Doktori (PhD) értekezés tervezet

Fábri Barbara

2026

NEMZETI KÖZSZOLGÁLATI EGYETEM

Katonai Műszaki Doktori Iskola

Fábri Barbara:

A közösségi média alkalmazási lehetőségei az információs- és kibertér műveletekben

Doktori (PhD) értekezés tervezet

Témavezető:

Dr. Kovács László vőrgy., DSc, egyetemi tanár

……...

Budapest, 2026

Tartalom

BEVEZETÉS

A 21. század folyamatosan változó és egyre komplexebb biztonsági környezetében a digitális technológiák rohamos fejlődése alapvetően formálja a hadviselés természetét. Az információs műveletek és a kibertérben zajló hadviselés új kihívások elé állítják a katonai és nemzetbiztonsági szerveket, miközben egyre nagyobb szerepet kapnak a közösségi média által kínált lehetőségek és veszélyek. A közösségi média elterjedése nem csupán a hétköznapi kommunikációt alakította át, hanem radikálisan új dimenziókat nyitott a katonai műveletekben, ahol az információ hatalom, és az időben történő információs fölény elérése döntő szerepet játszik.

A digitális technológiák elterjedése új lehetőségeket nyitott meg a katonai szervezetek számára, különösen a tájékoztatás és kommunikáció terén. Ugyanakkor ezek az eszközök számos kiberbiztonsági, morális és etikai kihívást is hordoznak, amelyek kezeléséhez átfogó stratégiákra van szükség.

A közösségi média alkalmazása a katonai szervezetek számára olyan lehetőségeket kínál, amelyek segítségével hatékonyan terjeszthetők az információk és javítható a nyilvánossággal való kapcsolattartás. A platformok rugalmassága lehetővé teszi a gyors reagálást, a széleskörű tájékoztatást és a célzott üzenetek eljuttatását. Például a katonai tájékoztatási kampányok során a közösségi média eszközként szolgálhat a polgári lakosság informálására vészhelyzetek idején, valamint a katonai tevékenységek átláthatóságának elősegítésére.

Ugyanakkor a közösségi média felületein megosztott üzenetek értelmezése jelentős mértékben függ a célközönség kulturális és politikai kontextusától, ami bonyolíthatja a kommunikációs folyamatot. Az üzeneteket könnyen félreértelmezhetik, manipulálhatják vagy rosszindulatú célokra használhatják, amely növeli az információs káosz kockázatát. A katonai szervezeteknek ezért stratégiákat kell kidolgozniuk az üzenetek hatékony közvetítésére és a negatív hatások minimalizálására.

Tudományos probléma megfogalmazása

A kutatás alapgondolata, hogy a közösségi média nem csupán kommunikációs eszköz, hanem **stratégiai jelentőséggel bíró platform**, amelyet állami és nem állami szereplők egyaránt alkalmazhatnak tájékoztatási, befolyásolási, sőt offenzív műveleteik során. A katonai és kiberbiztonsági dimenziók közötti kapcsolat új kihívásokat jelent a hadseregek

és kormányok számára, különösen akkor, amikor a közösségi média szabályozatlansága és globális elérhetősége révén az információs műveletek egyre nagyobb hatékonysággal érhetnek el széles közönségeket. Fontos kiemelni, hogy **a közösségi média használata a katonai műveletekben számos kiberbiztonsági kockázatot rejt magában.** Az ellenséges szereplők kihasználhatják a platformokat érzékeny információk megszerzésére, hamis hírek terjesztésére vagy közvetlen kibertámadások végrehajtására. A közösségi médián keresztül végzett adathalászat és álhírterjesztés nemcsak a katonai személyzet, hanem a polgári lakosság körében is zavart okozhat, amely stratégiai előnyt jelenthet az ellenfél számára.

Az ilyen fenyegetések elleni védekezés érdekében a katonai szervezeteknek fejlett kiberbiztonsági protokollokat kell alkalmazniuk. Ez magában foglalja a biztonsági szoftverek folyamatos frissítését, a személyzet képzését az adathalászat felismerésére és a közösségi média használatának korlátozását olyan helyzetekben, amikor az OPSEC (operation security) szempontok kiemelten fontosak. Továbbá a mesterséges intelligencia alapú rendszerek, például a deepfake-detektorok alkalmazása jelentős előrelépést jelenthet a kiberbiztonsági kihívások kezelésében.

A közösségi média katonai műveletekben történő használata számos morális és etikai dilemmát is felvet. Az információs műveletek során alkalmazott propaganda és manipuláció kérdése központi jelentőségű, mivel ezek befolyásolhatják a közvéleményt és az ellenség morálját. Azonban a határok átlépése az igazságos és etikus kommunikáció terén aláásható a katonai szervezetek hitelességét, hosszú távon pedig hátrányos következményekkel járhat.

Az etikai kihívások kezeléséhez elengedhetetlen az átláthatóság és az igazságosság elvének betartása. A katonai szervezeteknek törekedniük kell arra, hogy információikat a lehető legpontosabban közvetítsék, miközben biztosítják a nemzetbiztonsági érdekek védelmét. Az etikai normák betartása nemcsak a közvélemény bizalmának megőrzése szempontjából fontos, hanem a katonai műveletek legitimációját is erősíti.

A közösségi média közvéleményre gyakorolt hatását is fontos vizsgálni, különösen a katonai műveletek kontextusában. A platformok lehetőséget biztosítanak arra, hogy a katonai szervezetek közvetlenül kommunikáljanak a lakossággal, ezzel formálva a konfliktusok percepcióját. Ugyanakkor az ellenfelek számára is teret adnak a

dezinformációs kampányok végrehajtására, amelyek célja a közvélemény manipulálása és a politikai instabilitás előidézése.

A közösségi média az információs műveletek kulcsfontosságú eszközévé vált, amelyet mind állami, mind nem állami szereplők hatékonyan használnak. Az ilyen típusú műveletek célja gyakran az ellenség moráljának csökkentése, valamint a saját erőfölény demonstrálása. A közvélemény befolyásolása azonban kettős élű fegyver, amely nemcsak előnyöket, hanem súlyos kockázatokat is hordozhat.

A katonai személyzet megfelelő képzése elengedhetetlen a közösségi média hatékony és biztonságos használatához. A digitális kompetenciák fejlesztése, valamint a közösségi média veszélyeinek és lehetőségeinek alapos ismerete jelentős mértékben hozzájárulhat a sikeres műveletekhez. A katonákat fel kell készíteni arra, hogy felismerjék és elkerüljék a manipulációs technikákat, valamint hatékonyan tudjanak reagálni az információs támadásokra.

Ezen túlmenően fontos a közösségi média alkalmazásának stratégiai szintű optimalizálása. Ez magában foglalja az olyan irányelvek kidolgozását, amelyek meghatározzák a platformok használatának korlátait és lehetőségeit, miközben biztosítják a nemzetbiztonsági érdekek védelmét. Az innovatív technológiák és a folyamatos képzési programok bevezetése jelentős előnyöket kínálhat a közösségi média katonai műveletekben való alkalmazásában.

A közösségi média használata a modern katonai műveletekben egyszerre kínál lehetőségeket és jelent kihívásokat. A tájékoztatásban és kommunikációban betöltött szerepe forradalmi változásokat hozott, ugyanakkor kiberbiztonsági, etikai és stratégiai szempontból is új kérdéseket vet fel. A hatékony alkalmazás érdekében elengedhetetlen az átfogó szabályozás, a képzés és a folyamatos innováció, amely biztosítja, hogy a közösségi média eszközei a katonai szervezetek előnyére váljanak, miközben minimalizálják a kockázatokat.

Hipotézisek

Az információs műveletek vizsgálata során több hipotézist állítottam fel, amelyek a közösségi média szerepét, hatékonyságát és kockázatait elemzik a modern katonai és kiberkörnyezetben. A megfogalmazott hipotéziseket az alábbiakban részletezem:

H1. A közösségi média hatékony eszközként alkalmazható az információs műveletek során.

H2. Az információs műveletek és a közösségi média egyaránt szabályozatlan mind nemzetközi jogi, mind nemzeti jogi szinten.

H3. A közösségi média önálló eszköz a stratégiai kommunikációban.

H4. A közösségi média a befolyásolás mellett offenzív kibertéri eszközként is alkalmazható.

Kutatási célok

A fent megfogalmazott hipotézisekkel összhangban az alábbi kutatási célokat fogalmaztam meg, amelyek a közösségi média szerepét és hatásait vizsgálják az információs műveletek kontextusában:

K1. Annak vizsgálata, hogy a közösségi média, mint az információs műveletek új eszköze önállóan is megállja-e a helyét.

A közösségi média az információs műveletekben potenciálisan önálló eszközként is alkalmazható, mivel lehetőséget kínál az üzenetek gyors, széles körű és célzott eljuttatására. Állami és nem állami szereplők egyaránt kihasználják ezen platformok adottságait az információs térben való beavatkozásra, különösen az információs káosz fenntartása, a percepciók manipulálása és a közönség befolyásolása érdekében. A közösségi média sajátosságai – így a valós idejű kommunikáció és az interaktív tartalomterjesztés – felvetik annak lehetőségét, hogy az információs műveletek végrehajtásában akár autonóm eszközként is működjön. A disszertációm elsődleges kutatási célja e lehetőség érvényességének és hatékonyságának kritikai vizsgálata.

K2. A közösségi média szerepének vizsgálata az információs környezet destabilizációjában, különös tekintettel az információs túltelítettség és a dezinformációs folyamatok előidézésére.

Állami és nem állami szereplők egyaránt kihasználják a közösségi média platformjait az információs környezet destabilizálására, különösen a dezinformáció célzott terjesztésén keresztül. E gyakorlatok jelentős hatást gyakorolhatnak a politikai döntéshozatalra és a katonai stratégiák formálására, mivel a digitális térben előidézett percepciótorzítások közvetlenül befolyásolhatják a közvéleményt, valamint a konfliktusok lefolyásának dinamikáját. Az információs műveletek központi célja az információs fölény megszerzése és a célcsoportok kognitív befolyásolása, amelyet a közösségi média technológiai sajátosságai – például a gyors terjedés, algoritmikus célzás és interakcióorientáltság – hatékonyan támogatnak.

K3. Az információs műveletek és a közösségi média szabályozási kereteinek hiányosságai és azok hatásainak vizsgálata a nemzetbiztonsági, politikai és társadalmi kockázatok tükrében.

Az információs műveletek és a közösségi média platformok szabályozása mind nemzetközi, mind nemzeti szinten számos stratégiai és jogszabályi hiányossággal küzd. E két terület összefonódása új típusú kihívásokat eredményez az információs térben, különösen a dezinformáció, a pszichológiai befolyásolás, valamint a demokratikus intézmények destabilizációjának lehetősége kapcsán. A jelenlegi nemzetközi jogi normák – beleértve a nemzetközi humanitárius jogot és a szuverenitás elvét – nem nyújtanak koherens válaszokat az államok és nem állami szereplők által végrehajtott információs műveletek jogszerűségének kérdésében. Ezzel párhuzamosan a nemzeti jogrendszerek is gyakran elmaradnak a technológiai fejlődés és a közösségi média működésének komplexitása mögött, ami jogalkalmazási és szabályozási vákuumot teremt. Ez a hiányos szabályozási környezet jelentős nemzetbiztonsági kockázatokat hordoz, különösen a kritikus infrastruktúrák védelme, a politikai stabilitás megőrzése, valamint a társadalmi kohézió fenntartása szempontjából.

K4. A közösségi média alkalmazhatóságának vizsgálata az információs és döntéshozatali fölény elérésének eszközeként, különös tekintettel az információs műveletek során betöltött stratégiai szerepére.

A közösségi média a modern információs műveletekben nem csupán kommunikációs platformként, hanem stratégiai kapacitásként is funkcionál, amely hozzájárulhat az információs és döntéshozatali fölény megszerzéséhez. Valós idejű információközvetítő képességei, valamint a célzott, algoritmusvezérelt üzenetirányítás

révén elősegíti a műveleti narratívák kontrollját és az események percepció általi alakítását. Különösen fegyveres konfliktusok esetén nyílik lehetőség arra, hogy katonai és politikai szereplők saját értelmezési kereteiket érvényesítsék a közvéleményben, ezáltal információs dominanciát építve ki. A közösségi média tehát eszközként jelenik meg a hadviselés új dimenziójában, ahol az információ feletti ellenőrzés közvetlenül hat a döntéshozatali folyamatokra is.

K5. Alátámasztani, hogy a közösségi média közvetlen veszélyt jelent a műveleti biztonságra.

A közösségi média nem csupán információs és befolyásolási célú eszközként funkcionál, hanem potenciális platformot biztosít a kibertérben végrehajtott, támadó jellegű műveletek számára is. A felhasználói interakciók és nyílt kommunikációs felületek lehetőséget teremtenek különböző technikák – például adathalászat, hamis profilok létrehozása vagy célzott *social engineering* – alkalmazására, amelyek közvetlen fenyegetést jelentenek a műveleti biztonságra (OPSEC). E gyakorlatok különösen megnehezítik az érzékeny információk védelmét, valamint a személyi és szervezeti biztonság fenntartását. A közösségi média továbbá elősegítette új, nem hagyományos kibertéri szereplők megjelenését is, akik képesek befolyásolni a konfliktusok dinamikáját és érdemben hozzájárulni az információs műveletek sikerességéhez, így átalakítva a modern hadviselés szerkezetét és szereplői körét.Ezek a kutatási célok biztosítják az elméleti és gyakorlati keretet a közösségi média katonai és kiberbiztonsági alkalmazásának mélyreható vizsgálatához.

A fentebb bemutatott kérdések vizsgálata érdekében a disszertációban többféle kutatási módszer is alkalmazásra kerül. Az értekezés kvalitatív kutatási módszereken alapul, és elsődlegesen szakirodalmi elemzésre támaszkodik, amely magában foglalja a legfrissebb tanulmányok, akadémiai publikációk és esettanulmányok áttekintését. A kutatás célja, hogy összefüggéseket tárjon fel a közösségi média katonai alkalmazásának stratégiai, etikai és operatív dimenziói között.

