetésében dolgozó szakemberekkel, a nyílt forrású információszerzés hatásairól napjaink műveleti környezetére;
- Technikai elemzés végrehajtása OSINT eszközök alkalmazásával.

II. Téma kifejtése

1) A nyílt forrású információszerzésről részletesen

A dolgozatom kifejtésének első szakaszaként fontosnak tartom ismertetni a nyílt forrású információszerzés fogalmát, előnyei és hátrányait egyaránt. Továbbá melyek azok a keresőmotorok, weboldalak és eszközök, amelyek segíthetnek az információszerzésben.

1.1 A nyílt forrású információszerzés fogalma, adatok típusai, a keletkezésükkel való összefüggések

Fogalommeghatározás

A nyílt forrású információszerzés, vagyis az Open Source Intelligence, rövidítve OSINT, egyre több területen jelenik meg ebben a rövidített formában, ennek megfelelően én is jellemzően ezt fogom használni jelen tanulmányban. Az OSINT célja alapvetően, hogy a felhasználó információigényeire minél pontosabb, teljesebb, hitelesebb választ tudjon adni, illetve a felhasználó szándékának megfelelő információt biztosítson. A nyílt forrású információszerzés a hírszerzési elemzők és a vállalati biztonsági elemzők által felhasznált információk nagy részét biztosítja a lehetséges rejtett kockázatok azonosításához vagy a stratégiai döntések időben történő meghozatalához. Az üzleti szférában, az újságíróknál és a pénzügyi intézeteknél is egyre inkább elterjedt. A kutatásomban viszont a legnagyobb hangsúlyt az állami és a kormányzati rendszerek OSINT technikai fogják kitenni. Kitérek továbbá a katonai műveletekre is, ahol előszeretettel használják csapatmozgások, vagy például nukleáris tárolók felderítésére műholdas térképek segítségével.

Milyen típusú adatokkal tudunk dolgozni?

- Open-Source Data (OSD): olyan adatok, amelyek még nem kerültek feldolgozásra. 'Nyers' adatoknak hívjuk őket, ezeket bárki szabadon felhasználhatja vagy terjesztheti,

szerzői jogok feltüntetésével. Ide tartozhatnak fényképek, magnófelvételek, műhold képek, online bejegyzések stb.

- Open-Source Information (OSIF): Az alábbiak nyilvánosan elérhető információk, amelyek külön engedély nélkül gyűjthetők és tárolhatóak. Általában négy kategóriába soroljuk: széles körben elérhető adatok és információk; célzott kereskedelmi adatok; szakértők és megfigyelők írásai; és a szürke irodalom², amely a magánszektor, a kormány és az akadémia által készített írásos információkból áll, amelyek korlátozottan hozzáférhetők, vagy azért, mert kevés példány készül, az anyag létezése nagyrészt ismeretlen, vagy az információkhoz való hozzáférés korlátozott. Ilyenek például a könyvek, újságok és híradások.
- Validated Open-Source Intelligence (OSINT-V): olyan információ, amelynek hitelessége megkérdőjelezhetetlen. Ez két kategóriára osztható fel: vagy amikor az információ megbízható forrásból kerül ki, vagy ha más médiumokból alátámasztható az információ hitelessége. Ennél az adatnál, főképp figyelni kell arra, hogy ne legyen hamisított vagy manipulatív célzatú. Ezek általában híradások, vagy felsőbb vezetők beszédei.

Ehhez kapcsolódóan szeretném letisztázni az adat és az információ közötti különbségeket. Először is az adatok a tények gyűjteménye; az információ pedig kontextusba helyezi azokat a tényeket, tehát a rendszerezetlen adattömegből egy rendszerezett információ fog létrejönni. Ezt megelőzően elemzést kell végrehajtani, hogy egy területet tudjunk feltérképezni. Az adatok pedig nem függenek információtól, viszont az információ az adatoktól függ.

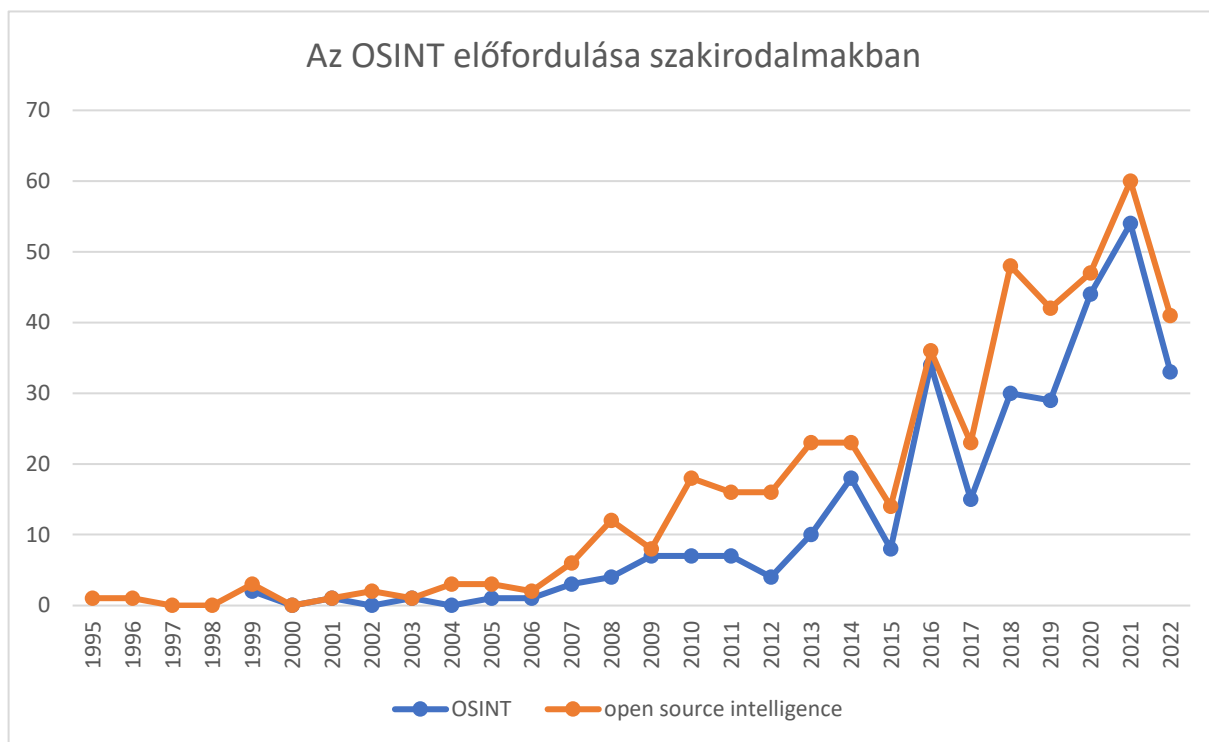
Keletkezése

Az OSINT nem jöhetett volna létre a közösségi média nélkül. A "közösségi média" kifejezést először 1994-ben használták egy tokiói online médiakörnyezetre, a Matisse-ra. Idővel, mind a közösségi média platformok száma, mind pedig az aktív felhasználók száma is jelentősen megnőtt, így a 21. században a közösségi média az internet egyik legelterjedtebb és legjelentősebb jelenségévé vált.³ Ez pedig teljesen átformálta jelen korunk hírszerzését is. A közösségi média mellett számos más nyílt forrás is rendelkezésre áll. Az interneten keresztül elérhetőek a rádió- és tv adások, visszakövethetők a publikációk, az újságok. Keresni lehet képekre, videókra, dokumentumokra, webkamerákat lehet nézni. Interneten a különböző

² A műfaj, téma és az információ hordozótól függetlenül azt jellemzi, hogy nehezen hozzáférhető és kívül marad a kereskedelmi kiadási-terjesztési hálózaton..

³ T. Aichner és mtsai., „Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019”, *Cyberpsychology, Behavior, and Social Networking* 24, sz. 4 (2021): 215–22, <https://doi.org/10.1089/cyber.2020.0134>.

geolokációs adatokat is le lehet kérdezni. Számos olyan adatbázis áll rendelkezésre, melyből következtetni lehet, hogy mi fog történni, abból, hogy milyen információk gyűltek össze. (megnézni a forrást) A tengeri és légi közlekedést is folyamatosan radarozzák egyes adatbázisok.

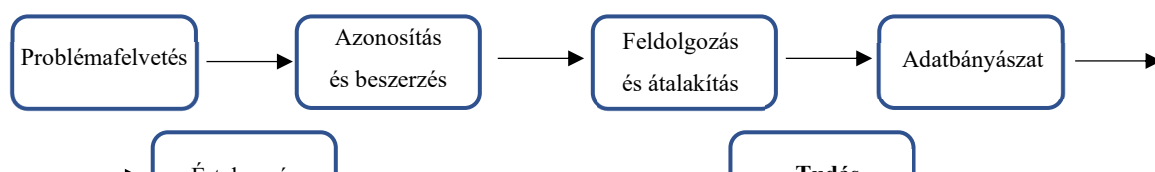


1. ábra: Scopus adatbázisban fellelhető irodalmak számtani listázása (saját szerkesztés)

Az 1. számú ábra is jól szemlélteti, hogy az nyílt forrásokból történő hírszerzés berobbanása a 2010-es években történik meg igazán, és ezután csak növekvő tendenciát mutat. Ez annak is köszönhető, hogy a különböző technológiák, lásd: mobiltelefonok, számítógépek, tabletek stb., olyan szintre fejlődtek, hogy mindent mindennel összeköttetésbe tudtak hozni. Napjainkban például egy jobb minőségű fénykép küldése is maximum másodperceket vesz igénybe, nem úgy, mint a 2000-es évek elején. Mind a két kulcsszónál látszik az egyezés, és hogy szorosan követik egymást az évek alatt. (kifejteni)

OSINT folyamata

Egy folyamatábrával szemléltetve a 2. számú ábrán bemutatom, hogy hogyan épül fel egy adat feldolgozása, analizálása és hogyan lesz ez egy kész információ, avagy a tudásunk alapja.



2. ábra Az adatok feldolgozásának lépései (saját szerkesztés)

1. Problémafelvetés; fontos meghatározni, hogy pontosan mit is akarunk keresni, vagy mi az a dolog, ami alapján elemezzük az adott témát.
2. Azonosítás és beszerzés; a problémánk meghatározása után, különböző keresőmotorok, alkalmazások és eszközök segítségével tudjuk megkeresni az elemezni kívánt adatainkat.
3. Feldolgozás és átalakítás; harmadik lépésként következik az információ nyers változata, melyben összeállítjuk a képet a kutatásaink segítségével.
4. Adatbányászat; ebben a fázisban kiegészítő információkat kereshetünk még a probléma megoldására.
5. Értelmezés; a véglegesen összegyűjtött információk esetleges csoportosítása és befogadása.
6. Tudás; 'végtermékként' megkaphatjuk a teljeskörű tudást az elemzett területről, egy bizonyos szintig.

A folyamatot pedig kiegészítve ismertetek pár példát az analízis eszközeiről;

- Létesítmények modellezése; ez a módszer tökéletes arra, ha bármely épület közelebről szeretnénk vizsgálni, felmérni a paramétereit, milyen környéken helyezkedik el, 3D-s modellek alapján. Erre a legjobb eszköz a Google Earth applikáció.
- Létesítmények kialakításának logikai összefüggésének a vizsgálata; szintén fontos terület, ha kritikus területeket érint az elemzett terület. Ilyenkor, ha tudjuk akkor megtehetjük a cég részletes adatainak a vizsgálatát, vagy szintén vizsgálhatjuk az adott épület környezetét és a város infrastruktúrális képességeit, továbbá érdemes vizsgálni a helyi médiumokban is.
- Hotspot-ok, vagy a területi változások elemzése; ezt általában a háborús övezetekben szokták használni, amikor a térbeli jelenségek elváltozását akarják lekövetni. Példa erre, ha rakétasilókat, új bekötőutakat építenek vagy a bombázások utáni érintett területet térképezik fel.
- Kapcsolatháló-elemzés; Magyarországon ugyan gyerekcipőben jár, de annál hasznosabb elemzési mód, ahol gráfok segítségével vizualizálják a kapcsolatok összefüggését.

1.2 Előnyök és hátrányok

Az OSINT használatának számos előnye van, azonban vannak bizonyos korlátai és gyengeségei is, amelyeket érdemes figyelembe venni.

Előnyök

Az OSINT használatának egyik legnagyobb előnye annak a költsége, hiszen az OSINT sokkal olcsóbb a hagyományos információgyűjtő eszközökhöz képest. Az OSINT potenciálisan nagyobb befektetési megtérülést kínál, és ez a funkció különösen fontos a szűkös intelligens költségvetéssel rendelkező szervezetek számára.

A költséghatékonyság mellett az OSINT számos előnnyel rendelkezik az információk elérésében és megosztásában.

Az információ legálisan és könnyen megosztható bárkivel, a nyílt forráskódok mindig elérhetőek és folyamatosan frissülnek bármilyen témában.

Végül, de nem utolsósorban, a nyilvános forrásokból gyűjtött információk nagyszerű forrást jelentenek például a nemzetbiztonsági hírszerzéshez, ugyanakkor az OSINT nem zárja ki a titkosított forrásokból gyűjtött hírszerzés lehetőségét sem.

Hátrányok

Az OSINT egyik legnagyobb problémája a lehetséges információ-túlterhelés, az értékes OSINT eszközök nélkül a megfelelő információk megtalálása és keresése időigényes tevékenység lehet.

Továbbá nagy mennyiségű elemző munkát igényel az embertől, hogy megkülönböztesse az érvényes, ellenőrzött információkat a hamis, félrevezető vagy egyszerűen pontatlan hírektől és adatoktól, tehát az OSINT-ot legtöbb esetben körültekintően ellenőrizni kell.

Ahhoz, hogy a legtöbbet hozzuk ki az OSINT-ből, részletes elemzésre és a használat követelményeinek megértésére van szükség. ⁴

1.3 Keresőmotorok, internetes weboldalak

Ebben az alfejezetben a mindennapi életben és a katonai műveletekben alkalmazható OSINT megoldásokat ismertetem kezdve véleményem szerint a legpopulárisabbaktól.

Google

A Google Search messze a legtöbbet használt keresőmotor az interneten. A teljes piac 92%-át birtokolják, napi 3,5 milliárd keresést lebonyolítva.

⁴ <https://www.expert.ai/blog/advantages-disadvantages-open-source-intelligence/>; letöltve: 2022. 10. 13.

A működésének az alapja rengeteg különböző oldal felkeresése, ezek indexálása és rangsorolása. A folyamatos oldalkeresést nevezzük „web crawling”-nak, ilyenkor a Google automatizált szoftverek segítségével keres fel általa ismert és ismeretlen oldalakat, és ezeket hosszú listában tárolja el későbbre. A Google által eddig ismeretlen oldalak megismerése érdekében a már ismert oldalakon található kívülre mutató linkek útján térképezik fel a teljes internetet.

Ezeket a felkutatott oldalakat indexálják, vagyis megismerik az oldal tartalmát, elemezve az ott található szöveges, képi és videóanyagokat. Ebből az információból tevődik össze a Google által használt „PageRank” amely minden egyes kereséshez hozzápárosítja a lehető legpontosabb találatokat. Ezen találatok fizetés útján nem változnak, tehát nem lehet magasabb találati helyet vásárolni, leszámítva az elhelyezett reklámokat. Azonban a felhasználóról elérhető információk alapján minden keresési eredmény más és más. Befolyásolja a felhasználó lokációja, nyelve, az eszköz, amit használ, korábbi keresései és a Google által rólunk eltárolt információk.

Egész könyveket írtak arról, hogy kifejezetten a Google keresőjét hogyan lehet tökéletesen kihasználni, de ezek többsége a betörési tesztekhez és hálózatzbiztonsághoz nyújt segítséget. Vagyis hogyan lehet a Google-n megtalálni olyan weblapokat és webalkalmazásokat, amelyek a célponthoz köthetőek és amiken keresztül a célpont támadható. Ezek a „Google Fu” -ként és „Google Hacking”-ként ismert területek azonban a legtöbb OSINT műveleten messze túlmutatnak, amennyiben a célunk egy személyről elérhető nyilvános információk gyors felkutatása.

A Google legnagyobb előnye a kifinomultabb rendszerekkel szemben, hogy használata közben nem lehet eltörni semmit, a rajta való keresés nem jár semmilyen jogi következménnyel, így a tanulási és gyakorlási folyamat is éles adatokkal, valódi feladatokkal történhet.

A Google lehetőséget biztosít célzottan különböző weblapokon történő keresésre, a találatokat továbbá lehet korlátozni fájlformátum alapján, vagy éppen egy célzott oldalhoz köthető további oldalakra is kereshetünk a „related” paranccsal. A Google az általános kereső mellett létrehozta a Programmable Search Engine-t. Itt bárki létrehozhat a Google alapjain működő saját keresőmotort, amin általunk megadott oldalakon, szabadon választható feltételekkel kereshetünk. Teljesértékű OSINT eszközt hozhatunk létre egy megfelelően kalibrált, általunk létrehozott keresőrendszerrel.

Alerts

Az általánosabb, folyamatos és hosszútávú információgyűjtéshez és megfigyeléshez nagyon hasznos a Google Alerts szolgáltatása, ami lehetőséget ad bizonyos témakörök figyelemmel

követésére az interneten. Az általunk megadott gyakorisággal értesítést és összefoglalót kapunk a Google által az utóbbi időben talált oldalakról, amelyek relevánsak számunkra.

Előnye, hogy ingyenes, könnyen használható, tudja kezelni a magyar nyelvet és miután egyszer elindul, ha megfelelően van kalibrálva folyamatosan értékes információt tud biztosítani a felhasználó számára az általa figyelt területről.

DuckDuckGo

A DuckDuckGo egy egyszerű kereső, alapvető funkciója ugyan az, mint a Google-nek. Egyetlen jelentős különbség, hogy a DuckDuckGo nem tárol személyes adatokat, semmit nem ment el a kereséseinkből és mivel nem szeretné tudni, hogy épp ki használja a találatokat sem teszi személyessé. Érdekes ugyanakkor megjegyezni, hogy a TOR böngésző is ezzel a keresőmotorral dolgozik.

Amennyiben az információgyűjtésnek feltétele az objektivitás, egy kiváló opció ennek a keresőnek a használata.

Bing

A Microsoft keresője a Bing, amelyet 2009 óta a Yahoo is használ. Emiatt, ha gyűjtésünkhöz használtuk a Bing-et a Yahoo már redundáns.

A funkciók hasonlóak, mint a Google esetében, keresésünket különböző operátorok használatával szűkíthetjük weblapokra, időpontokra, fájl típusokra stb. Azonban a Bing sajátosság, hogy a LinkFromDomain parancs segítségével a Bing össze tudja gyűjteni az összes linket, amelyet egy weboldalon találunk, sokkal gyorsabban, mint azt kézzel lehetne.

A Google filetype operátora az adott oldalon található Powerpoint prezentációkat, Excel táblákat vagy épp PDF kiterjesztésű dokumentumokat gyűjti össze, azonban gyakran ezeket a célzott oldalakat nem a saját szerverükön tárolják, csak linkkel mutatnak rá. Erre megoldás a Bing Contains operátora, amely az oldalon található általunk megadott kiterjesztésű fájlok összegyűjtése mellett azokat is listázza, amelyre az általunk vizsgált oldal mutat, de más lapon vannak tárolva.

Images

A Google és a Bing is tud képekre keresni az interneten. Ezek a keresések azonban messze nem olyan kifinomultak, mint a szövegre való keresés, hiszen az alapvető működés itt is nagyon hasonló: azokat a képeket kapjuk meg találatként, amelyek körül, vagy a file nevében megjelenik az általunk keresett szöveg. A képkeresésnél a Google által biztosított leghasznosabb funkció a fordított keresés, amikor egy általunk feltöltött képre keres rá, összeszedi azokat az oldalakat, ahol az a kép megtalálható és gyűjt általa hasonlóknak gondolt képeket.

A Bing nagyobb erőfeszítést tesz azért, hogy kitalálja mi lehet az általunk feltöltött képen. Az esetek nagyrésztében, ha személyről töltött képet töltünk fel megpróbálja, hogy ki látható rajta. A képkeresés esetében pedig olyan beállítással is kereshetünk, hogy személyeknek csak az arca, vagy csak a feje és a válla legyen a képen. A fordított keresés tekintetében a Bing gyakran jobban teljesít, mint a Google.

Ilyen fordított keresést a TinEye nevű webalkalmazással is lehet csinálni, elmondásuk alapján közel 40 milliárd kép között keresik azt, amit mi feltöltöttünk és hasznos információt tudnak adni arról, hogy hol és mikor jelent meg az a kép az interneten.

A Bing és Google kizárólag akkor domináns, amikor Észak-Amerikához vagy az Európai Unió területéhez köthető témakörben próbálunk keresni az interneten. A keleti világról sokkal többet és pontosabban találhatunk a helyi oldalakon, mint a kínai Baidu, vagy az orosz Yandex és FindFace.

Ezekén kívül rengeteg szolgáltatás épült a képek felismerésére, mint például a kifejezetten lopott médiatartalmak felkutatására specializálódó Berify és Image Raider, a Microsoft arcfelismerő mesterséges intelligenciája a Microsoft Azure Facial Recognition, vagy a Wolfram projekt Image Identification projektje, amely szintén értelmezni hivatott a feltöltött képet és arról minél több információt összegyűjteni.

Nemzetközi keresőmotorok

A képkeresésnél már felmerült az a probléma az OSINT műveletek esetén, hogy a leggyakrabban használt keresők kifejezetten előnyben részesítik a nyugati világ által létrehozott információforrásokat.

Emiatt, főleg Magyarországtól keletre javasolt a kereséshez orosz, kínai és egyéb ázsiai keresők használata. Az orosz Yandex-nek van elérhető angol nyelvű változata, ami a Yandex.com címen érhető el, a kínai Baidu-nak ezzel szemben nincsen, bár ettől függetlenül még kivitelezhető a használata a nyelv ismerete nélkül is.

A találatok az esetek nagyrésztében hasonlóak lesznek, mint a Google-nél, de amennyiben a teljeskörű feltérképezés a cél, úgy megéri vetni egy pillantást ezekre az oldalakra is. A Yandex rendelkezik pár különleges funkcióval is, amelyek nagyon hasonlóak a Google operátoraihoz. Az egyik ilyen az ismeretlen szóra való keresés, amelyet keresésünkben egy csillag karakterrel tudunk jelölni. Amennyiben rákeresünk az "Open Source **", akkor az OSINT-on kívül sok találatot kapunk nyíltan hozzáférhető szoftverekről és ezek fejlesztéséről. Ez a módszer hasznos lehet emberek teljes nevének felkeresésére.

Több száz nemzetközi keresőoldal van, amelyek általában akkor hasznosak, amikor a keresésünk egy bizonyos országra korlátozódik, és abban az esetben a Google mellett az adott ország vagy nyelvi kultúrkör saját keresőjét is célszerű megnézni.

I Search From

Google keresések manipulációjához könnyen lehet VPN-t használni, amely elrejtí a személyazonosságunkat és átvisz minket egy másik ország területére virtuálisan, hogy a keresésünket onnan tudjuk elvégezni és az adott ország lokális találatait kapjuk meg. VPN szoftver nélkül ezt az isearchfrom.com oldalon keresztül is el lehet végezni.

Itt alapvetően három beállítást kell kiválasztanunk keresésünk előtt: honnan keresünk, milyen nyelven és milyen eszközről. Ez az oldal kifejezetten hasznos weblapok optimalizálásához, ennek segítségével az üzemeltető megnézheti, hogyha valaki arabul keres Izlandról egy Android táblagépen, akkor a Google felajánlja-e neki az ő oldalát.

Ezekon kívül lehet további korlátozásokat is megadni, mint például, hogy csak a célzott nyelven, vagy csak a beállított országból kapjunk találatokat, de lehet a városra is pontosítani. OSINT műveletek esetében ez akkor hasznos, amikor egy bizonyos témáról több nézőpontot is meg akarunk vizsgálni, vagy a műveletet végző kíváncsi rá, hogy adott országokban a mit látnak a megbízójáról.

Web archivum

Minden keresőmotor elsősorban friss információt akar biztosítani a számunkra és ezt minél gyorsabban. Emiatt folyamatosan térképezik fel az internetet és az általuk talált oldalak tömegéről úgynevezett cache verziót tárolnak el. Ennek következtében gyakran a keresők segítségével olyan információkat is meg tudunk találni, amelyek az élő oldalon már nem elérhetőek. Ezek az elmentett oldalak általában maximum pár naposak, feltéve, ha frissül a cím. Amennyiben elérhetetlenné válik az oldal pontos kereséssel továbbra is megtalálható a keresők által elmentett verzió. Az időtartamnak pontos határa nincs, de szerencsés esetben akár évekig is fennmaradnak így oldalak.

Amennyiben így akarunk keresni a Google esetében a célzott oldal elé a cache: operátort kell beírni, így a Google elénk tárja az általa elmentett összes lapot az adott címről. A legfrissebb verziók általában a Google-n és Bing-en találhatóak meg, a korábban már ismertetett Yandex és Baidu sokkal régebbi cache-elt verziókkal dolgozik.

Ennél is régebbi, akár több éves verziókat az archive.org által üzemeltetett The Wayback Machine segítségével tudunk fellelni. Ennek a szolgáltatásnak konkrét célja, hogy több éves, vagy akár évtizedes információ is elérhető maradjon. Az általunk keresett címet átfuttatva a The

Wayback Machine keresőjén megkapjuk az összes mentett verziót, amelyek közül időrendben kiválaszthatjuk azt amelyik minket érdekel.

2016 óta a Wayback Machine rendelkezik kulcsszavas kereső funkcióval is. A web.archive.org/web/*/kulcsszó oldal az általunk keresett kulcsszót a teljes adatbázisukon végig futtatja, tehát az összes elmentett oldalon. Azonban a gyakorlatban ez, főleg magyar témakörökben nagyon akadozva működik, a találatok az esetek többségében nem relevánsak a kereső számára. Viszont így találhatunk olyan oldalakat is, amelyek kifejezetten megtiltották az archiválást egy szerver oldali beállítással, magára az oldal címére keresve nem is lehet fellelni őket, viszont kulcsszavas kereséssel elérhetőek.

TOR

A The Onion Router, vagyis TOR egy ingyenesen elérhető internetes böngésző, amely anonimizált kommunikációt tesz lehetővé az interneten keresztül. Az internetes kommunikációt egy önkéntes alapon működő hálózaton futtatja végig és a többrétegű titkosításnak hála rejti el teljesen.

Ezen a hálózaton a szokásos internetes oldalakat is el tudjuk érni, azonban a működési elvből kifolyólag nagyon lassan. Ami OSINT szempontból érdekes, hogy vannak olyan weboldalak és szolgáltatások, amelyek kizárólag a TOR hálózaton keresztül érhetőek el. Sajnos elsősorban ezeken az oldalakon illegális tevékenység folyik, gyakori a drogkereskedelem és a gyermekpornográfia viszont az OSINT művelettől függően itt is rengeteg információra találhatunk. A legfőbb nehézség azonban abból ered, hogy az oldalak nagyon nehezen fellelhetőek.

Ezt kezelendő hoztak létre keresőket és linkgyűjteményeket, amelyek kifejezetten a TOR-ra vannak specializálva. Az ezekkel való keresés felhasználói élménye természetesen messze elmarad a korábban megismert keresőektől.

Az első ilyen az Ahmia.fi, amely egy nagyon erős TOR kereső. Természetesen semelyik motor nem tudja megtalálni és indexálni az összes oldalt, mégis ezen találjuk a legtöbbet. Minden TOR-os OSINT műveletet itt célszerű kezdeni. Az alkalmazás működik tradicionális böngészőből, de az oldalak megnyitásához természetesen TOR böngészőre van szükség.

A darksearch.io 2019-ben jelent meg és nagy reményeket fűznek hozzá. Gyakran az Ahmia találatainak többszörösét hozza a keresés a Dark Search-en és email címekre is ad találatokat.

Az Onion.link az Ahmia-hoz hasonlóan próbál weboldalakat megismerni a TOR hálózaton. A korábban már említett Google Custom Search Engine-t alkalmazza és minden talált oldalhoz .link végződést ad, ennek köszönhetően a keresőn belül megnyithatóak ezek az oldalak. Nem

valódi TOR kereső, de oldalak felkutatásához hasznos lehet még így is, hogy a felszíni interneten keres utalásokat TOR oldalakra.

Még létezik pár TOR kereső, amely a felszíni internetből is elérhető, de mégis a legerősebb keresőket magán a TOR-on keresztül tudjuk elérni. Ezek közül az elsőszámú a Not Evil kereső, amelyet az alábbi linken lehet elérni:

<http://hss3uro2hsxfogfq.onion/>

Azonban a TOR gyakran kiszámíthatatlan mivoltából adódóan semmi garancia nincsen rá, hogy ez az oldal a jövőben is ezen a címen lesz elérhető. A TOR használata akkor hozhat eredményt általában, ha feltételezhető, hogy valaki korábban már illegálisan, esetleg egy adatszivárgás folytán megszerezte a célpontunk személyes adatait. Míg egy másik felhasználási lehetőség az, hogy ellenőrizzük, hogy magunkról került-e fel bármilyen információ a sötét webre. Erre első lépésként azonban a haveibeenpwned.com is tökéletes eszköz, ahol email címre és telefonszámra kereshetünk, hogy megtudjuk megtalálhatóak-e bármilyen korábbi ismert adatszivárgásban és pontosan milyen típusú adatok keringenek az interneten, amelyek adott személyhez köthetők.

Keresőmotor gyűjtemények

Kettő alkalmazást lehet megemlíteni itt. Az első a Search Engine Colossus, amely országokra lebontva felsorol minden oda köthető keresőmotort és linkgyűjteményt, továbbá információt szolgáltat, hogy ezeken az oldalakon milyen típusú találatokra számíthatunk.