Módszertan

A disszertáció módszertani megközelítése többkomponensű, kvalitatív dominanciájú, ugyanakkor kiegészítő empirikus elemeket is integráló kutatási designon alapul, amely ötvözi a szisztematikus irodalomkutatást, az esettanulmány-elemzést, a félig strukturált szakértői interjúkat, valamint a kérdőíves adatfelvételt. E módszertani trianguláció célja

a vizsgált jelenség komplexitásának több nézőpontból történő feltárása, valamint a kapott eredmények érvényességének és megbízhatóságának növelése.

A kutatás elsődleges módszertani pillérét a szisztematikus irodalomkutatás és a másodelemzés képezi, amelynek során a releváns hazai és nemzetközi tudományos publikációk, katonai doktrínák, nemzetközi szervezetek (pl. NATO, EU) iránymutatásai, valamint jogi és szabályozási dokumentumok kerültek feldolgozásra. Az irodalomkutatás célja egyrészt az információs műveletek és a közösségi média katonai alkalmazásának elméleti kereteinek feltárása, másrészt a meglévő tudományos eredmények kritikai értékelése és összehasonlító elemzése. A szakirodalom másodelemzése lehetővé tette a releváns elméleti modellek, koncepcionális keretek és korábbi empirikus megállapítások azonosítását, amelyek alapul szolgáltak a kutatási hipotézisek megalapozásához és a vizsgálati keret kialakításához.

A kutatás második meghatározó eleme az esettanulmány-alapú kvalitatív elemzés, amely a közösségi média információs műveletekben betöltött szerepének empirikus vizsgálatát szolgálja. Az esettanulmányok kiválasztása célzott mintavételi stratégiával történt, figyelembe véve azok relevanciáját, dokumentáltságát és a vizsgált jelenség szempontjából való reprezentativitását. A vizsgált esetek közé tartozik különösen a 2014-es Krím-félsziget orosz annexiója, valamint a 2022-ben eszkalálódott orosz–ukrán fegyveres konfliktus, amelyek során a közösségi média kiemelkedő szerepet játszott az információs műveletek végrehajtásában. Az esettanulmányok elemzése során a kutatás kvalitatív tartalomelemzési módszereket alkalmaz, amelyek lehetővé teszik a narratívák, kommunikációs stratégiák, valamint a platformokon megjelenő információs mintázatok azonosítását és értelmezését. Az elemzés különös figyelmet fordít az információterjesztés mechanizmusaira, a dezinformációs kampányok struktúrájára, valamint a közvélemény befolyásolásának módszereire.

A kvalitatív elemzést kiegészítik a félig strukturált szakértői interjúk, amelyek célja a gyakorlati tapasztalatok és szakmai perspektívák integrálása a kutatásba. Az interjúalanyok kiválasztása célzott mintavétellel történt, és olyan szakembereket foglal magában, akik közvetlen tapasztalattal rendelkeznek a kiberbiztonság, az információs műveletek, a katonai kommunikáció vagy a nemzetbiztonsági elemzés területén. Az interjúk során nyert kvalitatív adatok hozzájárulnak a közösségi média operatív

alkalmazásának mélyebb megértéséhez, valamint lehetővé teszik az elméleti megállapítások gyakorlati validálását.

A kutatás empirikus dimenzióját tovább erősíti a kérdőíves adatfelvétel, amelynek célja a közösségi média és az információs műveletek közötti összefüggések percepciójának és gyakorlati megjelenésének feltérképezése egy meghatározott célcsoport körében. A kérdőíves módszer lehetővé teszi strukturált adatok gyűjtését, amelyek kiegészítik a kvalitatív elemzés eredményeit, és hozzájárulnak az általánosítható következtetések levonásához. A kérdőíves adatok feldolgozása leíró statisztikai módszerekkel történik, amelyek célja a válaszok közötti mintázatok és összefüggések azonosítása.

A kutatás során alkalmazott elemzési logika egyaránt támaszkodik induktív és deduktív következtetési módszerekre. Az induktív megközelítés lehetővé teszi az empirikus adatokból kiindulva új mintázatok és összefüggések feltárását, míg a deduktív megközelítés a meglévő elméleti keretek és hipotézisek empirikus tesztelését szolgálja. A deduktív elemzés különösen a megfogalmazott kutatási hipotézisek vizsgálatában játszik központi szerepet, lehetővé téve annak értékelését, hogy a közösségi média milyen mértékben tekinthető önálló információs műveleti eszköznek, valamint milyen hatással van az információs fölény megszerzésére és a műveleti biztonságra.

A módszertani megközelítés integrált jellege biztosítja, hogy a kutatás ne csupán elméleti szinten vizsgálja a közösségi média szerepét az információs és kibertéri műveletekben, hanem empirikus bizonyítékokkal is alátámassza a megállapításokat. A különböző módszerek kombinációja lehetővé teszi a jelenség komplex, multidiszciplináris értelmezését, hozzájárulva a közösségi média katonai és információs alkalmazásának mélyebb megértéséhez, valamint a releváns stratégiai, jogi és operatív következtetések levonásához.

1. FEJEZET
KATONAI MŰVELETEK, INFORMÁCIÓS MŰVELETEK, KIBERTÉR MŰVELETEK ÉS A KÖZÖSSÉGI MÉDIA

Az információs társadalom és a digitalizáció forradalma alapvetően alakította át a hadviselés fogalmát és gyakorlatát. A hagyományos fegyveres konfliktusok mellett egyre nagyobb szerepet kapnak az információs műveletek és a kibertéri konfrontáció, amelyek nemcsak a katonai műveletek kereteit bővítik ki, hanem az államok és a nemzetközi közösség biztonságpolitikáját is újragondolásra késztetik. A digitalizáció olyan átalakulást hozott, amely megváltoztatta az erőviszonyokat és új lehetőségeket, de egyben új fenyegetéseket is teremtett a modern hadviselés területén.

Az elmúlt évtizedekben a hadviselés generációinak elmélete keretében megkülönböztették a hagyományos állami háborúk első három generációját, amelyek során a reguláris seregek és a nemzetállami struktúrák voltak a főszereplők. A negyedik generációs hadviselés paradigmaváltást hozott és az állam monopolizálta konfliktusok helyett előtérbe kerültek a nem állami szereplők, valamint az olyan konfliktusok, amelyek az ellenség motivációinak és társadalmi kohéziójának gyengítését célozzák. Ezzel párhuzamosan a digitális technológiák megjelenése és elterjedése új dimenziókat nyitott meg a hadviselésben, amelyek meghatározzák a jelen és a jövő konfliktusainak dinamikáját.

A kibertér, amely egykor csupán a technológiai innováció színtere volt, mára önálló harctérré vált. A kibertámadások és a kiberháború nemcsak katonai, hanem civil célpontokat is érintenek, mint például az energetikai infrastruktúrák, pénzügyi rendszerek vagy kommunikációs hálózatok. Az államok számára a kiberbiztonság nemcsak technológiai, hanem stratégiai prioritássá vált, amely új típusú képességek és módszerek fejlesztését követeli meg. Az intelligens fegyverrendszerek, az önvezető drónok és a mesterséges intelligencia alapú elemzési technikák olyan eszközöket kínálnak, amelyek alapvetően formálják át a hadviselés hatékonyságát és rugalmasságát.

Az információs műveletek szintén kiemelt szerepet kapnak a modern konfliktusokban. A hagyományos propaganda eszközök mellett megjelentek az információs fölény megszerzésére és fenntartására irányuló stratégiák, amelyek a

tömegtájékoztatási eszközök és a közösségi média révén valósulnak meg. Az információs műveletek egyik kulcsterülete a közösségi média, amely egyszerre szolgálhat az információk gyűjtésére, terjesztésére és manipulálására, valamint védendő infrastruktúraként is megjelenik. A közösségi média nem csupán az állami és nem állami szereplők közötti konfliktusokban játszik szerepet, hanem az államok belső stabilitására és társadalmi kohéziójára is jelentős hatást gyakorolhat.

A kiberhadviselés másik lényeges eleme a virtuális szimulációk és az adatelemzés. A modern technológiák lehetővé teszik a valósághű kiképzési környezetek kialakítását, valamint a nagy mennyiségű adat feldolgozását és elemzését, amelyek elősegítik a gyorsabb és pontosabb döntéshozatalt. Ezek a képességek nemcsak a katonai műveletek tervezésében, hanem az előre nem látható helyzetekre való reagálásban is kulcsfontosságúak.

A jelen fejezet célja, hogy átfogóan bemutassa, miként határozzák meg a katonai, információs és kibertérben zajló műveletek a hadviselés modern stratégiáit és gyakorlatait. Az egyes alfejezetek kitérnek a digitális technológiák hatásaira, a közösségi média szerepére és a kiberbiztonsági kihívásokra, miközben felvázolják a jövőbeni konfliktusok lehetséges irányait. Az itt tárgyalt kérdések nemcsak a hadviselés elméleti kereteit érintik, hanem a mindennapok biztonságát is, hiszen a digitális technológiák mind az egyéni, mind a társadalmi szinten átszövik életünket.

1.1. Hadviselés a digitális korban

A hadviselés az emberi történelem egyik állandó eleme, amely mindig is alkalmazkodott az adott kor társadalmi, technológiai és politikai környezetéhez. Az elmúlt évtizedekben a háborúk természete gyökeresen átalakult. A klasszikus, nemzetállamok közötti konfliktusok helyét egyre inkább átvették az aszimmetrikus harcmodorok, amelyeket nem állami szereplők vívnak, valamint a digitalizáció által meghatározott új dimenziók. Kiss Álmos Péter generációs elmélete [1] jól tükrözi e változásokat, különösen a negyedik generációs hadviselés paradigmáját, amely szakít a hagyományos hadviselési modellekkel. Emellett a digitalizáció nemcsak új eszközöket és módszereket adott a hadviseléshez, hanem teljesen átalakította annak lényegét.

A hadviselés történetét négy generációra lehet osztani, amelyek közül az első három a nemzetállamok dominanciáján alapul. Az első generációs hadviselés az ipari forradalom előtti időszakra jellemző, ahol a harcászat főként nagy létszámú hadseregek

vonalharcaira épült. Ekkor a fő cél az ellenséges erők közvetlen megsemmisítése volt. A második generáció az ipari technológia, például a lőfegyverek és a tüzérség térnyerésével új stratégiák alkalmazását követelte meg, például a lövészárok-hadviselést. A harmadik generáció a villámháborús technikákat és az információs fölényt helyezte középpontba, amelyek különösen a második világháború során váltak meghatározóvá. [1]

A negyedik generációs hadviselés alapvetően eltér a korábbi modellektől, hiszen nem állami szereplők, például terrorista csoportok, gerillák és más aszimmetrikus erők dominálnak benne. Ezek a konfliktusok nem kizárólag az ellenség katonai képességeinek megsemmisítésére törekednek, hanem annak pszichológiai és társadalmi kohézióját is célba veszik. A negyedik generáció alapvető eszköze az információs hadviselés, amely a civil lakosság manipulálásával és az ellenség akaratának aláásásával éri el céljait. Ez a megközelítés jelentős kihívások elé állítja a hagyományos hadviselésre berendezkedett nemzetállamokat, amelyeknek új stratégiákat kell kidolgozniuk a változó fenyegetésekkel szemben. [1]

A digitalizáció megjelenése forradalmasította a modern hadviselést, mind az alkalmazott eszközök, mind a stratégiák szintjén. Az információs technológia és a hálózatok sérülékenysége új dimenziókat nyitott a konfliktusok kezelésében. A kiberhadviselés lehetővé teszi, hogy államok és nem állami szereplők kritikus infrastruktúrákat, informatikai rendszereket és adatbázisokat támadjanak. Ezek a támadások célzottan kémkedésre, adatlopásra, vagy akár a fizikai világban is megjelenő károk okozására irányulhatnak. A kiberbiztonság mára stratégiai prioritássá vált a globális politikában, amit a NATO részéről felkért szakértői munkacsoport által kidolgozott Tallinn Manual 2.0[1] is hangsúlyoz, amely a kiberhadviselés nemzetközi jogi kereteit fekteti le. [2]

[1] A *Tallinn Manual* és annak kibővített változata, a *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* a kibertér műveletek nemzetközi jogi értelmezését célzó, nem kötelező erejű szakértői kézikönyv. Az első változat (*Tallinn Manual 1.0*, 2013) elsősorban a kibertérben zajló fegyveres konfliktusokra és a nemzetközi humanitárius jog alkalmazhatóságára összpontosított. A gyors technológiai fejlődés és az államok közötti kibertér műveletek növekvő száma azonban szükségessé tette egy átfogóbb elemzés elkészítését, amely a békeidőben végrehajtott kibertér műveletekre is kiterjed. Ennek eredményeként készült el a *Tallinn Manual 2.0* (2017), amely a nemzetközi jog teljes spektrumát vizsgálja, beleértve az állami szuverenitás, a felelősség, a be nem avatkozás és az erő alkalmazásának kérdését a kibertérben. A kézikönyvet a NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) kezdeményezésére létrehozott független nemzetközi szakértői csoport dolgozta ki. A csoport tagjai nemzetközi jogászok, akadémikusok, katonai jogi tanácsadók és kiberbiztonsági szakértők voltak, akik különböző NATO-tagállamokból és partnerországokból érkeztek. Fontos hangsúlyozni, hogy a kézikönyv nem hivatalos NATO-doktrína,

Az intelligens fegyverrendszerek, például az önvezérelt drónok és a mesterséges intelligenciával vezérelt robotok, szintén új szintre emelték a harctéri hatékonyságot. Ezek az eszközök minimalizálják az emberi veszteségeket, miközben lehetővé teszik a precíziós támadásokat. Az ilyen rendszerek nemcsak a jelenlegi, hanem a jövőbeli konfliktusok szempontjából is meghatározó szerepet játszanak. [3]

A digitális kommunikáció alapjaiban változtatta meg a katonai döntéshozatal folyamatát, hiszen a valós idejű adatok elemzése és az információk azonnali megosztásának lehetősége jelentősen felgyorsította és pontosabbá tette a stratégiai és taktikai döntéseket. Az olyan adatelemzési technológiák, mint a big data, egyre fontosabb szerepet töltenek be a helyzetek gyors értékelésében és a különféle fenyegetések hatékony kezelésében. [4]

A közösségi média szintén kulcsszereplővé vált a modern hadviselésben. Ezek a platformok lehetőséget adnak információs kampányok indítására, dezinformáció terjesztésére és az ellenség manipulálására. A NATO Strategic Communications Centre of Excellence (NATO StratCom COE, magyarul: NATO Stratégiai Kommunikációs Kiválósági Központ) kutatásai szerint a közösségi média hibrid hadviselési eszközként jelentős szerepet játszik a társadalmi és politikai befolyásolásban. Az ukrajnai háború során például a közösségi média aktívan részt vett a konfliktus alakulásának befolyásolásában, mind az információs műveletek, mind a dezinformációs kampányok terén. [5]

A hadviselés történeti változásai szorosan követik az emberi társadalmak technológiai fejlődését. Az első három generációs hadviselés klasszikus konfliktusai után a negyedik generációs paradigma az aszimmetrikus stratégiákra és a nem állami szereplők tevékenységére helyezte a hangsúlyt. A digitalizáció ezen túlmenően radikálisan átalakította a háborúk természetét, új eszközöket és módszereket hozva a konfliktuskezelésbe. A modern hadseregek és államok számára elengedhetetlen, hogy alkalmazkodjanak ezekhez a változó körülményekhez, miközben biztosítják nemzetbiztonságukat és stratégiai előnyeiket.