A másik pedig a Fagan Finder, amin több száz különböző keresővel tudunk a kulcsszavunkra rákeresni, de ennek a felhasználása nagyon specializált és az esetek nagyon nagy hányadában nem jutunk vele többre, mint a Google használatával.

FTP keresés

Az FTP vagyis File Transfer Protocol szerverek szinte teljesen kiesnek a Google keresésekből. Ezek a nyilvános számítógépek különböző fájlok megosztására lettek létrehozva és bár a Google és a Bing is indexálja ezeket, a sima keresések között nagyon hátra sorolja őket. Erre megoldás az `inurl:ftp -inurl:(http|https) "kulcsszó"` keresés, amely rákényszeríti a keresőt, hogy kizárólag FTP találatokat mutasson.

1.4 OSINT eszközök, azoknak funkciói, rendeltetése

Társadalmunkban többször merül fel a kérdés, hogy hol is van a határ az OSINT-tevékenységekkel kapcsolatban. Jelen állításban csak a nyíltan megtekinthető adatokat vagy némi ismeretet igénylő módszerek használatával elnyert információkat vesszük alapul. Egy OSINT-jellegű kutakodás kapcsán szinte biztosan megfogalmazódik a tevékenységet végző

személy végzője számára a kérdés, hogy az interneten megtalálható minden megoldás etikusnak, esetenként jogszerűnek tekinthető-e.⁵

Az OSINT szoftverek olyan eszközök, amelyek lehetővé teszik a nyilvánosan elérhető vagy nyílt forráskódú információk gyűjtését. Az internetes adatok több mint 99%-ához nem férhetek hozzá a nagy keresőmotorok. Ide tartoznak azok a nyilvános adatok is, amelyeket az OSINT eszközök segíthetnek összegyűjteni. Egy fejlettebb OSINT szoftver segít több adatpont kombinálásában az információk kereszthivatkozása érdekében – és az igazság forrásának megszerzésében.

Általánosságban elmondható, hogy két kulcsfontosságú tulajdonságot kell figyelembe venni az OSINT szoftver kiválasztásakor:

- Passzív: Az információszerzés leggyakoribb módja. Az elemző beírja a már birtokában lévő adatokat egy passzív OSINT eszközbe, és további információkat tud szerezni. Ez egy hétköznapi példára levetítve ahhoz hasonlít, mintha széles hálóval halásznánk.
- Aktív: A kezdetben esetleg rejtett információkon alapuló adatgyűjtés célzottabb módja. Például barátkozni egy célpont ismerősével a Facebookon, hogy hosszabb távon többet megtudjunk róluk. Visszatérve a halászhasonlathoz, ez inkább a lándzsás horgászathoz hasonlít. Bár nincs szükség speciális szoftverre az aktív taktikákhoz.

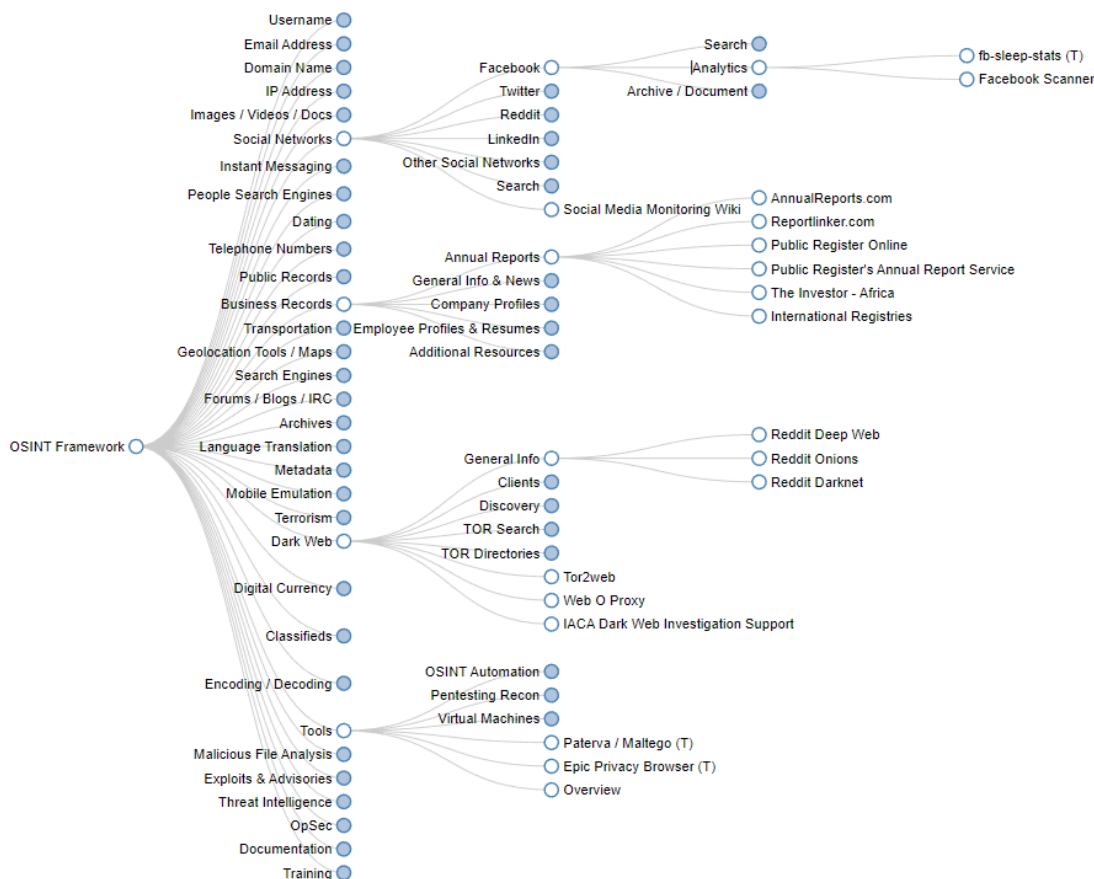
Ezen kívül minden jó OSINT szoftver segít elérni az alábbi információkat:

- közzétett vagy sugárzott (hírek, média, online bejegyzések stb.)
- nyilvános kérésre elérhető (pl. kormányzati népszámlálási információ)
- előfizetéses vagy megvásárolható (fizetős kiadványok, kiadványok)
- nyilvánosan kereshető (surface web)⁶

Rengeteg ilyen eszközt találhatunk az interneten, a legtöbbnek a tárháza az osintframework.com, ahol kategóriákra osztva találhatunk megfelelő eszközöket, weboldalakokat.

⁵ Dobák, Imre: OSINT – Gondolatok a kérdéskörhöz, NEMZETBIZTONSÁGI SZEMLE (ONLINE) 7 : 2 pp. 83-93., 11 p. (2019)

⁶ <https://seon.io/resources/the-best-tools-for-osint/>; letöltve: 2022. 10. 17.



3. ábra OSINT Framework előnézete (forrás: <https://osintframework.com/>)

A 3. számú ábra is jól mutatja, hogy szinte minden témakörben mélyen be lehet ásni magunkat, ha valamit meg szeretnénk találni.

A következőkben pedig néhány eszközt mutatnék be.

OSINT-eszközök lehetnek:

- innovatív adatbányászati és adatelemzési módszerek,
- intelligens nyelvészeti alapokra épülő keresési módszer,
- intelligens keresőmotorok,
- tematikus leválogató rendszer (pl. RSS-csatornák figyelésének automatizálása),
- közösségi oldalak figyelése (pl. flash mobok azonnali kockázati értékelése),
- honlapok forráskódjának értékelése, rejtett tartalmak megjelenítése,
- domain search, whois tools (a honlap domain-előfizetőjéhez kapcsolható adatok kinyerése),
- magyar és nemzetközi sajtófigyelés⁷

⁷ Nemzetbiztonsági alapismeretek - szerkesztette: Resperger István, Dialóg Campus Kiadó Budapest (2018), A nemzetbiztonsági szolgálatok (Dezső Lajos), III. fejezet, 100. oldal

Az alábbi legelterjedtebb OSINT eszközöket pedig felsorolásszinten ismertetném:

- Maltego
- SEON
- Lampyre
- Google
- Recon-ng
- SpiderFoot
- Spokeo
- Have I Been Pwnd?
- PhoneInfoga
- Email Hippo

2) A kibertér és a nyílt forrású információszerzés kapcsolata

Ebben a fejezetben a kibertérben tevékenykedő személyek tevékenységeit vizsgálom, továbbá az általuk végzett hálózatfelderítési, sérülékenységvizsgálati módszerek kapcsolatát az OSINT tevékenységekhez. Emellett elemzem a közösségi média szerepét a nyílt forrású információszerzésben, valamint annak kapcsolatát a kibertámadásokhoz.

2.1 Az etikus hackelés

Napjainkban sokszor halljuk ezt a kifejezést, de mit is jelent valójában? Mi teszi 'etikussá' a hackelést? A hackereket két csoportba tudjuk osztani, black hat (fekete kalapos) és white hat (fehér kalapos) hacker-ek, ahol az utóbbi tartozik az etikus kategóriába.

Pontosan mi is az a hackelés?

„A hackelés nem más, mint törekvés arra, hogy hozzáférj olyan számítógépekhez vagy más IT eszközökhöz, azon tárolt adatokhoz, amelyekhez jogosultsággal nem rendelkezel. Továbbá a hackelésbe természetesen beletartozik eszközök jogszerűtlen manipulálása is.”⁸

A felhasználói szinten bárki képes lehet futtatni olyan scripteket vagy programokat, amelyek segíthetik a hitelesítést pl. ismeretlen wifi hálózatokba, így képesek lehetünk bejutni egy olyan hálózatba, amelynek nem vagyunk legális felhasználói és akár titkosítva is van.

Ha viszont mi írjuk a programot, ami képes feltörni idegen wifi jelszót, akkor az már egy másik tudásszintet képvisel. Aki pedig tud programozni annyira, hogy írjon egy wifi kódot feltörő programot, az valószínűleg nem fog idegen kódot futtatni, mert tudja, hogy könnyen lehet benne egy másik kártékony kód (például telepíthetünk egy jelszó lopó programot önszántunkból a saját eszközünkre).

⁸ <https://bluebird.hu/mennyit-ernek-az-etikus-hackerek/> letöltve: 2022.11.05.

*Mikor lehet, és nem lehet hacker tevékenységet végezni? Ez különbözteti meg az etikus hackert a többi hackertől. Ha felhatalmazással futtatjuk a fentiek szerinti programot, akkor nevezhetjük magunkat etikus hackernek.) Ha viszont anélkül futtatjuk, akkor egyértelműen bűncselekményt követünk el.*⁹

Viszonyításképp pedig pontokba szedem a két hacker közötti lényeges különbségeket, amelyet az 1. számú táblázat szemléltet.

White hat hacker (etikus)	Black hat hacker (nem etikus)
Felhatalmazással rendelkezik	Nincs felhatalmazása
Tevékenységet szerződések szabályozzák	Tevékenysége illegális
Célja a biztonsági rések javítás miatti felfedése	Célja a biztonsági rések kijátszása, haszonszerzés
Munkaszerűen végzi tevékenységét	Hobbiként vagy anyagi érdek alapján végzi tevékenységét
Tevékenysége szabályozott	Tevékenysége szabályozatlan

1. táblázat Etikus és nem etikus hackerek összehasonlítása (saját szerkesztés)

Megkülönböztetünk még egy harmadik kategóriát is, ami a két csoport között helyezkedik el, ők pedig a grey hat hacker-ek („szürke kalapos hackerek”). Ők jellemzően olyan személyek, akik megsérthetik az etikai normákat vagy elveket, de rosszindulatú szándék nélkül teszik azt. Felhatalmazás nélkül keresnek biztonsági réseket, majd találat esetén értesítik a megtámadott rendszer üzemeltetőit. Az értesítést követően felajánlják segítségüket, persze többnyire pénzért cserébe. A „szürke kalapos hackerek” a középutat jelentik a white hat hacker-ek, akik a biztonságos rendszereket fenntartók nevében tevékenykednek, és a black hat hackerek között, akik rosszindulatúan cselekszenek a rendszerek sebezhetőségeinek kihasználása érdekében. További hacker típusok lehetnek még: blue hat hacker (új rendszerek tesztelésére), green hat hacker (kezdő hacker), script kiddie (mások által megírt programokat használnál fel).¹⁰

⁹ <https://bluebird.hu/mennyit-ernek-az-etikus-hackerek/> letöltve: 2022.11.05.

¹⁰ <https://www.techopedia.com/definition/15450/gray-hat-hacker>; letöltve: 2022.11.05.

Viszont, hogyan is kapcsolódik ez a témához, merül fel a kérdés. Több cég is foglalkozik etikus hackeléssel, és működik szolgáltatásként más cégek vagy szervezetek számára. Ez alól a katonai szervezetek sem kivételek. Ha békeidőben nem is – vagy pontosabban hiteles tudomásunk nincs róla - háborús időkben (lásd, orosz-ukrán konfliktus, amelyet a következő fejezetben részleteznék) annál inkább fontosnak tartják a sérülékenységek, az esetleges károk kivizsgálását és az adatszivárgás megállítását. Kiemelendő továbbá, hogy minden esetben rendelkezni kell az adott cégnek/személynek megbízólevéllel, amely megfelelő jogi védelmet biztosít.

2.2 Közösségi média szerepe a nyílt forrású információszerzésben

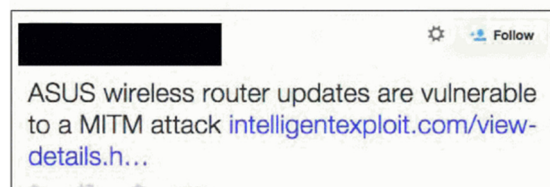
Ebben az alfejezetben a legnagyobb közösségi média platformok közül a Twittert ismerettem, amely az elmúlt évtizedben a nyílt forrású információszerzés létfontosságú eszközévé vált. A közösségi oldal adatait a kutatók arra használták, hogy információkat gyűjtsenek a természeti katasztrófák, terrortámadások, kormányválasztások, tőzsdei előrejelzések stb. hatásairól. Magánszemélyek vagy neves biztonsági szakértők, mint például Brian Krebs (oknyomozó újságíró, aki a kiberbűnözésről ír) értékes források lehetnek a kiberbiztonsági eseményekkel kapcsolatban. Az olyan elismert cégek, mint a @web_security vagy a @intersecww, vagy híreket, tippeket és legfrissebb információkat terjesztenek a webes biztonságról, a webes alkalmazások védelméről, a hacker incidensekről, az adatvédelmi incidensekről, a behatolástesztek eredményeiről stb. Nyilvánvaló okokból az ilyen fent említett szervezeti fiókok értékes információforrások a kiberbiztonsági események tekintetében. A Twitter-felhasználók, ha új sebezhetőségek kerülnek nyilvánosságra, vagy saját tapasztalat alapján észreveszik azokat, akkor tweetelnek¹¹ ezekről a sérülékenységekről, hogy az információt

¹¹ tweet: a Twitteren közzétett bejegyzések neve

terjesszék a hálózaton és mások is felhasználhassák az adott információt a rendszereik védelmére,¹² a 4. és 5. számú ábrák példák ezekre.