---

hanem független szakértői elemzés, amely a meglévő nemzetközi jog kibertérre történő alkalmazhatóságát értelmezi és rendszerezi.

Az információs technológia rohamos fejlődése alapjaiban formálta át a hadviselés jellegét, hiszen a digitalizáció nem csupán új eszközökkel bővítette a hadseregek lehetőségeit, hanem egészen új szintre emelte a fegyveres konfliktusok lefolyását is. A harcok egy része ma már a digitális térben zajlik, ami a kibertér műveletektől az intelligens fegyverrendszerek bevetéséig terjed, és ez gyökeresen megváltoztatta a modern háborúk működését és dinamikáját. A kiberbiztonság időközben kulcsfontosságú stratégiai tényezővé vált, miközben a legújabb kommunikációs technológiák lehetővé tették az információk valós idejű áramlását és a döntések azonnali meghozatalát.

A kibertér műveletek a digitalizáció egyik legfontosabb katonai megnyilvánulásai, amelyek új szintre emelték a konfliktusokat. A kibertérben zajló támadások célzottan irányulnak informatikai rendszerek, kritikus infrastruktúrák és adatbázisok ellen. Ezek a támadások kémkedési célokat szolgálhatnak, vagy akár súlyos károkat is okozhatnak, amelyek hatásai a fizikai világban is érzékelhetők. A modern háborúk során a kibertámadások célja nem csupán az információ megszerzése, hanem az ellenfél működési képességének bénítása is. [6]

A kiberbiztonság emiatt ma már stratégiai prioritásként jelenik meg az államok és a hadseregek stratégiáiban. A NATO és más nemzetközi szervezetek különös figyelmet fordítanak a kibervédelem fejlesztésére, hiszen a digitális rendszerek sérülékenysége nemcsak a katonai, hanem a gazdasági és társadalmi stabilitást is fenyegetheti. Az olyan nemzetközi kezdeményezések, mint a Tallinn Manual, világos irányelveket adnak a kiberhadviselés jogi kereteire, segítve a nemzetközi együttműködést ezen a kritikus területen.

Az intelligens fegyverrendszerek, például az önvezérelt drónok és robotok, a modern hadviselés egyik leginnovatívabb területeként jelentek meg. Ezek az eszközök jelentősen növelik a hadműveletek hatékonyságát és rugalmasságát. Az önvezérelt drónok lehetővé teszik a precíziós támadásokat, miközben minimalizálják az emberi veszteségeket. Az ilyen rendszerek képesek valós idejű adatok alapján önállóan döntéseket hozni, ami különösen hasznos a dinamikusan változó harci helyzetekben. [3]

A robotizált rendszerek nemcsak a harctéren, hanem a logisztikai és felderítési feladatokban is kulcsszerepet játszanak. A mesterséges intelligencia által vezérelt eszközök lehetővé teszik az információk gyors feldolgozását, ami különösen fontos az

időérzékeny döntéshozatali folyamatokban. Ezáltal az intelligens rendszerek nemcsak a jelenlegi, hanem a jövőbeli hadviselési stratégiák szerves részeivé válnak. [3]

A digitalizáció forradalmasította a katonai kommunikációt is, amely a modern hadviselés egyik legfontosabb tényezőjévé vált. A gyors és biztonságos információcsere lehetőségei drasztikusan növelték a katonai döntéshozatal hatékonyságát. A távközlési forradalom révén a csapatok valós időben képesek koordinálni a műveleteiket, ami jelentős előnyhöz juttatja őket a konfliktusok során. [7]

Az adatszolgáltatás és információgyűjtés terén bekövetkezett technológiai fejlődés lehetővé tette a döntéshozók számára, hogy pontosabb képet kapjanak a harctéri helyzetről. A digitális térben összegyűjtött adatok elemzése hozzájárul a műveleti tervek optimalizálásához és az információs fölény megszerzéséhez. Az információs rendszerek integrálása és a valós idejű adatfeldolgozás képessége alapvetően újra definiálta a modern hadviselést, ahol az információ jelentősége már nemcsak a támogatói szerepben jelenik meg, hanem a siker egyik kulcstényezőjévé vált. [7]

A digitális szimulációk és a virtuális valóság technológiák alkalmazása a katonai képzés egyik legjelentősebb újítása. Ezek az eszközök lehetővé teszik a valószerű körülmények közötti kiképzést, ami különösen fontos a változó harci körülményekhez való alkalmazkodás szempontjából. A katonák virtuális forgatókönyvek segítségével gyakorolhatják a különböző hadműveleti helyzeteket, miközben minimalizálják a tényleges konfliktusokkal járó kockázatokat. [8]

A virtuális valóság másik nagy előnye a döntéshozatali folyamatok optimalizálásában rejlik. A vezetők különféle forgatókönyveket szimulálhatnak és elemezhetnek, hogy a leghatékonyabb stratégiát válasszák ki. Ez nemcsak a harctéri műveletek során, hanem a hosszú távú tervezésben is előnyöket nyújt. [7]

A big data és az adatelemzés technológiái új dimenziókat nyitottak a katonai stratégiai tervezésben is. Ezek az eszközök lehetővé teszik a hatalmas mennyiségű adat gyors és hatékony feldolgozását, amely elengedhetetlen a modern hadviselés dinamikus környezetében. Az elemzett adatok segítenek a katonai vezetőknek abban, hogy pontosabb döntéseket hozzanak, javítva a harctéri helyzetértékelést és a fenyegetések felismerését. [4]

Az adatelemzési rendszerek az információs fölény megszerzésének kulcsfontosságú eszközeivé váltak. A mesterséges intelligencia által támogatott elemzési modellek lehetővé teszik a komplex helyzetek gyors megértését és a stratégiai döntések alátámasztását. [4]

Az elektronikai hadviselés technológiái az elmúlt évtizedekben jelentős fejlődésen mentek keresztül, és a modern hadviselés egyik alapvető elemévé váltak. Az elektronikai zavarórendszerek és lehallgatási technikák lehetővé teszik az ellenséges kommunikációs rendszerek megzavarását, valamint az érzékelési rendszerek hatékonyságának csökkentését. [9]

Az ilyen technológiák nemcsak a harctéri műveletekben játszanak szerepet, hanem az információs műveletek részeként is. Az elektronikai hadviselés egyik célja az ellenség információs fölényének megtörése, miközben saját rendszereink védelmét erősítjük. Az ilyen rendszerek fejlesztése különösen fontos az aszimmetrikus konfliktusokban, ahol az információ gyors feldolgozása és megosztása döntő szerepet játszik. [6]

A digitális forradalom nem csupán új lehetőségeket teremtett a hadviselésben, hanem új típusú fenyegetéseket is életre hívott. A kibertámadások, kiberkémkedés és az elektronikai zavarás eszközei olyan fenyegetéseket jelentenek, amelyek az államok és szervezetek kritikus infrastruktúráját, informatikai rendszereit és döntéshozatali folyamatait célozzák meg.

A kibertámadások az információs rendszerek és infrastruktúrák elleni célzott műveletek, amelyek célja lehet adatlopás, rendszerek működésének megbénítása vagy az ellenség döntéshozatali folyamataiba való beavatkozás. Ezek a támadások jelentős kockázatot jelentenek a modern társadalmakban, hiszen az államok és vállalatok egyre inkább függnek a digitális infrastruktúráktól. [6]

A kiberkémkedés ma már az egyik legsúlyosabb fenyegetésnek számít, mivel az ilyen típusú támadások során az elkövetők érzékeny információkat próbálnak megszerezni különféle kritikus rendszerekből. Gyakori jelenség, hogy állami háttérrel rendelkező csoportok hajtanak végre olyan akciókat, amelyek célja a stratégiai döntésekhez szükséges adatok megszerzése. Az ukrajnai háború során például az orosz fél célzott támadásokat indított az elektromos hálózatok ellen, ami jól mutatta a technikai felkészültségüket és az ilyen akciók elrettentő erejét. A kibertámadásokkal szembeni

védekezés szempontjából az egyik legfontosabb feladat az informatikai infrastruktúra biztonságának megőrzése, hiszen az olyan rendszerek védelme, mint az energiaellátás, az egészségügyi szolgáltatások vagy a pénzügyi hálózatok, ma már nemzetbiztonsági szinten is kiemelt jelentőséget kapott. Ezeknek a rendszereknek a sérülékenysége komoly társadalmi és gazdasági következményekkel járhat, ezért a kiberbiztonságot célzó stratégiák középpontjába került a megelőzés, valamint az esetleges támadások hatékony kezelése és az ehhez szükséges képességek folyamatos fejlesztése. [10]

Az elektronikai zavarás a modern hadviselés egyik leghatékonyabb eszközévé vált, amely lehetővé teszi az ellenséges kommunikációs és érzékelési rendszerek célzott megzavarását. Ezek az eszközök csökkentik az ellenség döntéshozatali képességeit, miközben saját rendszereink biztonságát növelik. Például az orosz hadsereg az ukrajnai konfliktus során rádió- és navigációs zavarórendszereket alkalmazott, amelyek hatékonyan akadályozták meg az ellenséges erők koordinációját. [11]

A kommunikációs rendszerek elleni támadások másik fontos aspektusa az, hogy megzavarják az ellenség információs hálózatát, ezzel akadályozva meg az időben történő döntéshozatalt. Az ilyen támadások a modern információsműveletek alapvető részét képezik, különösen aszimmetrikus konfliktusok során, ahol az információs fölény megszerzése döntő jelentőségű. [12]

Az új típusú fenyegetések, mint a kibertámadások, kiberkémkedés és elektronikai zavarás nemcsak az ellenséges rendszerek fizikai működését zavarhatják meg, hanem pszichológiai hatást is gyakorolnak azáltal, hogy aláássák az ellenfél döntéshozatali képességét és bizalmát. A védekezéshez ezért elengedhetetlen a megfelelő kiberbiztonsági stratégiák kidolgozása, az infrastruktúra védelmének megerősítése, valamint az elektronikai hadviselési képességek fejlesztése.

A modern hadviselés dinamikusan fejlődő környezetében a digitalizáció és az innovációk alapjaiban formálták át a stratégiai gondolkodást és a szervezeti kultúrát. A hadseregeknek alkalmazkodniuk kell a gyors technológiai változásokhoz, miközben a védelmi és támadó képességeiket is optimalizálniuk kell. A digitalizáció, a mesterséges intelligencia, az adatelemzés és az új típusú hadviselési technológiák integrációja mind hozzájárulnak a modern katonai stratégiák sikerességéhez.

A digitalizáció jelentősen megnövelte a stratégiai és taktikai tervezés hatékonyságát, mivel lehetővé tette a valós idejű információgyűjtést és -elemzést. Az

információs rendszerek, a mesterséges intelligencia és a hálózatba kapcsolt technológiák segítenek gyorsabban reagálni a harctéri helyzetekre, miközben minimalizálják a döntéshozatali ciklusok hosszát. [13]

A stratégiai tervezésben a mesterséges intelligencia által támogatott szimulációk és modellezések lehetővé teszik a különböző forgatókönyvek tesztelését. Ezáltal a katonai vezetők képesek előre látni a különböző stratégiák várható következményeit, és megalapozottabb döntéseket hozhatnak. Az olyan technológiák, mint a GPS és a fejlett szenzorok, tovább javítják a harctéri helyzetek elemzését, biztosítva a vezetők számára a folyamatosan frissített adatokat. [14]

A hadviselés folyamatosan változó környezete az adaptáció képességét követeli meg a hadseregektől. Az adaptáció azt jelenti, hogy a technológiai újításokat gyorsan és hatékonyan kell integrálni, miközben a meglévő stratégiákat és szervezeti kultúrát is folyamatosan fejleszteni kell.