4. ábra Tweet egy egyéni felhasználótól egy közelmúltbeli biztonsági sebezhetőségről (forrás: CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities – IEEE)



5. ábra A felhasználók és a szervezetek a Twittert használják a potenciális fenyegetések bejelentésére (forrás: CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities – IEEE)

Továbbiakban egy egyetemi hallgatót szeretnék ismertetni, Justin Peden, akit Intel Crab álnéven ismernek. Személye valószínűtlen információforrássá vált a kibontakozó ukrán-orosz háborúval kapcsolatban.

A 20 éves férfi műholdképeket, TikTok-videókat és biztonsági hírfolyamokat böngész át, és a Twitteren több mint 220 000 követővel osztja meg az olyan megállapításokat, mint a csapatok mozgása és a repülőgép-modellek. Peden elmondta, hogy bejegyzései 20 millió emberhez jutottak el, követőinek száma pedig több mint 50 000-rel nőtt az elmúlt hónapban a Twitter-elemzése szerint.

Ma Peden a nyílt forrású információszerzés (OSINT) egyik legjelentősebb alakja a Twitteren.

13

Ez mondhatni a twitter pozitív oldala, amikor olyan dolgokat ismerhetünk meg, amelyek hasznosak lehetnek a felhasználók számára.

¹² S. Mittal, P. K. Das, V. Mulwad, A. Joshi and T. Finin, "CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities," 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2016, pp. 860-867, doi: 10.1109/ASONAM.2016.7752338.

¹³ <https://restofworld.org/2022/osint-viral-ukraine/>; letölve: 2022. 05. 26. fordította: szerző

2.3 A nyílt forrású információszerzés szerepe a kibertámadásokban

Egyértelmű az, hogy a kibertámadások nélkülözhetetlen eleme az információszerzés, és különböző támadási célok lehetnek, amikhez más és más információk szükségesek. Egy kibertámadás céljai igen sokrétűek lehetnek, többek között irányulhatnak információk gyűjtésére, módosítására, megváltoztatására, zárolására, törlésére, illetve megsemmisítésére, továbbá egy szolgáltatás vagy, infrastruktúra megfelelő működésének akadályozására, korlátozására, valamint gazdasági, politikai előny szerzésére, álhírek terjesztésére, hírnévrontásra, károkozásra, bizalomvesztés generálására, vagy akár vallási célok elérésére is.¹⁴ Ezeket a legkönnyebben úgy lehet megszerezni, ha kihasználják a sérülékenységeket és a kockázatokat. Három csoportba lehet az információkat sorolni, amelyek a 6. számú ábrán látható, majd pár mondatban ismertetném a különböző információkat.



6. ábra A kibertámadások végrehajtásához szükséges információk¹⁵

Az informatikai rendszerre vonatkozó információk, amelyek tartalmazzák az adott rendszer működését a rá csatlakoztatott eszközparkot és annak jellemzőit és a többi lényeges adatot.

A célpontra vonatkozó információkon belül még két típust különböztetünk meg, a szervezetre jellemzőket és a személyekre jellemzőket. A szervezeten belüli magába foglalhatja a felépítést, a szervezet tevékenységét, munkavállalóit és az elérhetőségeit. A személyekre vonatkozóan pedig az elkövető emberek hibáit kihasználva próbálja megszerezni a támadó az adott információt. Ilyen lehet például, a nem megfelelő jelszóvédelem, naivitás, nyitottság, valamint de sorolnám továbbá a social engineering témakörét is.

¹⁴ Deák Veronika: A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során – Hadmérnök, XIII. évfolyam 3. szám – 2018. szeptember 393. oldal

¹⁵ Deák Veronika: A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során – Hadmérnök, XIII. évfolyam 3. szám – 2018. szeptember 394. oldal

A tervezési, szervezési, végrehajtási információk jellemzői, hogy magukba foglalják a konkrét támadás kivitelezéséhez szükséges technikai, személyi, tárgyi és pénzügyi feltételeire vonatkozó ismereteket.

A célok tisztázása után kitérnék a potenciális eszközökre, amelyeket használhat egy támadó. Az eszközei lehetnek:

- személyes megkeresés;
- rádió- és televíziós adások, médiahírek;
- kuka átvizsgálás;
- internetes információgyűjtés;
- megfigyelés;
- hagyományosan publikált anyagok;
- telefonos információgyűjtés.

Ebből következően, egy kibertámadás előkészületeit is legnagyobb százalékban az OSINT teszi ki, hiszen az előbb felsorolt eszközök közül is nagy részüket megtalálhatjuk akár a Google keresőszolgáltatásával is. Továbbá különböző applikációk is segíthetik a támadók munkáját, mint például a Creepy alkalmazás, amely ki tudja nyerni a helyadatokat a tweet-ekből és a fényképekből, és ha egy felhasználónak több tweet-je is van akkor képes egy térképet összeállítani a megszerzett geolokációs adatokból.¹⁶

A sebezhetőségek, sérülékenységek feltárása azért kiemelkedő jelentőségű, mert ennek tudatában a támadó fel tudja mérni, hogy a támadást pontosan hol kell végrehajtani. Ugyanakkor a social engineering technikák is nagy szerepet játszanak a kibertámadás előkészületeiben, ezért fontos ügyelni a megfelelő tájékoztatásra és a biztonságtudatosági tréningekre az alkalmazottak körében.¹⁷

A Thales cég kifejlesztett egy szoftvert a kibertámadások követésére, és a támadó csoportok tevékenységét is részleteiben bemutatja és mindig élő képet mutat.

Példaképpen szemléltetek egy csoportot, aminek a neve az ATK64, amelynek a fő támadási szektora a hadsereg és a védelem. A következő területeket támadja, Afganisztán, Németország,

¹⁶ <https://creepy.en.softonic.com/>; letölve: 2022.11.08., fordította: szerző

¹⁷ Deák Veronika: A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során – Hadmérnök, XIII. évfolyam 3. szám – 2018. szeptember

Pakisztán, Irán és India és az alábbi Malware¹⁸-eket használja: Crimson, ObliqueRAT, CapraRAT.

Ezen a linken érhető el: <https://cyberthreat.thalesgroup.com/>

2.4 Geolokációs információgyűjtés

A geolokációs információgyűjtést azért is szerettem volna kiemelni, mert véleményem szerint az egyik kulcsfontosságú tényezője az információk keresésének és rengeteg adatot tud szolgáltatni a felhasználójának. A műholdképek, valamint más források, például a közösségi médiában közzétett bejegyzések és a videók földrajzi helymeghatározása/metaadatai lehetővé teszik a nyílt forrású információk elemzését a nyilvánosan elérhető adatokból.

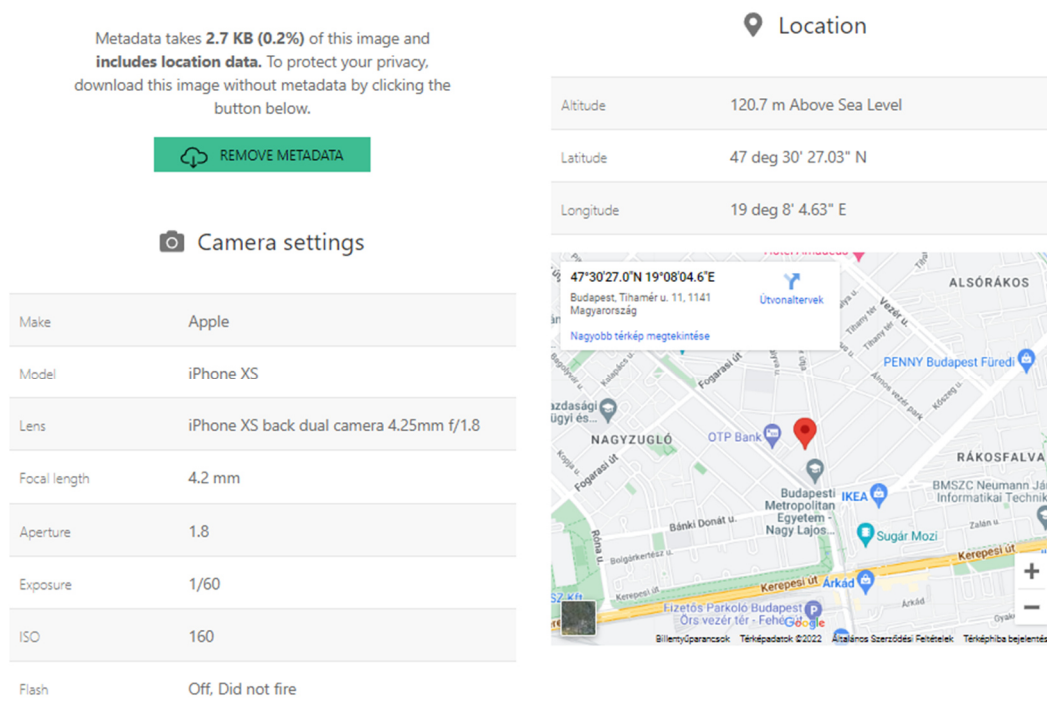
Először is tisztázásra szorul egy fogalom, mi is az a metaadat? A metaadatok választ adnak nekünk a "ki", "mit", "mikor", "hol" kérdésre és talán segítenek a "miért"-re következtetni.

Fontos tudni viszont, hogy a metaadatok törölhetők vagy hamisíthatók.

A metaadatok megtekintésének két módja van:

- Megtekinthetjük a fájlt létrehozó program segítségével
- Egy erre a célra készült alkalmazás használata (online vagy a számítógépre telepítve).

¹⁸ „Az angolul malware (az angol malicious software rövidítése), magyarul szó szerinti fordításban rosszindulatú szoftver (egyéb megnevezései kártevő szoftver, kártékony szoftver, káros szoftver). Mint ilyen, a rosszindulatú számítógépes programok összefoglaló neve. Ide tartoznak a vírus, féreg, kémprogram (spyware), zsarolóprogram (ransomware), agresszív reklámprogram (adware), és a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszköz (rootkit). A számítógépes kártevő programok mennyisége folyamatosan növekszik, és időről időre új típusok terjednek el. Az ellenük való védekezés víruskereső programnak nevezett szoftverekkel történik.”; forrás: Wikipédia



7. ábra Egy kép adatai (saját forrás)

Ha egy képet elemzünk ki, akkor ez esetben sokat tudhatunk meg az EXIF¹⁹-fájlokból. Az 7. ábra is jól részletezi, a készítés helyét, idejét, milyen eszközzel készítették stb.

A következőkben pedig kifejténék pár eszközt, mik is az azok az alternatívák, amik segíthetnek a geolokációs információgyűjtésben.

- a) műholdképek
- b) nyilvános kameraképek
- c) légifelvételek
- d) földrajzi koordináták
- e) geoinformációs rendszerek és szoftverek
- f) tematikus térképek
- g) épületek kutatása²⁰

Utolsónak pedig egy példa alapján szeretném ismertetni, mennyi információ állhat rendelkezésre, akár egy Google Street View vagy egy nyilvános kamerakép által.

Példa 1:

¹⁹ „Az EXIF-fájl olyan adattárolási forma, amely különleges információkat tartalmaz a fényképekről, például a fényképezőgép beállításait, az időt és a dátumot, valamint a fénykép készítésének helyét.” (forrás: <https://www.adobe.com/hu/creativecloud/file-types/image/raster/exif-file.html>)

²⁰ Open Source Intelligence Tools and Resources Handbook 2020 – Aleksandra Bielska



8. ábra Utcakép (forrás: osintme.com)

Vizuális nyomok a 8. ábra alapján:

- Egy logónak tűnő jel és egy részben látható név - "Golden T";
- Országzászlók, melyek közül az első Dél-Afrika zászlója, az afrikai zászlókat meg lehet találni az alábbi oldalon: https://www.nationsonline.org/oneworld/flags_of_africa.htm;
- Tágas parkoló az elülső oldalon, zárt kerítés, pollerek és zászlótartó oszlopok - talán egy szálloda lehet;
- Nagy, hosszú, határozott formájú építmény - a Google Maps légifelvételein láthatónak kell lennie;
- Afrikai származású személyek az előtérben;
- Régebbi kinézetű autók, fejlődő országra utalva;
- Trópusi / meleg ország növényzete - tehát minden bizonnyal valahol a déli féltekén;
- Távközlési antenna a közelben.

Módszerek:

- Érdeemes váltani a Google dél-afrikai verziójára a jobb, lokalizált keresési eredményekért;
- Keresés a következőre: golden t hotel +Afrika;
- Első találat - a "Golden Tulip Africa" Facebook oldala;
- Váltás a Google-ban a fényképek fülre, majd böngészés manuálisan a képek között;

- A Golden Tulip hotel azonosítása Accra, Ghána városában a képek felismerésével;
- Ellenőrzés a Google Maps utcakép segítségével, így megtalálhatjuk, ugyanazt a szöveget
- GPS-koordináták másolása a Google Maps-ról.

Végezetül pedig megkapjuk a pontos helyzetet: Golden Tulip, 37 Liberation Rd, Accra, Ghána.

5° 35'35.5" N 0° 10'50.5" W

Példa 2:



9. ábra Kamerakép (forrás: osintme.com)

Most pedig nem csak a helymeghatározásra keressük a választ, hanem arra is, hogy milyen IP-cím tartozik ehhez a kamerához és hogy melyik internetszolgáltatóhoz tartozik az adott IP-cím.

Módszertan a 9. ábra alapján:

- Néhány nyilvánvaló vizuális nyom keresése - aki Európában született azonnal fel fogja ismerni az építészet alapján az európai jellemvonásokat (a tornyok, a piros tetők, a lakóházak stb.);
- Fordított keresés a célképen a Firefox Image Search Options bővítményével (vagy egy hasonló böngészőbővítménnyel a képek fordított kereséséhez);
- Megtekinteni azt a weboldalt, amit a Google megjelenített (<https://www.webcam-netzwerk.de/Estonia/Pirso/750577.html>);

- Megkeresni azt a webkameraképet, amely vizuálisan megfelel a célképnek (Tipp: ezt érdemes az adott hely nappali óráiban, (jelen esetben: UTC/GMT+1 vagy +2), mert sötétben nem fog látszódni a kép legtöbb jellemzője);
- Az eredeti weboldal felkeresése, ahonnan a kép származik;
- Ellenőrizzük le a weboldal domain információit a Big Domain Data (vagy egy másik hasonló eszköz segítségével, amely megjeleníti a kapcsolódó IP-címet);
- Az IP Info oldal felkeresése, majd futtassuk le a kapcsolódó IP-cím ellenőrzését, hogy megtaláljuk az internetszolgáltatót.

Itt is választ kapunk az összes kérdésre, amelyek a következők: Tallin, Észtország. 217.159.186.253. AS3249 Telia Eesti AS.²¹

Ezekkel a példákkal az volt a célom, hogy szemléltessem, mennyi részlet kiderülhet egy egyszerű kép alapján is, és hogy mennyi alkalmazás és weboldal a segítségünkre van ebben. A weboldalak kategória szerinti összefoglalóját az alábbi kötetben találhatjuk meg a legspecifikusabban: Open Source Intelligence Tools and Resources Handbook 2020 – Aleksandra Bielska.