Az innovációk, például az önvezérelt drónok, a mesterséges intelligencia vezérelte rendszerek és a precíziós fegyverek, jelentősen megnövelik a hadseregek képességeit. Az ilyen fejlesztések nemcsak a harctéri hatékonyságot javítják, hanem a logisztikai műveletek koordinációját is elősegítik. Az önvezérelt rendszerek lehetővé teszik a döntéshozók számára, hogy gyorsan alkalmazkodjanak a változó helyzetekhez, minimalizálva az emberi hibák lehetőségét. [15]

A mai hadseregek számára kulcsfontosságúvá vált, hogy megtalálják az egyensúlyt a hagyományos hadviselési eljárások és a digitális technológiák használata között, mivel csak így tudják hatékonyan fejleszteni és összehangolni védelmi és támadó képességeiket. A kibervédelem különösen nagy szerepet kapott a kritikus infrastruktúrák biztonságának megőrzésében, hiszen a modern konfliktusok során egy-egy kibertámadás komoly fennakadásokat és következményeket okozhat. Ezzel párhuzamosan az elektronikai hadviselés, például a kommunikációs rendszerek zavarása vagy lehallgatása, új eszközként jelenik meg az ellenséges műveletek megakadályozásában, mivel ezek a technológiák hatékonyan képesek gyengíteni az ellenfél működését. [14]

A digitalizáció nemcsak a stratégiai tervezést forradalmasította, hanem az új technológiák széleskörű alkalmazásával új szintre emelte a katonai műveletek hatékonyságát is. Az adatelemzés és a big data technológiák lehetővé teszik a hatalmas mennyiségű adat gyors és pontos feldolgozását, ami elengedhetetlen a komplex helyzetek

kezeléséhez. Az elemzett adatok révén a katonai vezetők pontosabb képet kaphatnak a harctéri helyzetről és a potenciális fenyegetésekről. [4]

Az elektronikai hadviselés új lehetőségeket kínál az ellenséges rendszerek megzavarására és az információs fölény megszerzésére. Az ilyen technológiák hatékonyan csökkenthetik az ellenség működési képességeit, miközben saját rendszereink biztonságát növelik. [16]

1.2. Az információs műveletek értelmezése

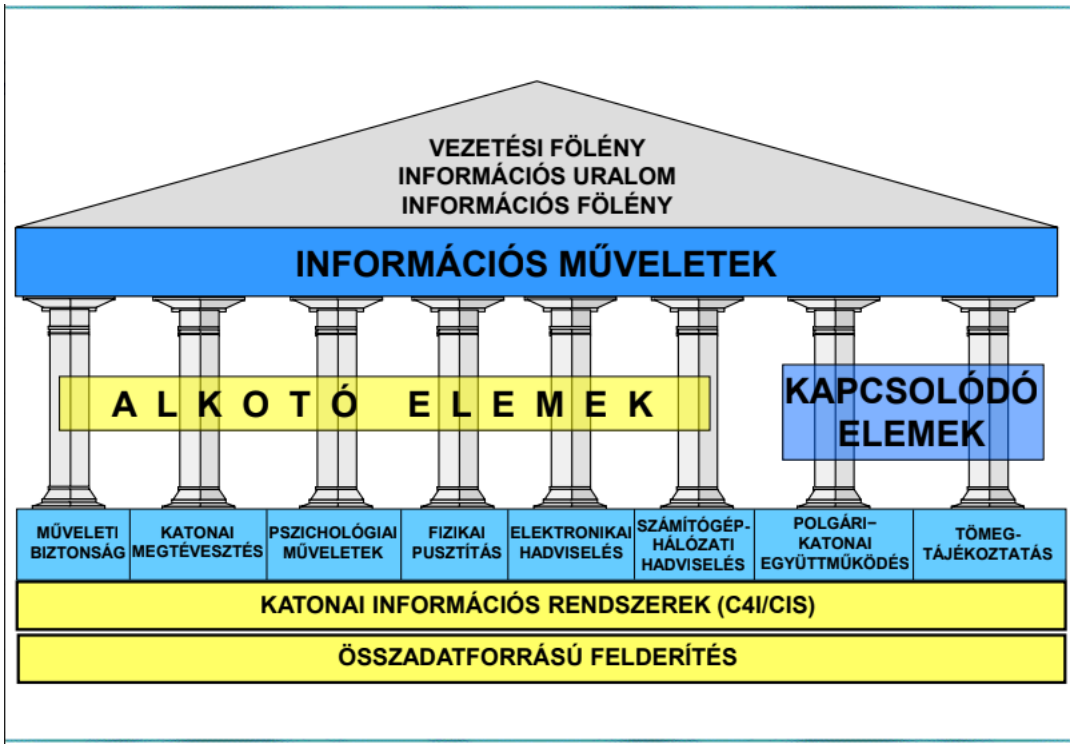
Az információ korában a hadviselés és a geopolitikai küzdelem színtere gyökeresen megváltozott.

A NATO meghatározása szerint az információs műveletek olyan integrált katonai törzsfunkciók, amelyek célja az információs környezet elemzése, tervezése és befolyásolása az ellenfél akaratára és döntéshozatali képességére gyakorolt hatás révén a katonai célok támogatása érdekében [17]. Haig Zsolt értelmezésében az információs műveletek olyan koordinált tevékenységek összességét jelentik, amelyek célja az ellenfél információs rendszereinek és döntéshozatali folyamatainak befolyásolása, megzavarása vagy kihasználása, miközben biztosítják a saját információs rendszerek védelmét és az információs fölény megszerzését [18] [19].

Tehát, az információs műveletek nem csupán kiegészítő eszközök a katonai stratégiákban, hanem önálló hatalmi tényezőként is működnek, amelyek képesek befolyásolni a nemzetközi rendet, a politikai döntéshozatalt és az egyének viselkedését. Az információs műveletek alatt olyan stratégiai tevékenységeket értünk, amelyek célja az információs fölény megszerzése és fenntartása, legyen szó katonai konfliktusról vagy békeidőbeli versengésről. [20] Az elmúlt évtizedekben az információs műveletek fogalma fokozatosan alakult ki, különösen a hidegháború és az azt követő időszakban. Ezek a műveletek célja nem pusztán az ellenséges katonai rendszerek megtévesztése vagy semlegesítése, hanem az ellenfél döntéshozóinak pszichológiai és kognitív befolyásolása is. [21]

A globális digitalizáció és az internet elterjedése új távlatokat nyitott meg az információs műveletek előtt. Az orosz-ukrán konfliktus példája jól mutatja, hogy a közösségi média egyszerre lehet eszköz a dezinformáció terjesztésére és a valós idejű információközlésre. [5] A közösségi média térnyerése nem csupán kommunikációs platformként jelent meg, hanem az információs hadviselés alapvető eszközévé vált. Az

ukrajnai háború során például a közösségi média valós idejű információforrássá vált, amelyen keresztül a konfliktus résztvevői és megfigyelői egyaránt hozzáférhettek az eseményekről szóló hírekhez. Ez az új kommunikációs környezet lehetőséget nyújtott arra, hogy a dezinformáció kampányok hatékonyabbá váljanak, ugyanakkor a hiteles információk terjesztése is gyorsabb és szélesebb körű lett. [22]



1. ábra Az információs műveletek ábrázolása [23]

Az információs műveletek (Information Operations – IO) a katonai stratégia és doktrína olyan területe, amely az információs környezet integrált befolyásolására és kihasználására irányul. A csatolt ábra szemlélteti ezt a koncepciót, ahol az információs műveletek a teljes szerkezet „fedelét” és átfogó célját képezik. Ezen átfogó cél, a **Vezetési Fölény**, az **Információs Uralom** és az **Információs Fölény** megszerzése és fenntartása. Ez azt jelenti, hogy a saját parancsnoki és irányító rendszereink hatékonyabban működnek, mint az ellenfélé, és mi rendelkezünk a pontosabb, aktuálisabb helyzetképpel, ami döntő előnyt jelent a hadviselésben. [23]

Az információs műveletek fajtái az alábbiak:

- **Műveleti Biztonság (OPSEC):** Célja, hogy megakadályozza az ellenfelet abban, hogy a saját tervezésünkre, szándékainkra, képességeinkre vagy korlátainkra

utaló lényeges információkat szerezzen meg. Ez a saját, látszólag jelentéktelen adatok és tevékenységek védelmét jelenti.

- **Katonai Megtévesztés (Military Deception):** Célja, hogy az ellenfél döntéshozóit szándékosan félrevezessék a saját erők létszámát, helyzetét, szándékait vagy képességeit illetően, ezáltal arra kényszerítve őket, hogy hibás vagy a mi terveinknek megfelelő döntéseket hozzanak.
- **Pszichológiai Műveletek (PSYOP):** Célja, hogy célzott információk, üzenetek és jelzések eljuttatásával befolyásolják a külföldi célközönségek (mind a lakosság, mind a katonai erők) érzelmeit, motivációit és végül magatartását, hogy támogassák a saját céljaink elérését.
- **Elektronikai Hadviselés (Electronic Warfare – EW) (színnel kiemelve az oszlopok között):** Célja, hogy az elektromágneses spektrum feletti ellenőrzést megszerezze. Ez magában foglalja az ellenfél kommunikációs és érzékelő (pl. radar) rendszereinek zavarását (Electronic Attack), valamint a saját rendszereink védelmét (Electronic Protection) az ellenfél hasonló tevékenységeivel szemben, valamint az elektronikai támogatást (Elctronic Support Measures). ().
- **Számítógép-hálózati Hadviselés (Computer Network Operations – CNO):** Célja a számítógépes hálózatok és az infrastruktúra elleni támadó (CNA), védelmi (CND) és információszerzési (CNE) tevékenységek végrehajtása. [23]

Mindezen műveletek alapját az információ megszerzése (Intelligence, Surveillance, Reconnaissance,) és az ehhez szükséges vezetési rendszerek (pl. C4I – Command, Control, Communications, Computers and Intelligence) képezik. [23]

A kibertér műveletek az információs műveletek egyik leghatékonyabb eszközei. Az infrastruktúrák elleni támadások, például az ukrán elektromos hálózat elleni kibertámadás 2015-ben, jól szemléltetik ezen műveletek súlyát. [2] A kiberhadviselés nem csupán a kritikus infrastruktúrák elleni támadásokra korlátozódik, hanem magában foglalja a pénzügyi rendszerek, kommunikációs hálózatok és más fontos rendszerek megbénítását is. Ezek a műveletek gyakran előkészítenek hagyományos katonai támadásokat, vagy önállóan próbálják megbénítani az ellenfelet.

Az információs műveletek komplexitása számos kihívást hordoz magában. Az egyik legnagyobb probléma az igazság meghatározásának nehézsége. A dezinformációs műveletek sikeressége abban rejlik, hogy az igazságot és a hamis információt nehezen

lehet megkülönböztetni egymástól. [19] A technológiai fejlődés előnyei mellett a rendszerek sebezhetősége új fenyegetéseket teremtett. A technológiai rendszerek biztonságának hiánya nemzetközi problémává vált, amely komoly következményekkel járhat a nemzeti biztonságra nézve. [20] Emellett a nemzetközi szabályozás hiánya tovább súlyosbítja a helyzetet. Bár a Tallinn Manual 2.0 megkísérelte kodifikálni a kiberhadviselés nemzetközi szabályait, a nemzetközi jog alkalmazása az információs műveletekre továbbra is korlátozott marad. [2]

Az információs műveletek jelentősége a modern világban vitathatatlan. Az információs fölény megszerzése és fenntartása stratégiai előnyt jelent, amely befolyásolja a nemzetközi politikát, a katonai konfliktusokat és a társadalmi stabilitást. Az információs műveletek típusai és elemei szorosan összefonódnak a digitális korszak kihívásaival és lehetőségeivel. Ahogy a technológia fejlődik, úgy válik egyre sürgetőbbé az információs műveletek szabályozása és az azokkal szembeni védelem kialakítása. A jövőbeni konfliktusokban az információs műveletek valószínűleg még fontosabb szerepet kapnak, hiszen a modern technológiák fejlődése új lehetőségeket és veszélyeket hoz létre.

A modern hadviselésben az információs műveletek széles spektrumot ölelnek fel, amelyek különböző célokat és módszereket alkalmaznak az információs fölény megszerzésére vagy fenntartására. Ezek a műveletek nem csupán támadó vagy védekező szerepet töltenek be, hanem a stratégiai és taktikai célok megvalósításának elengedhetetlen elemei is. Az információs műveletek kategóriái között kiemelkedő jelentőséggel bírnak a hírszerzési műveletek, az ellenséges információs műveletek elhárítása, az információs befolyásolás és a kiberalapú műveletek.

A hírszerzési műveletek az információs műveletek alapját képezik, amelyek célja az ellenséges vagy semleges entitások viselkedésének megértése az információk gyűjtése és elemzése révén. Ez magában foglalja az olyan technikákat, mint az emberi hírszerzés (HUMINT), a jelhírszerzés (SIGINT) és a nyílt forrású hírszerzés (OSINT). Kovács (2018) hangsúlyozza, hogy a hírszerzési műveletek nem csupán katonai célokat szolgálnak, hanem politikai és gazdasági döntéshozatalban is meghatározó szerepet játszanak. Például a nyílt forrású hírszerzés lehetővé teszi a közösségi médiából, nyilvános adatbázisokból és más digitális forrásokból származó információk összegyűjtését és elemzését, amelyek elősegítik az ellenfél szándékainak és képességeinek megértését. [19]

Az ellenséges információs műveletek elhárítása a védekező stratégia kulcsfontosságú eleme, amelynek célja a dezinformációs kampányok hatástalanítása és a saját információs rendszer védelme. A dezinformációs kampányok az egyik leghatékonyabb módszert jelentik az ellenséges narratíva terjesztésére, amelynek célja a társadalmi bizalom megingatása és a döntéshozók befolyásolása. [22] Az ilyen kampányok elleni küzdelem során kulcsszerepet játszik az ellenőrzött információk terjesztése és a közvélemény tájékoztatása. Például a NATO országai az elmúlt években fokozott figyelmet fordítottak a digitális térben zajló orosz dezinformációs tevékenységek azonosítására és ellensúlyozására. [5]

Az információs befolyásolás célja a közvélemény vagy célzott csoport véleményének formálása, gyakran stratégiai kommunikáció és pszichológiai hadviselés alkalmazásával. Ez a típusú művelet különösen fontos a modern konfliktusok során, mivel a narratívák alakítása és a társadalmi érzelmek befolyásolása kulcsszerepet játszik a politikai célok elérésében. Rácz szerint az információs befolyásolás eszközei közé tartoznak a média manipulációja, a közösségi média kampányok és a célzott hirdetések. Az orosz-ukrán konfliktus során az orosz stratégiai kommunikáció célja nem csupán az ukrán kormány destabilizálása volt, hanem a nyugati közvélemény befolyásolása is, az orosz narratívák terjesztése révén. [21]

A kiberalapú műveletek az információs műveletek támadó és védekező oldalának is részét képezik. Ezek a műveletek magukban foglalják a hálózati támadásokat, például a hackertámadásokat és a malware[2] terjesztését, amelyek célja az ellenséges infrastruktúra megbénítása vagy az információk eltulajdonítása. Schmitt szerint a kiberhadviselés olyan terület, ahol az állami és nem állami szereplők egyaránt jelentős

[2] Malware (malicious software) olyan rosszindulatú szoftverek gyűjtőneve, amelyeket azzal a céllal fejlesztenek vagy alkalmaznak, hogy jogosulatlan hozzáférést szerezzenek informatikai rendszerekhez, adatokat lopjanak, módosítsanak vagy megsemmisítsenek, a rendszer működését megzavarják, vagy a felhasználó tudta nélkül káros tevékenységet hajtsanak végre.

A malware leggyakoribb típusai közé tartoznak:
– vírus (virus),
– féreg (worm),
– trójai program (trojan),
– zsarolóprogram (ransomware),
– kémprogram (spyware),
– reklámprogram (adware),
– billentyűzetfigyelő (keylogger),
– bot és botnet-kliens,
– hátsó kapu (backdoor). [146]

fenyegetést jelentenek. Az ilyen műveletek azonban nem korlátozódnak kizárólag támadó tevékenységekre; a védekező mechanizmusok fejlesztése, például a kritikus infrastruktúrák védelme és a hálózati biztonság biztosítása, szintén elengedhetetlen része ennek a kategóriának. Az ukrán energiahálózat elleni 2015-ös támadás példát szolgáltat arra, hogy a kiberhadviselés hogyan válhat egy ország alapvető működésének veszélyforrásává. [2]

Az információs műveletek fajtáinak vizsgálata rávilágít arra, hogy ezek a katonai stratégiák mennyire szorosan összefonódnak a modern hadviselés és a geopolitikai küzdelem különböző aspektusaival. Legyen szó hírszerzésről, ellenséges dezinformáció elleni védekezésről, befolyásolási stratégiákról vagy kiberhadviselésről, ezek az eszközök alapvető szerepet játszanak a nemzetek közötti konfliktusokban és a globális hatalmi dinamikák formálásában.

A modern információs társadalomban a tömegtájékoztatás és a propaganda közötti különbség meghatározása alapvető fontosságú, mivel mindkettő kulcsszerepet játszik a közvélemény alakításában és a társadalmi kommunikációban. Bár a két fogalom eltérő célokat és eszközöket képvisel, a gyakorlatban gyakran elmosódik a határvonal közöttük, ami számos vitát és problémát vet fel. [20]

A tömegtájékoztatás célja az objektív információátadás és a közérdekű hírek bemutatása. Ez magában foglalja a tényszerű, kiegyensúlyozott és elfogulatlan tartalmak közvetítését, amely lehetővé teszi az emberek számára, hogy megalapozott döntéseket hozzanak. A tömegtájékoztatás eszközei közé tartoznak a hírportálok, televíziós híradók, rádiós közlemények, valamint a hivatalos sajtótájékoztatók és közlemények. Például az olyan nemzetközi hírszolgáltatók, mint a BBC vagy a Reuters, törekednek arra, hogy minél pontosabb és elfogulatlanabb információkat közöljenek, ezáltal biztosítva a széles körű tájékozódást és az átláthatóságot. [18]

Ezzel szemben a propaganda egy adott politikai, gazdasági vagy társadalmi nézőpont népszerűsítését célozza meg. Az ilyen típusú kommunikáció elsősorban érzelmi alapú, gyakran manipulatív eszközöket használ, mint például a félretájékoztatás, a narratívák szelektív bemutatása vagy a tények eltorzítása. A propaganda célja nem az objektivitás, hanem a közönség meggyőzése egy adott ügy vagy ideológia támogatásáról. Példaként említhetők a politikai kampányok, amelyek során egy adott párt vagy politikai vezető népszerűsítésére fókuszálnak, vagy a szélsőséges csoportok üzenetei, amelyek

érzelmi retorikával próbálják megnyerni a támogatást vagy radikalizálni a közvéleményt. [22]

A tömegtájékoztatás és a propaganda közötti határvonal azonban sok esetben problémás és vitatott. Az egyik legnagyobb kihívás az elfogultság kérdése, amely akkor jelentkezik, ha a tömegtájékoztatás látszólagos objektivitása mögött egy adott politikai vagy gazdasági érdek húzódik meg. Például bizonyos médiumok tartalmait gyakran befolyásolják a tulajdonosi érdekek vagy a hirdetői nyomás, ami torzíthatja a hírek bemutatását. [24] Emellett a szándékosság is kulcskérdés: vajon a tájékoztatás szándékosan tartalmaz-e elfogult vagy manipulált elemeket, vagy csupán az emberi hiba eredményeként válik pontatlanná? Az orosz dezinformációs kampányok kapcsán számos tanulmány mutatta ki, hogy a propaganda tudatos eszközként szolgál az információs hadviselés részeként, miközben sokszor nehéz megkülönböztetni az ilyen kampányokat a hivatalos állami kommunikációtól. [5]

A tömegtájékoztatás és a propaganda közötti különbségek tisztázása kulcsfontosságú a modern társadalomban. Míg a tömegtájékoztatás célja az átláthatóság és az információkhoz való hozzáférés biztosítása, addig a propaganda célzottan befolyásolja a közvéleményt. A gyakorlatban azonban a két fogalom sokszor összemosódik, ami megnehezíti a hiteles információk felismerését és az átláthatóság fenntartását. Ezért elengedhetetlen a médiatudatosság növelése és az olyan szabályozási keretek kidolgozása, amelyek elősegítik a hiteles tájékoztatást és korlátozzák a manipulatív tartalmak terjedését.

A közösségi média térnyerése alapjaiban változtatta meg az információs műveletek dinamikáját, különösen a nyílt forrású hírszerzés (Open Source Intelligence, OSINT) és a közösségi médiából származó információszerzés (Social Media Intelligence, SOCMINT) területén. Az online platformok nem csupán kommunikációs eszközökké váltak, hanem jelentős információforrásként is szolgálnak a modern hírszerzési műveletek számára. A SOCMINT, mint az információszerzés új dimenziója, különösen értékes, mivel lehetővé teszi a felhasználói adatok és viselkedésminták elemzését, amelyek pontosabb betekintést nyújtanak egyének és közösségek gondolkodásába, szokásaiba és szándékaiba. [20]

Az információszerzési potenciál egyik legfontosabb aspektusa a felhasználók által generált adatok és azok viselkedésmintáinak elemzése. Az emberek közösségi médiában

történő aktivitása, például a bejegyzések, megosztások, lájkok és megjegyzések, olyan adatokkal látják el a hírszerzőket, amelyekből következtetni lehet politikai nézetekre, társadalmi kapcsolatokra vagy akár radikalizálódási folyamatokra is. Ezek az adatok nem csupán egyének, hanem csoportok és társadalmak viselkedésének elemzésére is felhasználhatók. [19] A SOCMINT és az OSINT szorosan kapcsolódik egymáshoz, mivel mindkettő a nyilvánosan elérhető információk feldolgozását és értelmezését célozza. A különbség abban rejlik, hogy míg az OSINT általánosan a nyílt forrásokból származó információkra támaszkodik, a SOCMINT kifejezetten a közösségi média által generált adatokra és azok elemzésére koncentrál. [5]

A közösségi média azonban nem csupán az információszerzés eszköze, hanem az információs műveletek terepévé is vált. Ez a kettős szerep számos kockázatot és kihívást rejt magában. Az egyik legjelentősebb probléma a platformokon keresztül terjedő dezinformáció és propaganda. Az orosz-ukrán konfliktus példája rávilágított arra, hogy a közösségi média miként válhat a dezinformációs kampányok egyik legfontosabb csatornájává, amelyek célja az ellenfél destabilizálása és a közvélemény manipulálása. [22] A közösségi médiában terjedő hamis hírek és propagandatartalmak nemcsak a politikai diskurzust befolyásolják, hanem az emberek közötti bizalmat is aláássák, ami súlyos társadalmi következményekkel járhat.

A közösségi média szabályozási és védelmi feladatai ezért kiemelt figyelmet érdemelnek. Bár a platformok szabályozása és az illegális vagy manipulatív tartalmak eltávolítása alapvető fontosságú, a nemzetközi jogi és technológiai környezet bonyolultsága miatt ez rendkívül nehéz feladat. Ahogy Schmitt [2] rámutatott, a közösségi médiában megjelenő tartalmak szabályozása során a szólásszabadság és a biztonság közötti egyensúly megteremtése kritikus kihívás.

A közösségi média, mint információforrás (SOCMINT) témájának részletesebb vizsgálata a későbbi szakaszokban foglalkozik azokkal a konkrét mechanizmusokkal, amelyek révén a közösségi média szabályozási és védelmi rendszerei hatékonyabbá tehetők. A SOCMINT növekvő szerepe az információs műveletekben rávilágít arra, hogy a digitális térben folytatott tevékenységek jelentősége nem csupán a hírszerzés, hanem a nemzetközi biztonság szempontjából is kiemelkedő.

Az információs és vezetési fölény a modern hadviselés és döntéshozatal alapvető pillérei, amelyek központi szerepet játszanak a stratégiai előny megszerzésében. Az

információs fölény azt a képességet jelenti, hogy a releváns információkat gyorsan és hatékonyan szerezzük meg, dolgozzuk fel, majd alkalmazzuk. Ezzel szemben a vezetési fölény arra utal, hogy ezeket az információkat időben és pontosan használjuk fel a döntéshozatalban, biztosítva ezzel a stratégiai és taktikai célok sikeres megvalósítását. [20]

Az információs fölény meghatározása szerint az a képesség, amely lehetővé teszi az információ gyors megszerzését, feldolgozását és alkalmazását, alapvető fontosságú a modern konfliktusokban és a versenykörnyezetben. A hírszerzési rendszerek kulcsszerepet játszanak ebben, különösen a nyílt forrású hírszerzés (OSINT) és a big data elemzési technikák alkalmazása révén. Például a mesterséges intelligencia és az adattudomány lehetővé teszi a hatalmas mennyiségű információ gyors szűrését és elemzését, amely elősegíti az információs fölény fenntartását. [19] A modern hírszerzési rendszerek, például az Egyesült Államok által alkalmazott intelligens adatkezelési és -elemzési rendszerek, képesek valós idejű adatokat szolgáltatni, amelyek kulcsfontosságúak a döntéshozatalban. [2]

A vezetési fölény az információs fölény gyakorlati alkalmazása, amely biztosítja, hogy a pontos és időszerű információk alapján a döntések gyorsan és hatékonyan szülessenek meg. Az információ birtoklása stratégiai előnyt jelent, mivel lehetővé teszi, hogy az ellenfél előtt döntsünk, és proaktívan reagáljunk a helyzetekre. [21] A vezetési fölény és az információs fölény szoros kapcsolatban áll egymással; az előbbi nem létezhet az utóbbi nélkül. Például a NATO operációiban a valós idejű hírszerzés és kommunikáció biztosítja, hogy a katonai vezetők gyorsan reagálhassanak a helyzetváltozásokra, ezzel növelve az esélyt a sikeres küldetések végrehajtására. [22]

A gyakorlati alkalmazások terén mind a katonai, mind a civil vezetési rendszerek fejlődése az információs fölényre támaszkodik. A katonai területen a precíziós irányítási rendszerek, például a drónok és a mesterséges intelligencia által vezérelt célzórendszerek, az információs fölényre épülnek. Ezek a rendszerek valós idejű adatokat használnak fel a hatékonyabb műveletek érdekében, minimalizálva az emberi tévedés lehetőségét. [5] A civil szférában az innováció és a stratégiai tervezés szintén az információs alapú döntéshozatalon nyugszik. Például a városok okos rendszerei, amelyek a forgalomirányítástól az energiafelhasználás optimalizálásáig terjednek, az információ gyors feldolgozására és alkalmazására épülnek. [20]

Az információs és vezetési fölény jelentősége a modern társadalomban és konfliktusokban vitathatatlan. Az információs fölény lehetővé teszi a releváns adatok megszerzését és feldolgozását, míg a vezetési fölény biztosítja, hogy ezeket az információkat időben és hatékonyan használjuk fel. Ezek az elemek nemcsak a katonai siker, hanem a gazdasági és társadalmi fejlődés alapfeltételei is, különösen a technológiai innovációk korában, ahol az információ hatalma minden korábbinál nagyobb értékkel bír.

1.3. A kibertér-műveletek értelmezése

Az internet és a digitális technológiák globális elterjedése egy új hadszíntérré tette a kiberteret, amelyben a nemzetállamok, nem állami szereplők és egyének egyaránt tevékenykednek. A kibertér multidimenzionális jellege lehetőséget biztosít mind a katonai, mind a civil szektor számára, hogy támadó és védekező stratégiákat dolgozzanak ki, amelyek az információs fölény megszerzésére és fenntartására irányulnak. [20]

A kibertér műveletek szerepe a nemzetbiztonságban egyre növekszik, mivel a modern társadalmak függése a digitális infrastruktúrától mindennapos. A kritikus infrastruktúrák, mint például az energiahálózatok, a közlekedési rendszerek és a kommunikációs csatornák, különösen sebezhetők a kibertámadásokkal szemben. Az ilyen támadások nem csupán gazdasági károkat okozhatnak, hanem a társadalmi stabilitást is aláásható, miközben az államok közötti konfliktusok eszkalációjához is vezethetnek. [19] Az AJP 3.20 NATO doktrína kiemeli, hogy a kibertérben zajló műveletek célja a védelmi és támadó képességek összehangolása a stratégiai célok érdekében, miközben elősegíti a szövetséges államok közötti koordinációt. [2]

A nemzetközi kapcsolatokban a kibertér jelentősége tovább nőtt, különösen az információs műveletek területén. Az orosz-ukrán konfliktus jól példázza, hogy a kiberműveletek miként válhatnak a geopolitikai stratégiák központi elemévé. Oroszország rendszeresen alkalmazott dezinformációs kampányokat és kibereszközöket, hogy befolyásolja a nemzetközi közvéleményt és gyengítse Ukrajna politikai stabilitását. [22] Hasonlóképpen, a NATO stratégiai céljai között szerepel a kiberfenyegetések azonosítása és semlegesítése, valamint az olyan hibrid hadviselési technikák elleni védelem, amelyek a kibertérben valósulnak meg. [5]

A hazai doktrína szintén hangsúlyozza a kibertér műveletek szerepét a nemzeti biztonság megőrzésében. Az offenzív és defenzív kibertér műveletek kidolgozása és alkalmazása nemcsak a hadviselés új eszközeit képviselik, hanem az állami

infrastruktúrák védelmének és a társadalom biztonságának fenntartásához is hozzájárulnak. A magyar kiberbiztonsági stratégia prioritásként kezeli a kritikus információs infrastruktúrák védelmét és a kiberbűnözés elleni küzdelmet, amelyek elengedhetetlenek a nemzeti stabilitás fenntartásához. [20]

Az AJP 3.20 és a hazai doktrína relevanciája a kibertér műveletek felosztásában különösen jelentős. Az AJP 3.20 három fő kategóriára osztja a kibertér műveleteket: defenzív műveletek (defensive cyber operations, DCO), offenzív műveletek (offensive cyber operations, OCO), és hírszerző műveletek (Intelligence, Surveillance, and Reconnaissance**,** ISR). Ezek mind a NATO tagállamok közös fellépését szolgálják a kibertérben jelentkező fenyegetésekkel szemben. Ezzel szemben a hazai doktrína hangsúlyosabban foglalkozik a kritikus infrastruktúrák védelmével és a nemzeti szintű kiberbiztonság megerősítésével. [25]