3) A nyílt forrású információszerzés kapcsolata a hadsereggel

Több felsővezetővel is hitelesen alátámasztott, hogy a katonai műveletek előtt az információk körülbelül 80%-át nyílt forrásokból gyűlik össze. Magyar vonatkozásban az Információs Hivatal (IH) gyűjti össze az információkat és szűri ki ezek közül a feladatellátáshoz a legmegfelelőbbeket.²²

3.1 Az OSINT szerepe a nemzetbiztonsági szervezeteknél

„A világunkat elárasztó adat- és információmennyiség célirányos monitorozására és kutatására aligha lenne lehetőség a nyílt forrásból származó információgyűjtés nélkül. A nemzetbiztonsági szolgálatok eszköztárában az OSINT egyre inkább meghatározó szerepet tölt be.”²³

A nemzetbiztonsági szolgálatoknál fontos azt elemezni, hogy milyen adatot vagy információt szeretnénk megszerezni, ennek értelmében a képességek és lehetőségek jelentős mértékben függenek az adatszerzés jellegétől és módjától.

²¹ <https://www.osintme.com/index.php/2022/01/31/osint-dojo-student-challenge-geolocation-puzzles/>; letöltve: 2022.11.10., fordította: szerző

²² Nemzetbiztonsági alapismeretek - szerkesztette: Resperger István, Dialóg Campus Kiadó Budapest (2018), A nemzetbiztonsági szolgálatok (Dezső Lajos), III. fejezet, 100. oldal

²³ Szabó Károly: Az OSINT – Gondolatok a tevékenységről és az alkalmazás közegéről; NEMZETBIZTONSÁGI SZEMLE 7. évfolyam (2019) 2. szám 68–82. • doi: 10.32561/nsz.2019.2.6

Az információszerzést pedig az alábbi hírszerzési ágak végzik:

- emberi erőforrásokkal folytatott hírszerzés (HUMINT²⁴);
- rádióelektronikai felderítés (SIGINT²⁵);
- nyílt forrású hírszerzés (OSINT);
- képfelderítés (IMINT²⁶);
- mérés és jelmeghatározó hírszerzés (MASINT²⁷);
- kiberhírszerzés (CYBINT²⁸).²⁹

„A magyar nemzetbiztonsági gondolkodásban – a titkos információgyűjtés jogi szabályozásának elsődlegessége mellett – főként a hírszerzés-felderítés (intelligence) fogalomrendszerét és az ott megjelenő egyes ágakat (így pl. HUMINT, SIGINT, OSINT stb.) vehetjük alapul. Ennek kereteit tekintve azonban nem feltétlenül lehet és indokolt minden hazai információgyűjtő tevékenységet a jelzett fogalomrendszerbe besorolni, már csak az egyes területek eltérő adottsága vagy akár rendeltetése okán sem.”³⁰

Az egyik legfontosabb dolog az OSINT tekintetében a döntéshozatal. *„A nemzetbiztonsági szolgálatok eszköztárában lévő lehetőségeket aszerint is érdemes tehát megvizsgálni, hogy jellemzőik által milyen hatást gyakorolhatnak a döntéshozók munkájára. Ez az OSINT estében is szükségzerű.”³¹* Tehát különböző szolgálatoknak érdemes összpontosítaniuk az alkalmazási kockázatokra.

Minden tevékenység mozzgóeleme a különböző médiumokon alapszik. Igaz az, hogy a titkos információgyűjtés forrásaiból származó információk esetében megvan a kockázata annak, hogy a minősített információk előbb-utóbb nyílt információkká alakulnak át és a médiában is megjelenhetnek. A titkos információgyűjtés eszközeinek és módszereinek alkalmazása útján megszerzett, minősített információknak az OSINT lehetőségeivel történő visszaellenőrzése pedig szinte lehetetlen, ahogy a dolgozatom elejében is kifejtettem. Viszont, ezekből az információkból is lehet szűrni különböző adatokat, amik hasznosak lehetnek a szolgálatok számára. Vagy éppen az információk kikerülése kárt is okozhat egy másik országnak.

²⁴ Human Intelligence

²⁵ Signal Intelligence

²⁶ Imagery Intelligence

²⁷ Measurement and Signature Intelligence

²⁸ Cyber Intelligence

²⁹ Nemzetbiztonság elmélete a közszolgálatban - szerkesztette: Resperger István, Dialóg Campus Kiadó Budapest (2018), IV. Hírszerzés (Vida Csaba), 119. oldal

³⁰ Nemzetbiztonság elmélete a közszolgálatban - szerkesztette: Resperger István, Dialóg Campus Kiadó Budapest (2018), III. Az információgyűjtésről általában (Dobák Imre), 99. oldal

³¹ Szabó K. 2019

Ismertetőként mutatnám be a különböző adatok kikerülésének veszélyességi szintjeit hazai vonatkozásban, mely kategóriába tudjuk helyezni az OSINT által szerzett információkat.

„(4) Amennyiben az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele

a) rendkívül súlyosan károsítja a minősítéssel védhető közérdeket, akkor „Szigorúan titkos!”,

b) súlyosan károsítja a minősítéssel védhető közérdeket, akkor „Titkos!”,

c) károsítja a minősítéssel védhető közérdeket, akkor „Bizalmas!”,

d) hátrányosan érinti a minősítéssel védhető közérdeket, akkor „Korlátozott terjesztésű!”

minősítési szintű.”³²

Ezt az elemzés fázisában kell mérlegelni, és a következtetéseket levonni belőle.

Az egyes szolgálatok is a hírszerzési ciklust veszik alapul, amit a 2. ábrám is ismertet.

Az OSINT-tal összefüggve, egyre jobban kibontakozó ágba van az úgynevezett Cyber Intelligence (CYBINT) vagyis a kiberhírszerzés. Az ilyen típusú hírszerzés a fizikai kémkedés és a védelem keveréke a modern információs technológiával.

A kiberhírszerzés védelmet nyújt az olyan digitális fenyegetésekkel szemben, mint a vírusok, hackerek és terroristák, amelyek célja érzékeny információk ellopása az interneten keresztül.³³

A CYBINT és az OSINT közti különbségnek az tekinthető, hogy míg a CYBINT-nél szükséges hacker tevékenységet folytatni, addig az OSINT-nál ez nem túl nagy mértékben jelenik meg, hiszen lényegében csak a digitális lábnyomokat gyűjtjük össze.

Ehhez az alfejezethez zárszóként Vida Csaba véleményezését emelném ki, mely a saját meglátásommal is egybefügg; „[...] egy régi hírszerzési ágként az OSINT a hírszerzési ciklus adatszerzési szakaszának integrált része, bár a korábbiakhoz képest jóval nagyobb hangsúlyt kapott, és esetenként egyedül is képes biztosítani a szükséges adatokat. Az OSINT esetében azonban ügyelni kell arra, hogy a hírszerzés ne váljon egyoldalúvá, mert a hatékony és eredményes munkához továbbra is szükség van a többi hírszerzési ág által megszerzett adatokra és információkra. A CYBINT-tel kapcsolatban más a helyzet, mert az alapvetően nem információszerző hírszerzési ág, hanem funkcióját vizsgálva inkább a fedett és a titkos

³² 2009. évi CLV. törvény a minősített adat védelméről, II. Fejezet, 4. §

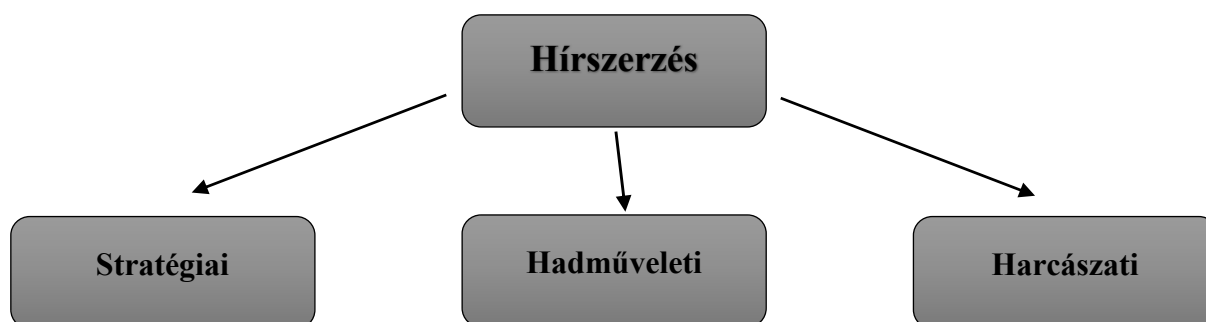
³³ <https://usnwc.libguides.com/c.php?g=494120&p=3381599>; letöltve: 2022. 11. 06.

hírszerzési akciókhoz lehet hasonlítani. ”³⁴

3.2 Az orosz-ukrán háború OSINT vonatkozásai

Hogyan is keveredik az OSINT a háborúhoz? A közösségi média a nyílt forrású információgyűjtés aranybányája és az egyének vagy a csapatmozgások felderítésére számos ingyenes, legális eszköz áll rendelkezésre, amit az előzőekben is kiemeltem.

Háborús helyzetben három felé lehet osztani a hírszerzést.



10. ábra Hírszerzés felosztása (saját szerkesztés)

Stratégiai szintű hírszerzés: Ide tartozik a HUMINT és az OSINT eszközei is. (pl. attasék, nagykövetek küldése)

Hadműveleti szintű hírszerzés: ezt a feladatot főképpen a különleges erők és a mélységi felderítők végzik el. Fontos továbbá a SIGINT – jelhírszerzés – és az IMINT – képi hírszerzés - is ebben a szakaszban.

Harcászati szintű hírszerzés: ez már csak felderítésnek tekinthető a parancsnok információigényei alapján, legjobb megoldása a drónokkal való felderítés.

Mindössze egy héttel azután, hogy Oroszország teljes körű inváziót indított Ukrajnában, az OSINT-ot széles körben kezdték el használni a hírekből és a közösségi médiából származó tényellenőrző narratívák megértésére.

Kiemeltem ezek közül három fontosabb lekövetést:

- A katonai csapatok mozgásának lekövetéséhez: A közösségi média tartalmaiból vett rendszámadatokat például arra használták, hogy járműveket kapcsoljanak össze a kormányzati szervekkel. A műholdfelvételek képei továbbá az orosz járművek mozgását is meghatározhatják.

³⁴ Vida, Csaba (2013) Létezik-e még a hírszerzési ciklus? Miről szól a hírszerzés? Felderítő Szemle, XII (1). pp. 43-57. ISSN ISSN 1588-242X

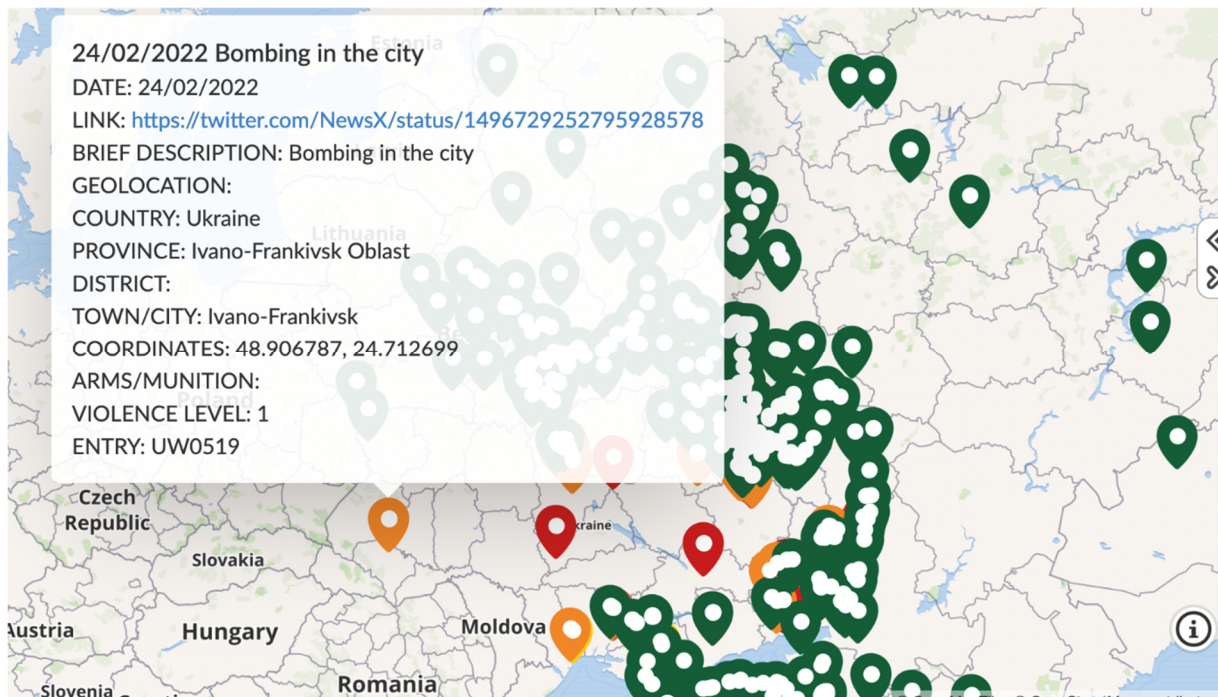
- Felmérni az éppen zajló eseményeket és a sérülteket: Miközben a felhasználók fotókat és videókat tesznek közzé az eseményekről, az elemzők figyelemmel kísérhetik a támadásokat és valós időben értékelhetik a károkat. A nyilvános közösségimédia-tartalmak és a műholdképek szintén segítenek az elemzőknek abban, hogy pontosan meghatározzák a tevékenységek földrajzi helyét.
- Ellenőrizni a dezinformált tartalmakat. Az elemzők használnak olyan alkalmazásokat, amelyek lehetővé teszik az események idő és hely szerinti csoportosítását. Több cég is foglalkozik ilyen típusú adat szelektációval.

A Russia-Ukraine Monitor Map a Center for Information Resilience (CIR) cég fő profilja az, hogy nyílt forrású információkból dokumentálja és ellenőrizze az információk hitelességét az ukrajnai konfliktus során történt jelentős eseményekről, majd egy térkép segítségével vizualizálja azt. Célja, hogy megbízható információkat nyújtson a politikai döntéshozók, újságírók, valamint igazságügyi szervek számára a változó helyzetekről. A Bellingcat és a Conflict Intelligence Team is képes hozzájárulni a térképek bővítéséhez azáltal, hogy a projekthez felülvizsgált összes tartalmat összegyűjtik, és megőrzésre elküldik a Mnemonicnak³⁵.