A kibertér műveletei a modern hadviselés és hírszerzési tevékenységek kulcsfontosságú elemei, amelyek célja az információs fölény megszerzése és fenntartása a digitális térben. A kibertér műveletek fogalmát a NATO AJP 3.20 doktrína (2020) és számos nemzeti stratégia egyaránt úgy határozza meg, mint olyan katonai, hírszerzési és védelmi tevékenységek összességét, amelyek elősegítik az ellenfél információs képességeinek csökkentését, a saját rendszerek védelmét, és támogatják a stratégiai döntéshozatalt. [25]

A kibertér műveletek elsődleges célja az információs fölény megszerzése, amely a modern konfliktusokban meghatározó tényezővé vált. Ennek részeként a kibertér műveletek képesek csökkenteni az ellenfél információs képességeit, például azáltal, hogy hozzáférhetetlenné teszik a kritikus rendszereket, vagy torzítják az információkat. Az orosz dezinformációs kampányok és kiberhadműveletek például hatékony eszközei ennek, amelyek az információs tér manipulálásával destabilizálták célpontjaikat. [22]

A saját információs rendszerek és adatok védelme a kibertér műveletek másik alapvető célja. A védekező tevékenységek közé tartozik a kritikus infrastruktúrák biztonságának fenntartása, a támadások előrejelzése és az azokra való reagálás. Az AJP 3.20 és a hazai kiberbiztonsági doktrína egyaránt hangsúlyozza, hogy a védelem első lépése a sebezhetőségek felismerése és a rendszerek folyamatos monitorozása. [25]

A kibertér műveletek harmadik alapvető célja a stratégiai döntéshozatal támogatása az információs fölény révén. A digitális technológiák, például a mesterséges

intelligencia és a big data elemzések lehetővé teszik a döntéshozók számára, hogy gyorsan és pontosan reagáljanak a változó helyzetekre. A hírszerzési műveletek során gyűjtött információk, például a nyílt forrású hírszerzés (OSINT) vagy a zárt rendszerek felderítése, alapvető szerepet játszanak ebben a folyamatban [19]

A kibertér műveletei nemcsak a hadviselés szempontjából létfontosságúak, hanem a nemzetközi kapcsolatok és a nemzeti biztonság számára is meghatározó szerepet játszanak. A Tallinn Manual 2.0 például rávilágít arra, hogy a kibertér műveletek nemzetközi jogi kereteinek megalkotása és betartatása kulcsfontosságú a kiberkonfliktusok megelőzése érdekében. [2] A kibertér műveletek dinamikus fejlődése ugyanakkor kihívást is jelent, mivel az államoknak folyamatosan alkalmazkodniuk kell az új fenyegetésekhez és technológiai változásokhoz.

Az AJP 3.20 NATO-doktrína a kibertér műveleteit három fő kategóriára osztja: defenzív kibertér műveletek (Defensive Cyberspace Operations, DCO), offenzív kibertér műveletek (Offensive Cyberspace Operations, OCO), és kibertéri hírszerző műveletek (Cyberspace Intelligence, Surveillance, and Reconnaissance, ISR). Ezek a kategóriák meghatározzák a kibertérben folytatott tevékenységek célját és eszközeit, egyaránt szolgálva a védekezési, támadási és hírszerzési célokat. [25]

A DCO elsődleges célja a saját hálózatok és rendszerek védelme az ellenséges támadásokkal szemben. Ezek a műveletek proaktív védekezési stratégiákat alkalmaznak, például anomáliák észlelését és a támadások forrásainak azonosítását. A védekezési eszközök közé tartoznak a tűzfalak, a behatolás-megelőző rendszerek (Intrusion prevention systems, IPS), valamint a rendszeres kiberbiztonsági gyakorlatok, amelyek célja a védekezési kapacitások tesztelése és fejlesztése. [2] A DCO műveletek különösen fontosak a kritikus infrastruktúrák, például az energiahálózatok és kommunikációs rendszerek védelme szempontjából, amelyek az ellenséges támadások fő célpontjai lehetnek. [20]

Az OCO az ellenséges hálózatok és rendszerek támadására irányulnak, hogy katonai célokat érjenek el. Ezek a műveletek magukban foglalják az ellenséges kommunikációs infrastruktúra megbénítását, az adatok eltulajdonítását vagy a rendszerek működésének megzavarását. Példák erre a malware használata, amely képes behatolni az ellenséges hálózatokba, vagy a szolgáltatásmegtagadási (Distributed denial of Service, DDoS) támadások, amelyek átmenetileg megbénítják az ellenfél digitális

infrastruktúráját. [22] Az offenzív műveletek célja az, hogy az ellenséges oldal képességeit jelentősen csökkentsék, miközben stratégiai előnyt biztosítanak a támadó fél számára.

A kibertéri ISR célja információk gyűjtése az ellenséges hálózatokról és rendszerekről, valamint a támadási és védekezési műveletek támogatása. Az ISR műveletek keretében alkalmazott eszközök közé tartozik az OSINT, amely az interneten elérhető információkat elemzi, valamint a zárt rendszerek feltérképezése, amely különösen érzékeny adatok megszerzésére irányul. [18] Az ISR műveletek különösen fontosak a katonai és hírszerzési döntéshozatal támogatásában, mivel a begyűjtött adatok lehetővé teszik a helyzet pontosabb megértését és a hatékony stratégiai tervezést.

Az AJP 3.20 szerinti felosztás átfogó keretet biztosít a kibertérben folytatott tevékenységek számára. Míg a defenzív műveletek a saját rendszerek védelmére, az offenzív műveletek az ellenség gyengítésére, a hírszerző műveletek pedig az információs fölény megszerzésére összpontosítanak, mindhárom terület szoros összefüggésben áll egymással. Ezek az elemek biztosítják, hogy a NATO és tagállamai hatékonyan reagálhassanak a kibertérben jelentkező fenyegetésekre és kihívásokra. [25]

A hazai doktrína, amely szorosan kapcsolódik a nemzetközi gyakorlatokhoz és jogszabályi keretekhez, átfogó rendszert nyújt a kibertér műveletek különböző típusaira. Ez a rendszer négy fő területet határoz meg: kiberbiztonsági műveletek, kiberhadviselési műveletek, kiberfelderítő műveletek és kiberelrettentés. E területek mindegyike a modern kiberfenyegetésekre adott stratégiai válaszokat tükrözi, amelyek célja az állam védelmi és támadóképességének biztosítása a kibertérben.

A kiberbiztonsági műveletek fő célja az állami és katonai rendszerek, valamint a kritikus infrastruktúrák védelme. Ide tartoznak például az energiaellátás, a közlekedési rendszerek és a kommunikációs hálózatok, amelyek sérülékenysége komoly veszélyt jelenthet a társadalmi stabilitásra. Magyarország nemzeti kiberbiztonsági stratégiája hangsúlyozza, hogy ezen rendszerek működésének biztosítása érdekében fejlett technológiák, például tűzfalak és IPS alkalmazása elengedhetetlen. Az Európai Unió NIS irányelve (Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, magyarul: Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve az Unió egész területén a hálózati és információs rendszerek magas közös biztonsági szintjének biztosítására irányuló

intézkedésekről), amelyet a magyar jogrendszer is implementált, kötelezi a tagállamokat a kritikus infrastruktúrák kiberbiztonságának fokozására. [20]

A kibertér műveletek célja az ellenséges rendszerek elleni támadások végrehajtása és a saját rendszerek védelme. Az offenzív műveletek közé tartozik az ellenséges hálózatok megbénítása, adatok eltulajdonítása, valamint a kommunikációs csatornák megzavarása. A védekező műveletek pedig olyan stratégiák kidolgozását igénylik, amelyek gyors és hatékony reagálást tesznek lehetővé az ellenséges támadásokra, beleértve a valós idejű fenyegetés-elemzést és a gyors reagálási csapatok működését. [19] A Tallinn Manual 2.0 szerint az ilyen támadó műveletek a nemzetközi jog keretei között csak akkor tekinthetők jogszerűnek, ha azok arányosak és a nemzetbiztonságot szolgálják. [2]

A kiberfelderítő műveletek legtöbb esetben a kiberfenyegetésekről szóló információgyűjtést célozzák. Ezek magukban foglalják az OSINT alkalmazását, valamint a mélyebb hálózati rendszerek felderítését, amelyek az ellenséges szándékok és képességek azonosítását szolgálják. Az orosz katonai doktrína kiemeli az ilyen jellegű tevékenységek fontosságát a stratégiai előkészítés és a védekező stratégiák kialakítása során. [21] A magyar kiberfelderítő műveletek külön hangsúlyt fektetnek a nemzetközi együttműködésre, amely kulcsfontosságú az európai biztonsági kihívások kezelésében.

A kiberelrettentés olyan műveleteket foglal magában, amelyek célja a támadók elrettentése a kibertérben való tevékenységeiktől. Ez magában foglalja a támadó kapacitások demonstrálását és a stratégiai kommunikációt, amelyek jelzik, hogy az ország képes reagálni a kibertérben jelentkező fenyegetésekre. Az ilyen stratégiák alapját a NATO által kidolgozott irányelvek és a hazai tapasztalatok adják. Az elrettentés része a rendszeres kiberbiztonsági gyakorlatok végrehajtása is, amelyek nemcsak a technikai képességeket fejlesztik, hanem erősítik a nemzetközi partnerek közötti bizalmat. [22]

Az AJP 3.20 NATO-doktrína és a magyar kiberbiztonsági doktrína egyaránt a modern kiberfenyegetések kezelésére szolgáló alapelveket és stratégiákat tartalmazza. Bár ezek a doktrínák több közös alapelvet osztanak meg, jelentős eltérések is vannak közöttük, amelyek az eltérő geopolitikai helyzetből és nemzeti prioritásokból erednek. [26]

A közös alapelvek közé tartozik a védekezés és támadás egyensúlyának fenntartása a kibertérben. Mind az AJP 3.20, mind a hazai doktrína hangsúlyozza, hogy

a védekezés és támadás közötti megfelelő egyensúly elengedhetetlen az információs fölény megszerzéséhez és fenntartásához. Az információs fölény alapvető fontosságú a modern hadviselésben, mivel biztosítja, hogy az adott állam hatékonyan tudja megelőzni, illetve elhárítani a kibertámadásokat, miközben képes támadó műveleteket is végrehajtani a stratégiai célok elérése érdekében [26] mindkét doktrína prioritásként kezeli az infrastruktúra és az adatok védelmét. Ez magában foglalja a kritikus infrastruktúrák – például az energiahálózatok, közlekedési rendszerek és kommunikációs hálózatok – biztonságának megőrzését, amelyek egy kibertámadás esetén súlyosan veszélyeztethetik az állam működőképességét. Az Európai Unió NIS irányelve alapján Magyarország törvényi szinten is szabályozza a kritikus infrastruktúrák védelmét [27]

Az AJP 3.20 kiemelten nemzetközi dimenzióval rendelkezik, ami az egyik legfontosabb különbség a hazai doktrínához képest. A NATO-doktrína fő célja a tagállamok közötti együttműködés előmozdítása, beleértve a közös gyakorlatokat, a fenyegetések elleni kollektív fellépést és az információmegosztást. Ez különösen fontos a kiberbiztonsági kérdések kezelésében, mivel a fenyegetések gyakran határokon átnyúló jellegűek, és egy állam egyedül nem képes hatékonyan kezelni azokat. [25]

Ezzel szemben a hazai doktrína prioritásokra és specifikus kihívásokra összpontosít. Nagyobb hangsúlyt helyez a magyar kritikus infrastruktúrák védelmére, és olyan megoldásokat szorgalmaz, amelyek kifejezetten a nemzeti sajátosságokhoz illeszkednek. Ez magában foglalja a magyar állam koordináló szerepét, amely biztosítja, hogy az infrastruktúrák tulajdonosai és üzemeltetői megfeleljenek a biztonsági követelményeknek, valamint fejlett technológiai rendszerek és eljárások alkalmazását a nemzeti kiberbiztonság fenntartása érdekében. [28]

A két doktrína közötti különbségek ellenére mindkettő azonosítja a kibertér jelentőségét a modern hadviselésben és nemzetbiztonságban. Az AJP 3.20 nemzetközi szövetségi kontextusban alkalmazható, míg a hazai doktrína nemzeti keretek között nyújt iránymutatást. Mindkét megközelítés hozzájárul ahhoz, hogy az államok hatékonyan reagálhassanak a folyamatosan fejlődő kiberfenyegetésekre, és biztosítsák a kiberbiztonságot globális és helyi szinten egyaránt.

A kibertérben zajló műveletek egyre komplexebbé és dinamikusabbá válnak, ami számos kihívást és stratégiai irányt vet fel a jövőre nézve. A technológiai fejlődés, a nemzetközi szabályozás hiányosságai és az emberi tényező kezelése egyaránt olyan

kulcsfontosságú területek, amelyek meghatározzák a kiberbiztonsági rendszerek fejlesztésének irányát és a globális együttműködés szükségességét.

A technológiai fejlődés üteme az egyik legnagyobb kihívás a kibertérben zajló műveletek számára. Az új technológiák, mint például a mesterséges intelligencia (MI) és a gépi tanulás, nemcsak a védelmi rendszerek hatékonyságát növelhetik, hanem új kiberfenyegetések megjelenését is előidézhetik. Az MI-alapú támadások például képesek valós idejű elemzésekre, automatikus sebezhetőség-feltárásra és célzott támadások végrehajtására, amelyek sokkal gyorsabbak és precízebbek lehetnek, mint a hagyományos módszerek. [29] Az ilyen fejlett fenyegetések elleni védekezés új technológiai innovációkat és adaptív stratégiákat igényel, amelyek képesek lépést tartani a támadók eszközeivel.