A 11. számú ábrán látható térképen látható minden egyes információ tartalom ellenőrizve van és a különböző pontokra kattintva további részletes információkat tudhatunk meg az ott történt eseményekről.³⁶

³⁵ A mnemonic egy kiberbiztonsági szolgáltató, amely egyértelmű válaszokat és utakat kínál összetett biztonsági kihívásokra. forrás: <https://www.mnemonic.io/company/>; letöltve: 2022.11.07., fordította: szerző

³⁶ <https://www.bellingcat.com/news/2022/02/27/follow-the-russia-ukraine-monitor-map/>, letöltve: 2022.11.07., fordította: szerző



11. ábra Ivano-Frankivszkban történt bombamerénylet részletes kimutatása a térképen, forrás: <https://www.bellingcat.com/news/2022/02/27/follow-the-russia-ukraine-monitor-map/>

A térkép az alábbi linken található meg: <https://maphub.net/Cen4infoRes/russian-ukraine-monitor>

Befejezésként pedig szót ejtenék a nem régi Joker-botrányról is, melyben az ukrán katonai parancsnokság által használt amerikai „Delta” programot feltörte a „Joker DPR” hacker csoport.

Korábban az ukrán média nyilvánosságra hozta az ukrán katonák által használt külföldi modern technológiákat és szoftvereket, amelyeket amerikaiaktól kaptak. Az ukrán katonák megalázták az oroszokat, mondván, hogy túl messze vannak az ilyen technológiáktól.

Az oroszok viszont mondhatni nem törődtek a saját rendszereik fejlesztésével, és feltörték az ellenség által használtakat. November 1-jén a DPR sajtószolgálatának vezetője, Daniil Bezsonov megerősítette, hogy a DPR hadserege hozzáférést kapott az ellenséges szoftverhez. Hogy világos legyen, ez egy parancsnoki és irányítási program, amelyben a baráti és ellenséges csapatokra vonatkozó összes adat szerepel, és rendszeresen frissül, többek között a hírszerzési forrásokból származó információkkal, és amelynek egy aktuális állapotát a 12. számú ábra szemlélteti.³⁷

³⁷ <https://southfront.org/us-delta-program-used-by-ukrainian-military-command-hacked-by-joker-dpr-hacker-team/>; letöltve: 2022. 11. 10., fordította: szerző



12. ábra kép a Delta rendszeren tárolt információkból (forrás: <https://southfront.org/us-delta-program-used-by-ukrainian-military-command-hacked-by-joker-dpr-hacker-team/>)

3.3 A katonai felsővezetőkkel végzett interjúk összefoglalója

Szekcióm zárásaként több felsővezetőt is meginterjúvoltam a témával kapcsolatban, akik nap mint nap dolgoznak OSINT eszközökkel. Az ő válaszaik elemzése után, jutottam a következő állításokra, megválaszolva ezzel a kutatási kérdéseimet.

- Milyen megoldásokat jelent a katonai műveletekben az OSINT szélesebb körben történő terjedése?

A katonai műveletekhez való szigorú kapcsolódást nehéz kívülről megítélni, de a jelenség gyökere abban rejlik, hogy azzal, hogy az infokommunikációs eszközök, online közösség megoldások széles körben elterjedtek a társadalom tagjai között, mindenki (és nem csak a katonai szereplők) szükségszerűen fordul ezekhez a megoldásokhoz. Kritikus eseményeknél pl. fegyveres konfliktus az információk kiemelt szerepet kapnak így minden forrásból (köztük a nyílt) forrásból is várják az aktuális, a helyzet megítélését segítő adatokat. Pl. az ukrán-orsz háború első napjaiban a keleti területen élő lakosság tömegesen osztotta meg az orosz csapatmozgásokra vonatkozó információkat (pl. twitter). Ezek nem csak szöveges, hanem képi információk, fotók, videók is. Pozitívum, hogy ezek egyrésztől rendkívül értékes

információként becsatornázták a helyszínen lévőktől érkező adatokat, másrésztől egyes elemeiben felmerülhet a hitelesség kérdése, így ezek tudatos kihasználásával ezen nyílt források, információk akár a dezinformáció elemeit is jelenthetik.

Az OSINT kapcsán létezik egy ún. CNN effektus, amikor a média a tudósítás és hírek tájékoztatásának szándékával akár hamarabb adott helyszínen lehet, mint más szereplők, így ebben az esetben ők lesznek az információk elsődleges forrásai. (itt is a hitelesség és a függetlenség kérdése merülhet fel.) További hátránya (nézőpont kérdése) is lehet, hogy könnyen bemérhetővé válik az adott célpont.

Minden bizonnyal a kihívások legyőzésére a mesterséges intelligencia használata, tanítása lesz tud hatással.

– Melyek azok az alkalmazások, amelyek a parancsnokokat segíthetik a döntéshozatal során? Számos megoldás nyíltan elérhető a neten, a komolyabb változatok már csak előfizetés ellenében, gondolhatunk itt pl. az információbrókerekre, akik fizetés ellenében szolgáltatnak adatokat, vagy akár biztosítják az adott célra kifejlesztett szoftvereiket.

Akár ajánlhatók bizonyos felületek, azonban ezeket a másik fél a már említett módon akár ki is használhatja a befolyásolás érdekében. Felmerül a nyílt források hitelességének a kérdése, így pl. a média szerepe is, amelyet azonban a felek szintén kihasználhatnak saját érdekeik érvényesítésére.

Az OSINT és megoldásai esetében a legnagyobb gond tehát az információk hitelességének kérdése, amelyek konfliktusos helyzetekben tömegesen jelennek meg, és szinte lehetetlen csak erre a forrásra hagyatkozva megállapítani azok valódiságát. (itt jönnek képbe a más forrásból származó információk).

A parancsnokokat kielégítő két legfontosabb információ igénye, az ellenségről és a terepről szerzett információk, ebben továbbá segíthetik a drónfelvételek is, amit az aktuális időben készítenek el és biztosan hiteles.

Fontossá válnak az OSINT előnyei:

- akár ingyenes megoldások
- nem kell hozzá engedély
- tömegesen keletkeznek információk (ez akár gond is lehet)
- az információk akár a helyszínről érkehetnek (pl. twitter videó)
- olcsóbb lehet, mint a HUMINT

Ezen felül hátrányai:

- tömegessége, amelyből nehéz kiszűrni a számunkra értékeset
- sokféle nyílt platform, amely forrásként szolgálhat
- nehéz kiszűrni a hiteles információt.

Továbbá nagyobb hangsúlyt kell fektetni a Cyber Threat Intelligence-re (CTI) is.

- Egy háborús helyzetben a HUMINT vagy az OSINT a célravezetőbb?

Mindkét felderítési fajta együttes alkalmazása (természetesen a többi felderítési móddal együtt) szükséges. A közeli és a távlobbi jövőben is szükség lesz a HUMINT-ra is. Ezek nem kizárólagosságot, hanem együttműködést jelentenek. A minden forrású felderítés (ASI – All Source Intelligence) elv továbbra is működik.

Amennyiben nincs adott helyszínen HUMINT forrás, akkor szükségszerűen fordulnak az OSINT-hoz. Ha csak OSINT van, akkor a már jelzett hitelességi és tömegességi problémák adódnak.

Ugyanakkor megfelelő szakmai tudással a civil szereplő is akár mélyebb információt kiáshat, mint egy HUMINT forrás.

- 10 év távlatában mennyire fog fejlődni a technológia ahhoz, hogy egyre kevesebb legyen az adatszivárgás?

A technológia folyamatosan fog fejlődni, amivel mindenképpen szükséges a lépést tartani, azonban többnyire ezek magas költségű licenzek, szolgáltatások keretében valósulnak majd meg, amelyet nem tud minden szervezet finanszírozni.

Annak ellenére is, hogy a technológia a védelemben is hatalmas fejlődésen megy keresztül, a jövőben is lesz adatszivárgás. A technológia mellett ebben a kulcs az emberi tényező lesz, hiszen a védelem egyik igen markáns tényezője az ember. Meg lehet zsarolni, tévesztetni, vagy más módszerekkel rá lehet venni a hibázásra. Ugyanakkor a technológiai és technikai fejlődés elérheti azt a szintet, amikor a humán eredetű veszélyek nagymértékben csökkenthetők, mert a viselkedés alapú védelem, azaz amikor a felhasználó eddigi tevékenységétől eltérő viselkedését automatizáltan figyeli/ellenőrzi nagy segítséget jelenthet majd.

Ami talán még érdekes lehet, hogy a hibrid hadviselés esetében a célok között jelenik meg a másik fél társadalmára való hatásgyakorlás, ahol értelemszerűen előtérbe fognak kerülni a nyílt infokommunikációs felületek, hiszen ezeket érik el a társadalom tagjai.

További radikális megoldást jelenthet még a teljes telefontilalom, amit az ukrán-orosz háborúban is bevezettek, azonban ez hosszútávon nem tartható cselekvési forma.

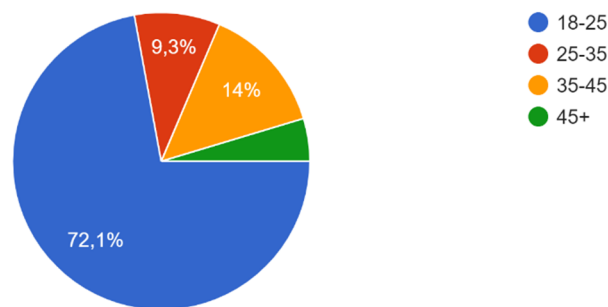
3.4 A kérdőíves felmérés kiértékelése, elemzése

Kutatási munkám zárásaként egy kérdőíves elemzést hajtottam végre a magyar katonák körében. Fő elemzési szempontom, hogy felmérjem milyen biztonságtudatossági attitűddel rendelkeznek. A kutatás online, Google Űrlapok segítségével valósult meg. A kutatás célja annak megvizsgálása, hogy a magyar katonák megfelelő biztonságtudatossággal rendelkeznek-e, azaz osztanak-e meg munkájukkal, szervezetükkel kapcsolatos információkat, alkalmazzák-e azokat a biztonsági megoldásokat, amelyekkel megakadályozhatók, hogy adataikat ellopják, azok kiszivároghassanak. Ebben az esetben nem csak a személyes adatokra gondolok, hanem minden olyan egyéb adatra is, amelyet munkájuk során kezelnek.

Elvárások:

Nagyobb spektrumban a 18-25 éves állomány volt a célpontom, hiszen ők lesznek azok, akik a jövőben parancsnokok lesznek és jobban kell figyelniük a megfelelő elektronikus biztonságra, és annak betartatására.

86 válasz érkezett be, melynek a megoszlási aránya, 65 férfi és 20 női kitöltő. Életkort vizsgálva is sikerült eleget tennem az elvárásaimnak, hiszen az alábbi arányok lettek:



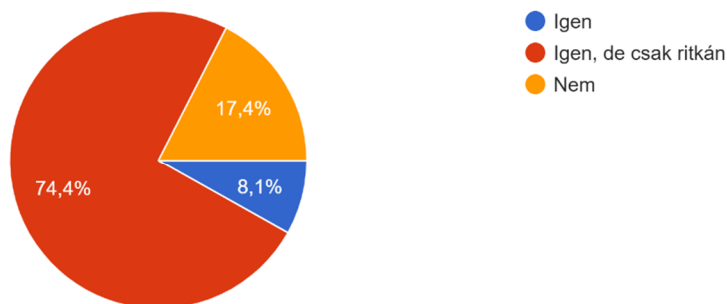
1. diagram Életkor szerinti megoszlás

Továbbiakban még arra voltam kíváncsi, hogy hány aktív felhasználóval rendelkezik az érintettek száma, és azok mennyien tudják biztonság tudatosan használni a különböző felületeket.

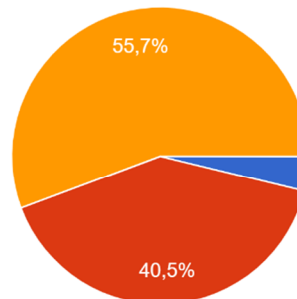
Általános megállapításaim:

A kérdőívet kitöltők közül mindenki használ legalább két közösségi média platformot, amelyek közül a legnépszerűbb a Messenger és a YouTube. A megkérdezettek közül jellemzően 8,1%-uk szokott rendszeresen posztolni közösségi média felületeken, és 17,4%-uk pedig elvétve. Ebből következtetett kérdésemben azt tudtam meg, hogy a felhasználók hány százaléka szokott Magyar Honvédséggel kapcsolatos információkat közzétenni. Ennek a száma

már jóval kevesebb, hiszen több mint a felére csökkent, amelynek az összehasonlítását a 2. és az 3. diagramon láthatjuk.



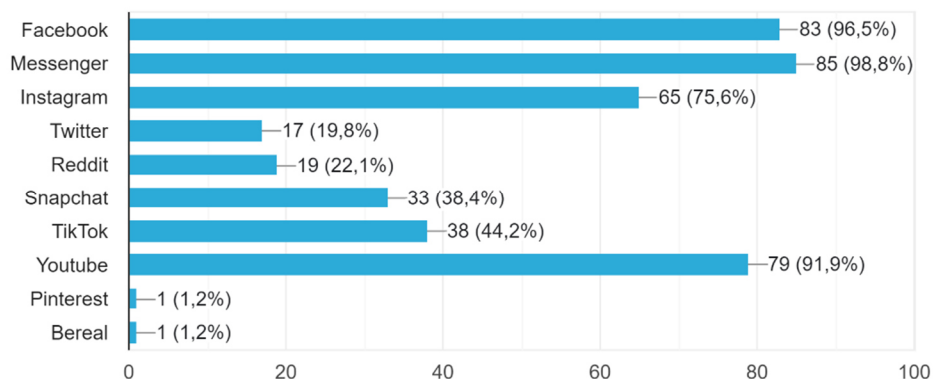
2. diagram Közösségi oldalakon posztolók



3. diagram Közösségi oldalakon honvédeggel kapcsolatban posztolók

A végső következtetett megállapításom az, hogy mivel sokan nem posztolnak, ezért jellemzően szórakozásra és információgyűjtésre használják a feltüntetett médiumokat, amely alapvetően megfelel már egy kezdeti OSINT tevékenységnek, még ha az nem is feltétlenül tudatos.

A 4. számú diagram azt szemlélteti, hogy a jellemző platformok, amelyeken a katonák leginkább tájékozódnak vagy kommunikálnak hogyan oszlanak meg:



4. diagram Közösségi médiák használatának megoszlása

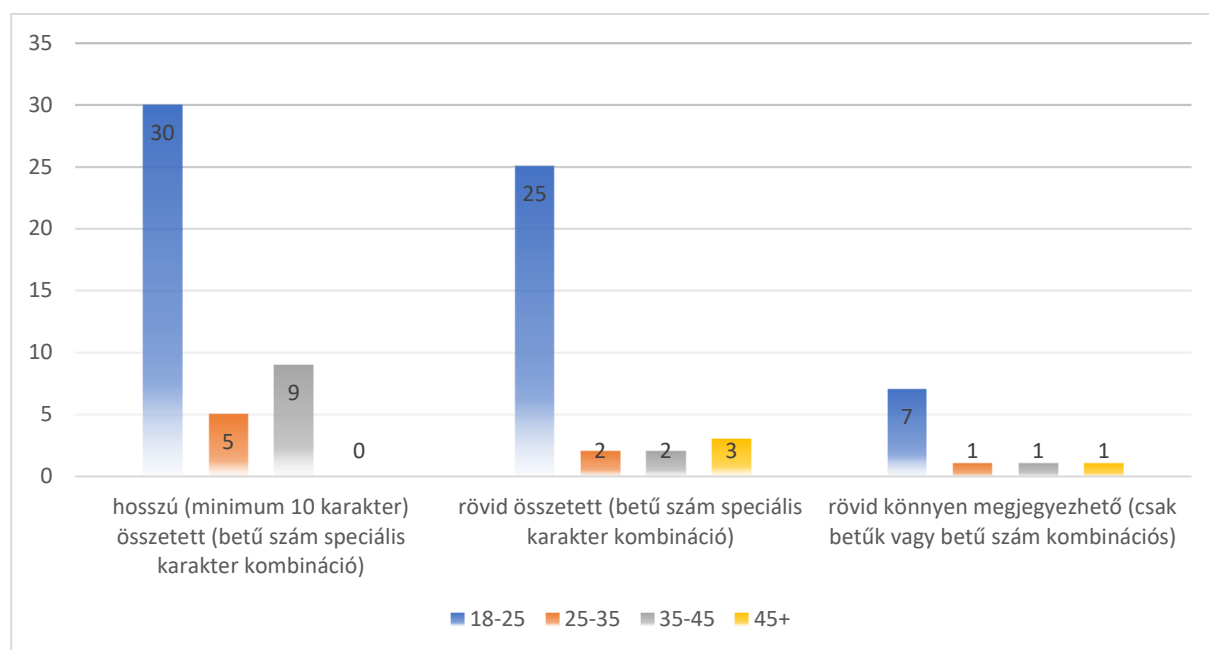
Elemzésem alapján rájöttem, hogy a fiatalabb korosztály van jelen a legtöbb közösségi oldalon és közülük az összes megkérdezett legalább három médián van jelen és használja. Legnépszerűbb ezek közül a 4. diagramon is kitűnő: Facebook, Messenger és a YouTube, de populáris még ebben a korosztályban az Instagram, Snapchat, Reddit és a TikTok is, amely a többi korosztályban már nincs nagy számban jelen.

Kérdéseim között volt az is, hogy mennyien vettek részt biztonságtudatossági előadásokon, és a válaszadók 67,4%-a igennel válaszolt, amely jó kiindulási érték, de véleményem szerint

minden katonának legalább egyszer részt kell venni egy ilyen a kockázatok csökkentése végett.

Negatív véleményként konstatálnám azt, hogy biztonságtudatossági előadáson részt vettek száma ellenére is voltak olyan fiatal korosztályúak, akik politikai megnyilvánulásokat tesznek ki a közösségi médiába, hiszen katonaként tilos bármilyen párt mellett nyíltan állást foglalni.

Rátérve a jelszavak fontosságára szemléltetem az ehhez kapcsolódó első kimutatásomat, amely a jelszóösszetételek felosztását jellemezi és az 5. számú diagramon látható.

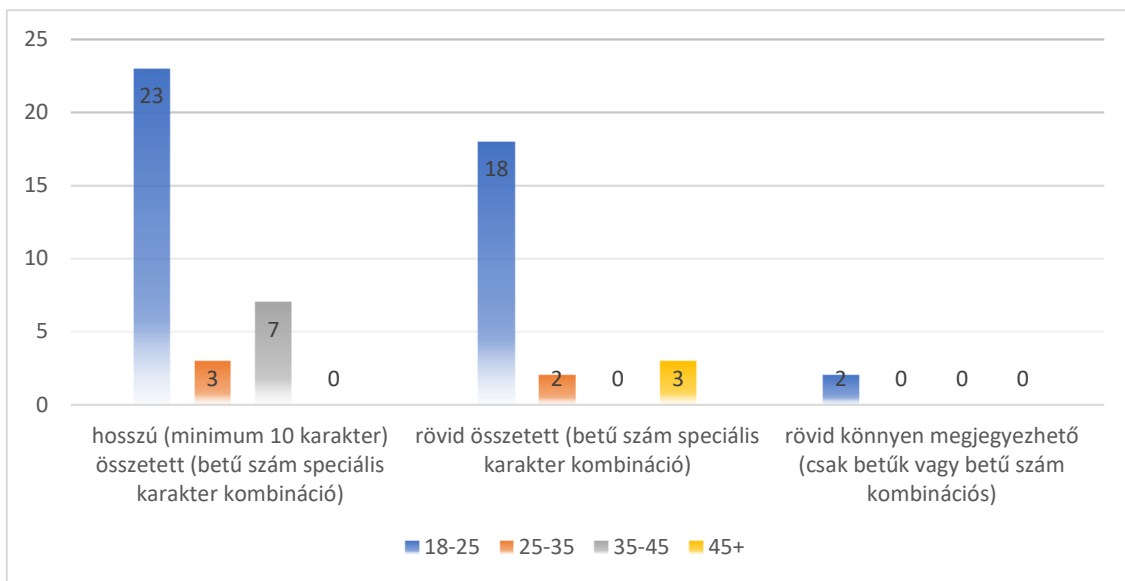


5. diagram Jelszóösszetételek a különböző korcsoportoknál

Három csoportba osztottam a jelszavak erősségét; hosszú (hosszú (minimum 10 karakter) összetett (betű szám speciális karakter kombináció), rövid összetett (betű szám speciális karakter kombináció), rövid könnyen megjegyezhető (csak betűk vagy betű szám kombinációs).

Biztonságtudatossági szempontból pozitívan bírálok az értékeket, hogy a legtöbben hosszú jelszavakat használnak és elhanyagolható számban vannak jelen a rövid jelszó használók.

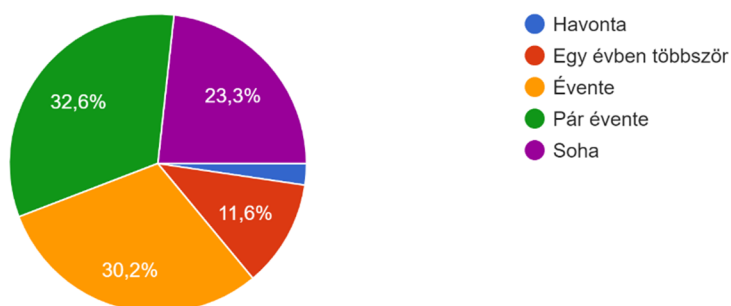
Ezek után azt is megvizsgáltam, hogyan oszlik meg akkor az arány, ha csak azokat veszem alapul, akik biztonságtudatossági előadáson részt vettek.



6. diagram Jelszóösszetételek a biztonságtudatossági előadáson részt vett személyeknél

A 6. számú diagramon látható, hogy akik részt vettek, azoknál megmutatkozik, hogy elhanyagolható a rövid egyszerű jelszavak száma, de körülbelül azonos szinten van a hosszú és a rövid összetett jelszavak száma, amelynél inkább a hosszúnak kéne előnyt élvezni. Megvizsgáltam azt is, hogy a rövid összetett jelszavakat használók milyen gyakran változtatják az adott jelszót és az eredmény itt is a sebezhetőséget támasztja alá, mert az a jellemző, hogy nagyon ritkán vagy szinte soha nem cserélik le a jelszavukat.

Jelszócsereére visszatérve, a 7. számú diagram bemutatja, hogy milyen gyakran szokták a jelszavukat cserélni a megkérdezettek. Szinte egyforma az eloszlás a 'pár évente' és az 'évente' között, de csalódásként tapasztalom azt, hogy egész nagy részt kitesz az a csoport is, amely soha nem változtatja meg a jelszavát, ezzel nagy kockázatot jelentve.

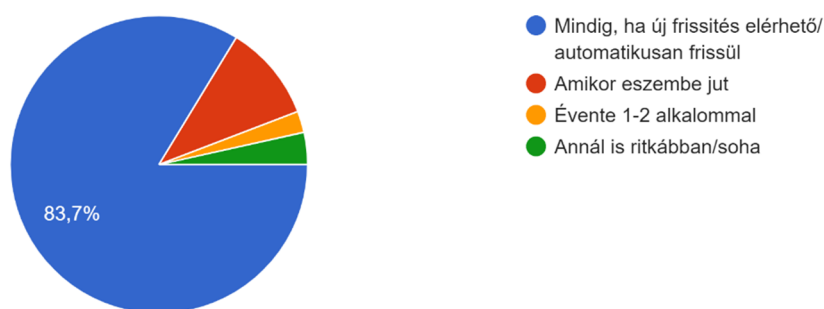


7. diagram Jelszavak megváltoztatásának aránya

Ezt tovább tárgyalva próbálok összefüggést keresni azzal, hogy a vizsgált személyek egy helyen többször is használják-e a jelszavukat.

Ugyanolyan arányban van azoknak a száma is, akik soha és akik szinte mindenhol egy jelszót használnak, de 65,1% azoknak az aránya, akik csak néhány helyre használják ugyanazt a jelszót. Vizsgálni kívántam ugyanakkor, hogy ismerik-e az emberek a jelszószerkezetet, 15,1%-uk használja is, akik viszont nem is ismerik a jelszószerkezetet, azok nagy arányban használnak mindenhol egy jelszót, vagy legalábbis több helyre. És megvan az összefüggés a között, hogy akik nem ismerik vagy nem használnak jelszószerkezetet, azok többsége papírra, vagy elektronikus jegyzetbe írja le a jelszavait.

Rátérve az eszközökre több kérdést is vizsgáltam ebben a témában. Az egyik legfontosabbnak tartottam a szoftverfrissítés fontosságát, a 8. számú diagram pedig megmutatja, mikor frissítik a felhasználók az okoseszközeiket.

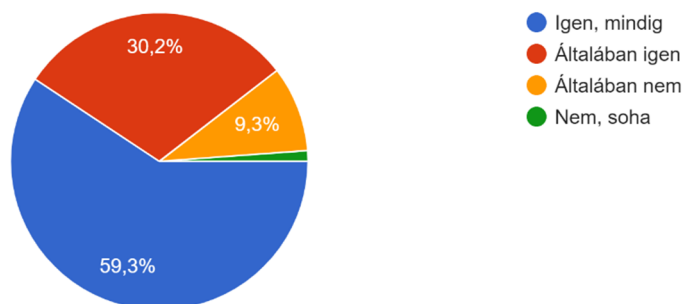


8. diagram Szoftverfrissítések gyakorisága

Szerencsésnek tartom megoszlást, mert a szoftverfrissítések által, többnyire javíthatók a hibák és a sérülékenységek, ezzel jobban védve az adatainkat.

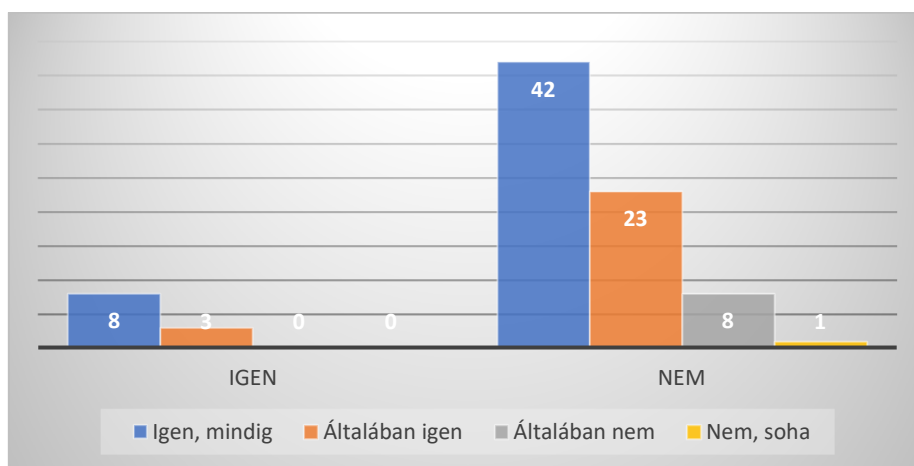
Vitatott állítás ugyan, de a véleményem szerint a biztonságosabb IOS mobil operációs rendszer nem aratott sikert a válaszadók körében, így előnybe került az Android rendszer, ezzel tovább növelve a sérülékenységek kockázatát. Ugyanígy a számítógépes operációs rendszereknél is előnyben van a Microsoft Windows aránya, mint a MacOS-é.

Vizsgáltam még a kettős hitelesítéssel kapcsolatos kérdéseket a banki és a pénzügyi szolgáltatásoknál, amelynek eredménye a 9. számú diagramon található. Itt is megosztó az arány, mondhatni meglepő, - mert mire másra nem vigyáznánk a legjobban, mint a pénzünkre.



9. diagram Kettős hitelesítés használata a banki és pénzügyi alkalmazásoknál

Ezzel összefüggve elemeztem, hogy azok, akik nem mindig használnak kettős hitelesítést voltak-e már részesei adatlopásnak, ennek eredményét a 10. számú diagram szemlélteti.

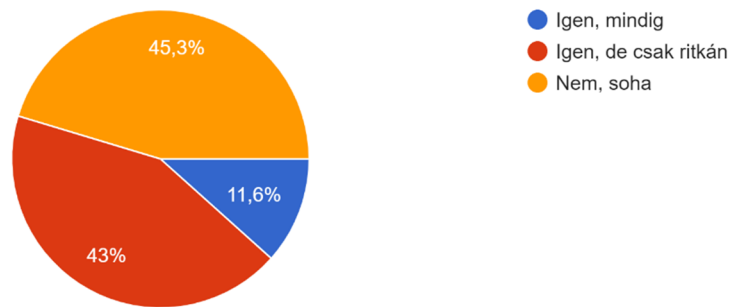


10. diagram Adatlopás és a kettős hitelesítés aránya

Meglepődve tapasztaltam azt, hogy azoknak volt már adatlopásuk, akik mindig és általában szoktak használni kettős hitelesítést. Így arra vonatkoztatok, hogy azért kezdtek el ilyen hitelesítést használni, hogy továbbiakban megvédjék az adataikat.