A nemzetközi szabályozás hiánya szintén jelentős problémát jelent a kibertér műveleteiben. A Tallinn Manual 2.0 szerint bár a nemzetközi jog alapelvei alkalmazhatók a kiberhadviselésben, az egységes jogi keretrendszerek még mindig hiányoznak. Ez megnehezíti a felelősségre vonást és az államok közötti együttműködést, különösen olyan esetekben, amikor a támadások anonim módon történnek, vagy állami támogatás áll mögöttük. [2] Az egységes szabályozás kialakítása, amely figyelembe veszi a nemzeti szuverenitást és a globális biztonsági kihívásokat, alapvető fontosságú a kibertérben zajló műveletek szabályozására és koordinálására.

A humán tényező szintén kiemelt jelentőségű a kiberbiztonságban. A szakértők képzése és a kiberbiztonsági tudatosság növelése nemcsak a védelmi rendszerek hatékonyságát javítja, hanem csökkenti a felhasználói hibákból eredő sebezhetőségeket is. A humán tényező továbbra is az egyik leggyengébb láncszem a kiberbiztonsági láncban, hiszen az adathalász támadások és a szociális manipuláció gyakran az emberi tévedéseket célozzák. [19] A szakértők képzése mellett a társadalmi szintű tudatosság növelése is szükséges, amely a mindennapi digitális eszközök biztonságos használatát és a fenyegetések felismerését célozza.

A jövőbeni irányok közé tartozik a mesterséges intelligencia és a gépi tanulás integrálása a kiberbiztonsági rendszerekbe, amelyek képesek valós idejű fenyegetés-elemzésre és automatikus válaszintézkedések végrehajtására. Emellett a nemzetközi együttműködés és az egységes jogi keretek kidolgozása elengedhetetlen a globális biztonsági kihívások kezeléséhez. Az emberi tényező fejlesztése és a társadalmi szintű

kiberbiztonsági tudatosság növelése pedig alapvető feltétele annak, hogy a kiberfenyegetésekre adott válaszok hatékonyak és fenntarthatók legyenek.

1.4. A kibervédelem értelmezése

A modern világ digitalizációja amellett, hogy megváltoztatta mindennapi életünket, ugyanakkor sebezhetővé tette a rendszereinket. A digitális térben tárolt információk és hálózatok egyre gyakoribb célpontjai a különböző kibertámadásoknak. A kibervédelem célja e rendszerek és adatok védelme, a támadások megelőzése, azonosítása és elhárítása. Ez az esszé a kibervédelem fogalmát, jelentőségét, gyakorlati példáit és hatásait vizsgálja a modern társadalomban, különös tekintettel a gazdasági, közszolgáltatási és nemzetbiztonsági vonatkozásokra.

A kibervédelem az informatikai rendszerek, hálózatok és adatok biztonságának megőrzésére irányuló tevékenységek összessége. Ide tartozik a megelőzés, a fenyegetések felismerése, az incidensekre adott válaszlépések és az érintett rendszerek helyreállítása. A kibertér, mint működési környezet, rendkívül dinamikus; a benne zajló események és fenyegetések folyamatosan változnak, ezért a kibervédelmi stratégiák fejlesztése elengedhetetlen. Kovács [30] szerint a kibertér műveletek természete a technológiai fejlődéssel párhuzamosan bonyolultabbá válik, így a védekezési mechanizmusok folyamatos korszerűsítése szükséges.

A kibervédelem tehát nemcsak technológiai kérdés, hanem társadalmi, gazdasági és politikai szinten is releváns probléma. Alapvető szerepe van a digitális infrastruktúrák védelmében, beleértve az energiaellátó rendszereket, a pénzügyi szektort és az egészségügyi szolgáltatásokat.

Az elmúlt évtizedekben a kibertámadások száma és hatása exponenciálisan növekedett. E támadások nem csupán technológiai kihívást jelentenek, hanem jelentős gazdasági, társadalmi és politikai következményekkel is járnak. A következőkben ezeket a támadásokat fogom részletesen vizsgálni.

Zsarolóvírusok (ransomware)

A zsarolóvírusok célja az adatok zárolása és bizonyos pénzösszeg követelése az érintett rendszerek helyreállításáért. Az egyik legismertebb eset a 2017-es WannaCry támadás volt, amely több mint 150 országban okozott fennakadásokat, köztük kórházak és közszolgáltatások működésében is. [31]

Adatlopások

A személyes és vállalati adatok ellopása az egyik leggyakoribb kiberfenyegetés. Az ilyen támadások nemcsak közvetlen anyagi károkat okoznak, hanem reputációs veszteséget is eredményezhetnek. Például 2018-ban a Facebook egyik legnagyobb adatvédelmi botránya több mint 50 millió felhasználó adatait érintette. [18]

Túlterheléses támadások (DDoS)

Ezek a támadások túlterhelik a célpont hálózati erőforrásait, lehetetlenné téve azok normális működését. Az ilyen incidensek különösen kritikusak lehetnek pénzügyi intézmények vagy közlekedési rendszerek esetében. [30]

A kibertámadások jelentős pénzügyi veszteségeket okoznak a vállalatoknak és kormányoknak. Egyes becslések szerint évente több milliárd dolláros károkat generálnak, beleértve a követelt pénzösszegek kifizetését, a helyreállítás költségeit és a kiesett termelést. [32]

Az elveszett vagy kompromittált adatok helyreállítása rendkívül költséges folyamat, és a bizalom helyreállítása is hosszú időt vehet igénybe. Az ilyen esetek különösen érzékenyen érintik az egészségügyi és pénzügyi szektort. [19]

A kibertámadások különösen veszélyesek a kritikus infrastruktúrákra nézve, beleértve az energiaellátást, a közlekedést és az egészségügyi szolgáltatásokat. Ezek a támadások akár nemzetközi válságokat is előidézhetnek. [33]

A kibervédelem az információs társadalom működésének alapkövévé vált, hiszen a digitális rendszerek, hálózatok és adatok védelme nélkülözhetetlen a modern élet minden területén. A digitális tér, más néven kibertér, a számítógépes hálózatok és rendszerek összessége, amelyeken belül az információ áramlik. Ez a tér magában foglalja az internetet, a vállalati hálózatokat, a felhőalapú szolgáltatásokat és az olyan új technológiákat, mint a dolgok internete (IoT). A kibervédelem célja, hogy ezt a komplex rendszert megóvja a különböző fenyegetésektől, miközben biztosítja az információk bizalmasságát, sértetlenségét és rendelkezésre állását. Kovács [30] kiemeli, hogy a kibertér sebezhetősége folyamatos innovációt és fejlődést követel a védelmi mechanizmusok terén.

A kibervédelem számos összetevőből áll, amelyek együtt alkotnak egy átfogó rendszert. Az egyik legfontosabb elem a megelőzés, amelynek célja a fenyegetések

felismerése és semlegesítése még azelőtt, hogy azok kárt okoznának. A megelőzés eszközei között szerepelnek a tűzfalak, amelyek szabályozzák a hálózati forgalmat, a vírusirtók, amelyek azonosítják és eltávolítják a kártékony szoftvereket, valamint a szoftverfrissítések, amelyek rendszeresen kijavítják az ismert sebezhetőségeket. Ezek az alapvető technológiák jelentik az első védelmi vonalat a támadásokkal szemben, és elengedhetetlenek a digitális rendszerek biztonságának fenntartásához. [18]

A megelőzést követően a felderítés lépése következik, amely a fenyegetések észlelésére és azonosítására irányul. A behatolás-észlelő rendszerek (IDS) különösen fontosak ebben a folyamatban, hiszen képesek felismerni a szokatlan hálózati tevékenységeket és az ismert támadási mintákat. Ezzel párhuzamosan a hálózati monitoring lehetővé teszi a teljes rendszer folyamatos ellenőrzését, ami elengedhetetlen a fenyegetések korai felismeréséhez. Kovács [30] azt is kiemeli, hogy a gyors reagálás kulcsfontosságú, hiszen a késlekedés jelentős károkat okozhat a hálózati rendszerekben és az adatokban.

Amikor egy támadás bekövetkezik, a reagálás azonnali lépéseket követel meg. Az incidens-kezelési protokollok célja a támadás azonosítása, elemzése és semlegesítése, miközben minimalizálják a károkat. A hatékony reagálás része a helyreállítási stratégiák kidolgozása is, amelyek biztosítják, hogy az érintett rendszerek és adatok a lehető leghamarabb visszatérjenek normális működésükhöz. A helyreállítás egyik alapvető eszköze az adatmentés, amely biztosítja a fontos adatok biztonsági másolatainak elérhetőségét. Emellett a redundáns rendszerek használata is jelentős szerepet játszik, mivel lehetővé teszik a folyamatosságot, még akkor is, ha az elsődleges rendszerek nem működnek. [31]

A kibervédelem alapjaihoz tartoznak azok a modern technológiai megoldások is, amelyek növelik a hatékonyságot és javítják a fenyegetésekkel szembeni védekezési képességet. A mesterséges intelligencia (artificial intelligence, AI) és a gépi tanulás például egyre fontosabbá válik a fenyegetések felismerésében. Ezek az algoritmusok képesek a korábbi támadások mintáinak elemzésére, és valós időben észlelik a szokatlan tevékenységeket. Az AI-alapú behatolás-észlelő rendszerek nemcsak az azonosításban segítenek, hanem automatizált válaszlépéseket is képesek generálni, ami jelentősen csökkenti a reagálási időt. Haig [18] szerint az AI alkalmazása jelentős előrelépést jelent

a kibervédelemben, mivel adaptív és folyamatosan fejlődő megoldást kínál a fenyegetésekre.

A kriptográfia szintén nélkülözhetetlen eszköze a kibervédelemnek. A titkosítás lehetővé teszi az adatok bizalmasságának megőrzését, még akkor is, ha azok illetéktelen kezekbe kerülnek. A modern titkosítási technikák, mint például az RSA (asszimetrikus titkosítású kulcsok) és az AES algoritmusok, hatékony védelmet nyújtanak a támadók ellen, és biztosítják az adatok integritását. Ugyanilyen fontosak a hozzáférés-kezelési rendszerek (identity and access management, IAM), amelyek garantálják, hogy csak az arra jogosult felhasználók férjenek hozzá az érzékeny információkhoz. Az IAM rendszerek, mint például a kétfaktoros hitelesítés és a szerepkör-alapú hozzáféréskezelés (role-based access control, RBAC), jelentősen csökkentik a jogosulatlan hozzáférés kockázatát, és fokozzák a rendszerbiztonságot. [30]

A kibervédelem alapjai tehát a megelőzés, a felderítés, a reagálás és a helyreállítás köré épülnek, amelyeket modern technológiák támogatnak. Ezek az elemek nemcsak a rendszerek és hálózatok védelmét szolgálják, hanem hozzájárulnak a bizalom fenntartásához is a digitális társadalomban. Ahogy a kibertér fenyegetései tovább fejlődnek, úgy kell a védekezési stratégiáknak is adaptálódniuk. Ezért elengedhetetlen a folyamatos innováció, a technológiai eszközök fejlesztése és a szakemberek képzése, hogy hatékonyan megvédhessük a digitális világunkat a jövő kihívásaival szemben.

A kibervédelem egyre összetettebbé válik, ahogy a digitális világban megjelenő fenyegetések száma és komplexitása folyamatosan növekszik. Az eredményes védekezés érdekében elengedhetetlen a különböző szereplők szoros együttműködése. Az állami, a magánszektorbeli és az egyéni szinten megvalósuló kibervédelem mind hozzájárul a digitális infrastruktúrák biztonságához és a társadalom stabil működéséhez. A kibervédelemben részt vevő szereplők feladatai és felelősségi körei különböznek, de közös céljuk a kibertér védelme és a fenyegetések minimalizálása.

Az állami szereplők kiemelkedő szerepet játszanak a kibervédelemben, hiszen az államok felelősek a nemzeti infrastruktúrák védelméért, ideértve az energiatermelést, a közlekedést és az egészségügyi rendszereket. Az állami kormányzatok speciális kibervédelmi ügynökségeket hoztak létre, például Magyarországon a Nemzeti Kibervédelmi Intézetet, amelyek feladata a kiberbiztonsági fenyegetések felderítése, az incidensek kezelése és a nemzeti szintű védelem biztosítása. [19] Az államok katonai és

nemzetbiztonsági szervezetei szintén aktívan részt vesznek a kibervédelemben, hiszen a kiberhadviselés egyre gyakoribbá válik, és komoly fenyegetést jelent az országok szuverenitására és biztonságára. Nemzetközi szinten az együttműködés elengedhetetlen, hiszen a kibertér határok nélküli, és egyetlen állam sem képes egyedül megvédeni magát a globális fenyegetésekkel szemben. Az olyan nemzetközi szervezetek, mint a NATO és az Európai Unió, jelentős szerepet játszanak a nemzetközi szabványok és stratégiák kidolgozásában, amelyek megkönnyítik az államok közötti együttműködést a kibertér védelmében. [31]

A magánszektor szintén meghatározó szereplője a kibervédelemnek, különösen a technológiai cégek és szolgáltatók, mint például a Google, a Microsoft vagy az Amazon. Ezek a vállalatok nemcsak saját rendszereik és ügyfeleik védelmét biztosítják, hanem jelentős technológiai és innovációs erőforrásaik révén hozzájárulnak az iparági szabványok kialakításához és az új védelmi technológiák fejlesztéséhez. A kiberbiztonsági cégek, mint például a Kaspersky és a Symantec, kifejezetten a kiberfenyegetések azonosítására és kezelésére szakosodtak. Ezek a vállalatok speciális eszközöket és szolgáltatásokat nyújtanak, például vírusirtókat, behatolás-észlelő rendszereket és titkosítási megoldásokat, amelyek kulcsfontosságúak a kibervédelemben. A magánszektor erőfeszítései nélkül a digitális világ védelme elképzelhetetlen lenne, hiszen ezek a vállalatok nemcsak a technológiai fejlődés motorjai, hanem a kiberbiztonsági innovációk élharcosai is. [30]

Az egyéni felhasználók szintén fontos szerepet játszanak a kibervédelemben, hiszen a felhasználói szokások és a tudatosság jelentősen befolyásolják a rendszerek biztonságát. Az online fenyegetések, mint például az adathalászat vagy a zsarolóvírusok, gyakran az egyéni felhasználók figyelmetlenségét használják ki. Ezért alapvető fontosságú, hogy az emberek tisztában legyenek az online fenyegetésekkel és a megfelelő védekezési módszerekkel. A biztonságos jelszókezelés, a kétfaktoros hitelesítés alkalmazása és a gyanús e-mailek elkerülése mind hozzájárulhatnak a fenyegetések minimalizálásához. [9] Emellett az oktatási kampányok és az informatikai biztonsági tréningek növelhetik a tudatosságot, ami elengedhetetlen az egyéni és társadalmi szintű védekezéshez.