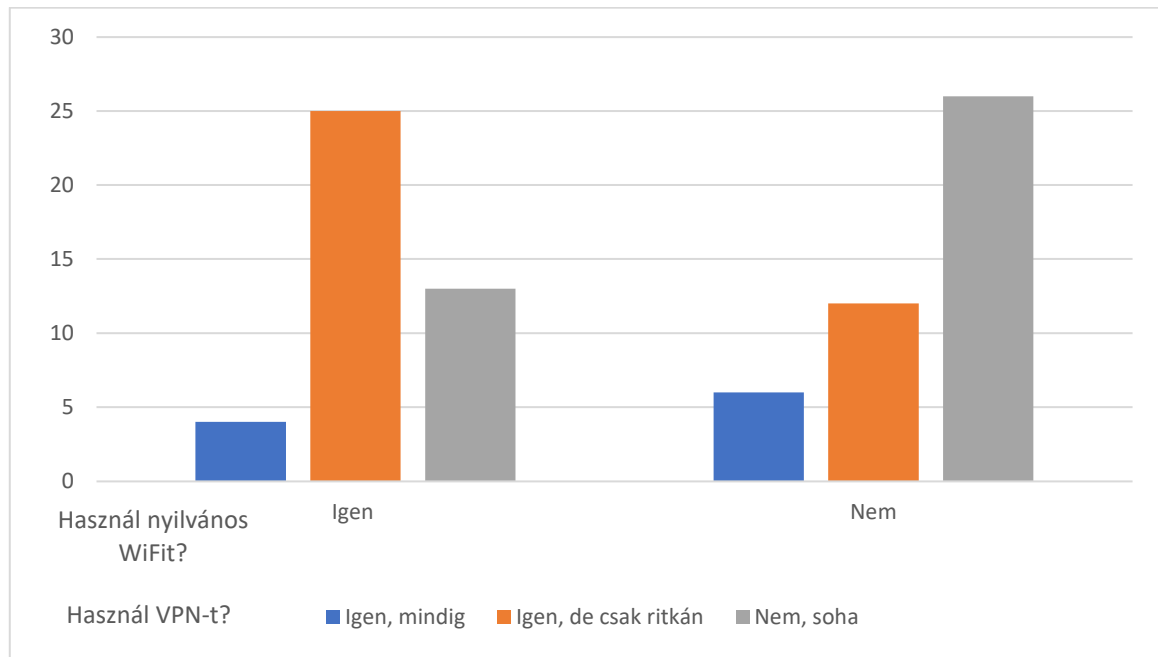
Következő vizsgálati pontomban pedig a VPN használatát vettem alapul. Miért is jó a VPN? „Alapvetően a VPN lehetővé teszi, hogy az adataid titkosított kapcsolaton keresztül az eszközeidről az internet egy másik pontjára – valószínűleg egy másik országba – jussanak el, majd onnan a nyilvános internetre. Egy jó szolgáltatás titkosítja és védi az adatokat és biztosítja, hogy a származási és eszközadatok is rejtve maradjanak”³⁸ Merül fel a kérdés, hogy akkor hányan is használnak VPN-t?

³⁸ <https://officetools.hu/miert-erdemes-vpn-t-hasznalni-az-elonyok-es-hatranynok-amelyekrol-tudnod-kell/>; letöltve: 2022.11.12.



11. diagram VPN-t használók megoszlása

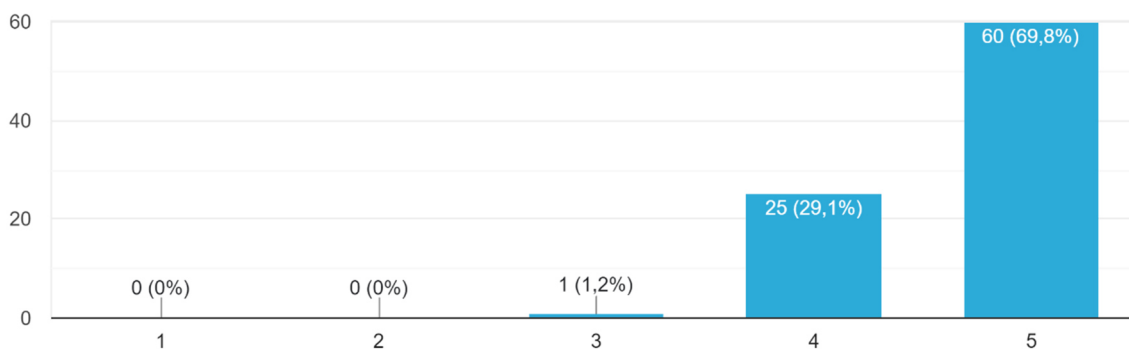
Elvárásom szerint, nem gondoltam volna, hogy ilyen magas lesz a szám, a használók körében, és azoknak az aránya, akik egyáltalán nem használnak 50% alatt lesz (11. számú diagram). Továbbiakban viszont azt is elemeztem, hogy a nyílt WiFi hálózatot használók közül, mennyien alkalmazzák továbbra is a VPN-t.



12. diagram Nyilvános WiFi és VPN-t használók aránya

A 12. számú diagram is mutatja, hogy azok, akik használnak VPN-t kevesebb aránnyal használnak nyilvános WiFi-t, és így van azoknál is, akik egyáltalán nem használnak VPN-t.

Utolsó elemzési szempontom pedig egy nyílt kérdéssel zárult, amelyben arra kérdeztem rá, hogy mennyire fontos a katonák biztonságtudatossága.



13. diagram Mennyire tartja fontosnak a katonák biztonságtudatosságát? (5-kiemelten, 1-egyáltalán nem)

A 13. számú diagramon egyértelműen látható, hogy szinte az összes megkérdezett fontosnak tartotta a biztonságtudatosság kérdését, több olyan válasz érkezett miszerint, a biztonságtudatosságnak és a fokozott óvatosságnak elengedhetetlennek kell lennie a szervezetben belül dolgozóknak, mivel speciálisabb munkakört látnak el.

És mivel a Honvédség - ahogy a nevében is benne van - elsődlegesen a haza védelmét szolgálja, annak szerves része, hogy megteremtse a biztonságot is, ehhez pedig a katonáknak individuálisan is hozzá kell járulniuk és nem csak fizikai keretek között, továbbá jellemzően érzékeny adatokhoz férnek hozzá, és nagyon sokszor kritikus információs infrastruktúrákon dolgoznak.

Ugyanakkor a kiberhadviselés korában bizonyos szint felett tehetetlen egy átlagos katona bizonyos támadásokkal, veszélyekkel szemben, hiszen az a magasfokú képzettség, szakértelem, amikkel ezen hackerek rendelkeznek, kivédhetetlen számára.

Alfejezetem zárásaként állíthatom, hogy a fiatalabb korosztály zöme már kapott biztonságtudatossági képzést, amit a jövőben remélem még többször és még több katona számára továbbítanak. Véleményem szerint, ennél többet nem tud tenni maga a honvédség, mert a radikálisabb módszerek (pl. telefonszám/Internet tilalom) nem mindig célravezetőek.

Ugyanakkor a fiatalok köre több közösségi oldalon is jelen van, nagyobb kockázatot és sebezhetőséget vonva maga után. Remélem a jövőben az fejlődő adatvédelem és mesterséges intelligencia alkalmazásával még biztonságosabban tudunk eljárni az értékeink megóvásába.

III. Összegzés

Dolgozatom összegzéseként leírhatom, hogy sikerült választ találnom a kutatási kérdéseimre, felépítenem egy olyan dolgot, amely tematikusan meghatározza az összefüggéseket az OSINT és a hadsereg között.

Tisztázom azt az állítást, hogy a mai technológia és energiaellátás nélkül a fent felsorolt technológiák és eszközök nem is léteznének, és a megfelelő kommunikációs eszközök az alappillérei az elektronikus hírszerzésnek egyaránt.

Az első részben bemutatam az OSINT általános jellemzőit, pozitív és negatív hatásait, amelyek a későbbi fejezetekben is említésre kerültek, továbbá a bizonyos keresőmotorok és OSINT eszközök kerültek ismertetésre.

A második fejezetemben szűkítettem a témakört és az etikus hackelés témakörét boncolgatva próbáltam a hangsúlyt fektetni a megfelelő védelem kialakítására, hiszen az ilyen szakemberek segítségével könnyebben meg tudjuk a szervezetünk adatait védeni, ezáltal elkerüljük azt adatszivargást és az ellenség se tud minket 'OSINT-olni'. Viszont, ha megtörtént az előbb említett szivargás, akkor melyik médiumon találhatnánk róla információkat? Ezért is szerettem volna néhány szót szólni a Twitterről, hiszen véleményem szerint itt található meg az egyik legtöbb nyílt információ a kiszivárgott adatokról, legyenek azok negatív vagy pozitív vonzatúak. És ha a Twitter nem is lenne elég, akkor számos különböző eszközzel tudhatunk meg szinte bármit a kijelölt célpontokról, és már katonai témára asszociálva emeltem ki a geolokációs keresés fontosságát, hiszen – ahogy a dolgozatomban is leírtam – a parancsnokokat kielégítő két legfontosabb információ igénye, az ellenségről és a terepről szerzett információk.

Rátérve a tanulmányom utolsó szegmensére, szinténre kerül a fő témám a katonaság és az OSINT összefonódása, és hogy ez a jelen időszakban is mennyire számottevő kérdéskör. Elsősorban a nemzetbiztonsági szolgálatok mentén kerestem az irányt, hiszen ők a fő mozgatórugói egy állam információszerzésének.

Ezután érintettem a jelen időnk egyik fő konfliktusát az orosz-ukrán háborút, reflektálva arra, hogy az OSINT mennyire befolyásolja a háború kimenetelét, és mennyire elterjed a híre az egész világon szinte másodpercről másodpercre, ezt nevezhetjük egy technológiai csodának is – például a hidegháború eszközeihez képest, ami szinte pár 10 éve volt -, ugyanakkor sokkal nagyobb technikai problémákkal és változó helyzetekkel kell szembenéznie a mai kor parancsnokainak. Ezért is kívántam meginterjúvolni hazánk felsővezetőit, akik tapasztalatukkal és hozzáértésükkel tudtak válaszolni a feltett kutatási kérdéseimre.

A végrehajtó állomány bevonásával pedig egy kérdőívet készítettem, hogy felmérjem a magyar katonák biztonságtudatosságát, nagyobb szórásban a 18-25 éves korosztályt vettem alapul, hiszen ők lesznek a jövő vezetői.

A hipotéziseket elemezve a következő állapításokra jutottam; az orosz-ukrán háború egy kitűnő példa volt az 1. számú hipotézisem alátámasztására, hiszen ott is megnyilvánult, mennyire meg tud változni egy hadszíntér, ha nem kívánt információ kerül fel az internetre. Hasonlóképpen vélekedek a 2. számú hipotézisemmel kapcsolatban is, hiszen több olyan példát ismerhettünk meg mi is a közösségi médiából, amely alátámasztotta, hogy bizonyos csapatok úgy mérték csapást az ellenségre, hogy előtte a közösségi médiából tájékozódtak. A 3. számú hipotézisemet viszont nem tudom sem alátámasztani, sem megcáfolni, inkább korosztályokra bontva elemezni. A fiatalabb korosztály jellemzően rendelkezik a megfelelő biztonságtudatossági ismervekkel, viszont az idősebb korosztályra ez már annyira nem jellemző. Többnyire ők is ismerik a megfelelő biztonsági megoldásokat, csak nem feltétlenül tudják vagy szeretnék őket használni.

Az előző Intézményi Tudományos Diákköri dolgozatomnak eleget téve, tovább fejlesztettem a tudásom és a hidegháború vívmányaiból megvizsgáltam a jelenünk egyik technológiai alapkövét remélem, hogy a jövőben a két dolgozathból szerzett tapasztalatot és információt még tovább tudom majd ápolni.

IV. Felhasznált irodalmak, folyóiratok

- Deák Veronika: A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során – Hadmérnök, XIII. évfolyam 3. szám – 2018. szeptember 393. oldal
- Dobák, Imre: OSINT – Gondolatok a kérdéskörhöz, NEMZETBIZTONSÁGI SZEMLE (ONLINE) 7 : 2 pp. 83-93. , 11 p. (2019)
- Nemzetbiztonság elmélete a közszolgálatban - szerkesztette: Resperger István, Dialóg Campus Kiadó Budapest (2018), III. Az információgyűjtésről általában (Dobák Imre), 99. oldal
- Nemzetbiztonsági alapismeretek - szerkesztette: Resperger István, Dialóg Campus Kiadó Budapest (2018), A nemzetbiztonsági szolgálatok (Dezső Lajos), III. fejezet, 100. oldal
- S. Mittal, P. K. Das, V. Mulwad, A. Joshi and T. Finin, "CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities," 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2016, pp. 860-867, doi: 10.1109/ASONAM.2016.7752338.
- Szabó Károly: Az OSINT – Gondolatok a tevékenységről és az alkalmazás közegéről; NEMZETBIZTONSÁGI SZEMLE 7. évfolyam (2019) 2. szám 68–82. • doi: 10.32561/nsz.2019.2.6
- T. Aichner és mtsai., „Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019”, *Cyberpsychology, Behavior, and Social Networking* 24, sz. 4 (2021): 215–22, <https://doi.org/10.1089/cyber.2020.0134>.

Internetes források

- <https://bluebird.hu/mennyit-ernek-az-etikus-hackerek/>; letöltve: 2022.11.05.
- <https://creepy.en.softonic.com/>; letöltve: 2022.11.08., fordította: szerző
- <https://hu.wikipedia.org/wiki/Malware>; letöltve: 2022.11.06.
- <https://maphub.net/Cen4infoRes/russian-ukraine-monitor>
- <https://officetools.hu/miert-erdemes-vpn-t-hasznalni-az-elonyok-es-hatranyok-amelyekrol-tudnod-kell/>; letöltve: 2022.11.12.
- <https://restofworld.org/2022/osint-viral-ukraine/>; letöltve: 2022. 05. 26. fordította: szerző
- <https://southfront.org/us-delta-program-used-by-ukrainian-military-command-hacked-by-joker-dpr-hacker-team/>; letöltve: 2022. 11. 10., fordította: szerző

- <https://usnwc.libguides.com/c.php?g=494120&p=3381599>; letöltve: 2022. 11. 06., fordította: szerző
- <https://www.adobe.com/hu/creativecloud/file-types/image/raster/exif-file.html>; letöltve: 2022.11.10.
- <https://www.bellingcat.com/news/2022/02/27/follow-the-russia-ukraine-monitor-map/>, letöltve: 2022.11.07., fordította: szerző
- <https://www.expert.ai/blog/advantages-disadvantages-open-source-intelligence/>; letöltve: 2022. 10. 13.; fordította: szerző
- <https://www.hacktify.eu/>; letöltve: 2022.11.05.
- <https://www.mnemonic.io/company/>; letöltve: 2022.11.07., fordította: szerző
- <https://www.osintme.com/index.php/2022/01/31/osint-dojo-student-challenge-geolocation-puzzles/>; letöltve: 2022.11.10., fordította: szerző
- <https://www.techopedia.com/definition/15450/gray-hat-hacker>; letöltve: 2022.11.05.; fordította: szerző

Ábrajegyzék

- CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=299708>; letöltve: 2022.11.10
- Deák Veronika: A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során – Hadmérnök, XIII. évfolyam 3. szám – 2018. szeptember 393. oldal
- <https://osintframework.com/>; letöltve: 2022. 10. 13.
- <https://southfront.org/us-delta-program-used-by-ukrainian-military-command-hacked-by-joker-dpr-hacker-team/>; letöltve: 2022.11.10.
- <https://www.bellingcat.com/news/2022/02/27/follow-the-russia-ukraine-monitor-map/>; letöltve: 2022.11.07.
- <https://www.osintme.com/index.php/2022/01/31/osint-dojo-student-challenge-geolocation-puzzles/>; letöltve: 2022.11.10.,
- S. Mittal, P. K. Das, V. Mulwad, A. Joshi and T. Finin, "CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities," 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2016, pp. 860-867, doi: 10.1109/ASONAM.2016.7752338.