A kibervédelem különböző szintjeinek és típusainak vizsgálta is fontos a fenyegetések elleni küzdelemben. A nemzeti kibervédelem elsősorban a kritikus

infrastruktúrák védelmét célozza, amely magában foglalja a kormányzati rendszerek, az energiatermelési hálózatok és a közlekedési rendszerek biztonságát. Az ilyen rendszerek elleni támadások nemcsak anyagi károkat okozhatnak, hanem komoly társadalmi és gazdasági következményekkel is járhatnak. A nemzeti szintű védelem része a törvényi szabályozás is, például az Európai Unió által elfogadott GDPR és NIS2 irányelvek, amelyek keretet adnak az adatvédelemnek és a hálózati biztonságnak. [34]

A vállalati kibervédelem a magánszektorban működő szervezetekre fókuszál. A vállalatok hálózatai és adatai állandó célpontjai a kiberbűnözőknek, ezért elengedhetetlen a belső ellenőrzési rendszerek, például az auditok és a penetrációs tesztelések alkalmazása. A vállalati szintű védekezés célja nemcsak a támadások megelőzése, hanem a károk minimalizálása és a működés folyamatosságának biztosítása is. Az egyéni kibervédelem pedig a magánfelhasználók biztonságára összpontosít, különös tekintettel a mobileszközök védelmére és az adatbiztonságra. Az ilyen szintű védelemhez hozzátartozik a felhasználók oktatása és a tudatosság növelése is, hiszen az informált felhasználók jobban képesek megvédeni magukat az online fenyegetésekkel szemben. [30]

A kibervédelem szereplői tehát különböző szinteken működnek együtt annak érdekében, hogy a digitális tér biztonságos és fenntartható maradjon. Az állami és magánszektorbeli szereplők technológiai és szervezeti hátteret biztosítanak, míg az egyéni felhasználók aktív részvétele hozzájárul az átfogó védelemhez. A kibervédelem hatékonysága azonban csak akkor érhető el, ha a különböző szintek összehangoltan működnek, és a technológiai fejlesztések, a szabályozási keretek és a tudatosság egyaránt hozzájárulnak a fenyegetések elleni küzdelemhez.

A kibervédelem kihívásai és jövője olyan témák, amelyek folyamatosan napirenden vannak a technológiai fejlődés és a globális fenyegetettségek miatt. A digitális világ térnyerésével a kibertámadások egyre változatosabb formákat öltenek, miközben az információbiztonság fenntartása bonyolultabbá válik. A kibervédelem nem csupán az aktuális fenyegetésekre adott reakciókat jelenti, hanem a jövőbeni kihívásokra való felkészülést is, amelyek jelentősen átalakíthatják a digitális tér védelmének stratégiáját.

A kibervédelem egyik legnagyobb kihívása a fenyegetések gyors változása. Az új típusú támadások, mint például a mesterséges intelligencia által vezérelt támadások vagy a deepfake technológiák, új dimenziót nyitnak a kiberbiztonság területén. A deepfake

technológia például a digitális manipuláció révén képes valósághű, de hamis információkat létrehozni, amelyek komoly károkat okozhatnak a személyek hírnevében, a vállalatok működésében vagy akár politikai válságokban is szerepet játszhatnak. [18]

Hasonlóképpen, az AI-alapú támadások új szintre emelik a kiberfenyegetéseket, mivel ezek az algoritmusok képesek tanulni és adaptálódni, így nehezebb felismerni és megállítani őket. A globális hackercsoportok aktivitása tovább fokozza a fenyegetettséget, hiszen ezek a szervezetek gyakran jól szervezettek és jelentős erőforrásokkal rendelkeznek, amelyekkel komoly károkat okozhatnak nemzeti és nemzetközi szinten is. [35]

A technológiai fejlődés újabb kihívásokat támaszt a kibervédelemben. A kvantumszámítógépek megjelenése például alapjaiban rengetheti meg a jelenlegi titkosítási rendszerek biztonságát. A kvantumalgoritmusok képesek lehetnek gyorsan feltörni azokat a titkosítási módszereket, amelyek ma a legbiztonságosabbnak számítanak, például az RSA vagy az AES titkosításokat. [36] Ez komoly kockázatot jelent az adatbiztonságra, hiszen a kritikus információk védelme jelenleg ezeken a rendszereken alapul. Az IoT, vagyis a dolgok internete szintén jelentős kihívást jelent. Az IoT-eszközök széles körű elterjedése új sebezhetőségeket hozott létre, mivel ezek az eszközök gyakran nem rendelkeznek megfelelő védelmi mechanizmusokkal, és könnyen célponttá válhatnak a támadók számára. Az IoT-hálózatok gyengeségei nemcsak az egyéni eszközöket, hanem a teljes rendszereket veszélyeztethetik, amelyek gyakran kritikus infrastruktúrákhoz, például energiahálózatokhoz vagy egészségügyi rendszerekhez kapcsolódnak. [37]

A jövőben a kibervédelemben egyre nagyobb szerepet kap az automatizáció. Az automatizált védelmi rendszerek képesek valós időben észlelni a kibertámadásokat, és azonnal reagálni rájuk, így jelentősen lerövidítik a válaszidőt és csökkentik a lehetséges károkat. Ezek a megoldások mesterséges intelligenciára és gépi tanulásra épülnek, amelyek folyamatosan elemzik a tapasztalatokat, tanulnak az új támadási módszerekből, és egyre hatékonyabban alkalmazkodnak a változó fenyegetésekhez. [38] Emellett a nemzetközi szabványok és szabályozások erősítése is kulcsfontosságú, hiszen a kibertér globális jellege miatt a nemzeti szintű intézkedések önmagukban nem elegendőek. Az Európai Unió GDPR és NIS2 irányelvei jó példái annak, hogyan lehet egységes kereteket

biztosítani a hálózati biztonság és az adatvédelem területén, de hasonló szabályozásokra van szükség világszerte.

A kiberhadviselés veszélye szintén a jövő egyik legnagyobb kihívása. A digitális térben zajló konfliktusok nemcsak a hagyományos katonai stratégiák kiterjesztését jelentik, hanem teljesen új eszközöket és módszereket is magukkal hoznak. Az államilag támogatott kibertámadások, amelyek célja például kritikus infrastruktúrák megbénítása, súlyos gazdasági és társadalmi következményekkel járhatnak. A kiberhadviselés kezeléséhez nemzetközi együttműködésre van szükség, amely magában foglalja a közös védelmi stratégiák kidolgozását, az információmegosztást és a gyors reagálási képesség fejlesztését. A NATO és más nemzetközi szervezetek már jelenleg is dolgoznak ilyen irányú kezdeményezéseken, de ezek hatékonysága nagyban múlik a résztvevő országok közötti együttműködés szintjén. [39]

A kibervédelem jövője tehát számos kihívással néz szembe, amelyek megoldása nemcsak technológiai innovációt, hanem társadalmi és politikai összefogást is igényel. A fenyegetések gyors változása, a technológiai fejlődés új dimenziói és a globális együttműködés szükségessége mind hozzájárulnak ahhoz, hogy a kibervédelem folyamatos fejlődést követeljen meg. A hatékony védekezéshez elengedhetetlen a tudatosság növelése, az oktatás fejlesztése, valamint az új technológiák integrációja, amelyek lehetővé teszik a fenyegetések gyors felismerését és kezelését.

1.5. A közösségi média kiberbiztonsági szempontú elemzése

A közösségi média fogalmának pontos meghatározása évek óta folyamatos vita tárgyát képezi. Elsőre egyszerűnek tűnhet a válasz, hiszen sokan a legismertebb közösségi hálózatokat, például a Facebookot vagy a LinkedInt tekintik a közösségi média prototípusának. Azonban, ha mélyebben megvizsgáljuk a kérdést, felmerül, hogy vajon a tartalomgyártásra és megosztásra szolgáló platformok, mint például az Instagram vagy a TikTok, ugyanúgy közösségi médiának számítanak-e. Mi a helyzet a blogokkal, fórumokkal vagy éppen a YouTube-bal? Ez a kérdéskör arra ösztönöz, hogy áttekintsük a közösségi média fogalmát különböző szempontokból és definíciókból kiindulva.

Az Investopedia [40] meghatározása szerint a közösségi média olyan számítógép-alapú technológia, amely lehetővé teszi az ötletek, gondolatok és információk megosztását virtuális hálózatokon és közösségeken keresztül. Ezt a definíciót tovább finomítja a Hanna és Lutkevich [41], amely a közösségi médiát a kommunikációra,

közösségi alapú bevitelre, interakcióra, tartalommegosztásra és együttműködésre összpontosító webhelyek és alkalmazások gyűjtőfogalmának nevezi. Ezek a definíciók rávilágítanak arra, hogy a közösségi média elsődleges funkciója az interakció és a közös információcsere lehetőségének biztosítása, ami azonban nem minden platform esetében valósul meg azonos módon.

Az elmúlt években a közösségi média fogalma folyamatosan alakult, párhuzamosan az online technológiák fejlődésével és a felhasználói szokások változásával. Kaplan és Haenlein 2010-es tanulmánya ebben a témában különösen fontos megközelítést kínál, mivel a közösségi médiát olyan internetes alkalmazások csoportjaként határozzák meg, amelyek a web 2.0 technológiai alapjaira épülnek. [42] Ez a meghatározás nemcsak a technológiai hátteret hangsúlyozza, hanem kiemeli a felhasználók aktív szerepét is, hiszen a tartalmak létrehozása és átalakítása központi elemként jelenik meg. Bár a web 2.0 fogalma mára részben háttérbe szorult, az általa képviselt alapelvek, mint a közösségi jelleg, az interaktivitás és az együttműködés, továbbra is alapvetően meghatározzák az online platformok működését.

A web 2.0 technológiák megjelenése az internet egy olyan korszakát nyitotta meg, ahol a felhasználók nem csupán passzív tartalomfogyasztók, hanem aktív résztvevők lettek. Ez az átalakulás tette lehetővé a közösségi média térnyerését, hiszen a tartalomgyártás és megosztás olyan eszközöket kapott, amelyek az egyéni kreativitást és az interakció lehetőségét helyezték előtérbe. Kaplan és Haenlein [42] továbbá kiemelik, hogy ezek az eszközök nem csupán a közvetlen kommunikációra szolgálnak, hanem olyan dinamikus folyamatokat indítanak el, amelyek során a tartalom új értelmet nyerhet. A tartalmak átalakítása az online kommunikáció egyik alapvető jellemzőjévé vált.

Ez a folyamat különösen meghatározó a befolyásolási célú műveletek során, mint amilyenek a pszichológiai hadviseléshez kapcsolódó PSYOPS-akciók is, ahol az információ tudatos manipulálásával próbálják befolyásolni a kiválasztott célcsoportokat. Dunlap 2014-es megállapítása szerint a közösségi média által kínált lehetőségek, például az úgynevezett hiperszemélyesítés, vagyis az egyénekhez igazított üzenetek létrehozása és terjesztése, új távlatokat nyitott a befolyásolás terén. [4] Az üzenetek új kontextusba helyezése nemcsak az információk hatékonyságát növeli, hanem lehetővé teszi azt is, hogy a tartalom kifejezetten a célközönség érzelmeire és véleményformálási folyamataira hasson.

Az ilyen manipuláció lehetősége azonban komoly etikai és társadalmi kérdéseket is felvet. Míg a közösségi média eredeti célja a szabad kommunikáció és az információmegosztás elősegítése volt, mára egyre nyilvánvalóbbá vált, hogy ezek az eszközök milyen mértékben használhatók az információ torzítására és dezinformáció terjesztésére. Kaplan és Haenlein [42] definíciója ugyanakkor arra is rámutat, hogy a felhasználók nem csupán passzív befogadók, hanem aktív szereplők is az online térben. Ez azt jelenti, hogy a manipulációval szemben is rendelkeznek bizonyos eszközökkel, például kritikus gondolkodással és az információ forrásának ellenőrzésével.

A közösségi média dinamikája tehát egy kettős folyamatot tükröz: egyrészt lehetőséget biztosít a szabad kommunikációra és a kreatív önkifejezésre, másrészt eszközt ad a manipuláció és az információ torzításának kezébe. Ez a kettősség teszi különösen izgalmassá és kihívásokkal telivé a közösségi média szerepének vizsgálatát a modern társadalomban. Kaplan és Haenlein [42] meghatározása ezen a téren egy olyan alapot kínál, amely megérteti velünk a közösségi média technológiai és társadalmi jelentőségét, miközben felhívja a figyelmet a folyamatosan változó digitális környezet kihívásaira is.

A közösségi média fogalmának értelmezése az elmúlt években számos megközelítést szült, hiszen az online kommunikáció és tartalomgyártás dinamikus fejlődése folyamatosan formálja annak határait. Nagy [43] egyedi perspektívát kínál a közösségi média definíciójához. Ő a közösségi médiát elsősorban a felhasználók által létrehozott tartalomhoz köti, amelyet széles körben hozzáférhető technológiák tesznek lehetővé, és amelyek megkönnyítik a kommunikációt és az interakciót. Ez a definíció nem csupán a tartalommegosztásra helyezi a hangsúlyt, hanem az interakciók és a visszacsatolás fontosságát is kiemeli. Nagy meglátása szerint a közösségi média nem statikus jelenség, hanem egy folyamatosan fejlődő dinamikus ökoszisztéma, amelyet a felhasználók aktivitása és az új technológiák alakítanak.

A közösségi médiát sokáig elsősorban mint tartalommegosztási eszközt tekintették. Azonban Nagy [43] definíciója rávilágít arra, hogy a közösségi média ennél jóval több. Az interakció és a visszacsatolás lehetősége révén a felhasználók nemcsak passzív befogadók, hanem aktív szereplők, akik hozzájárulnak a platformokon zajló kommunikáció folyamatos átalakulásához. Ez az aspektus különösen fontos, mivel a tartalmak nemcsak önmagukban léteznek, hanem a felhasználók által új kontextusba

helyezve új jelentésekkel gazdagodhatnak. Ez a folyamat teszi a közösségi médiát igazán dinamikussá és sokszínűvé.

Klausz 2016-os könyve tovább gazdagítja a közösségi média meghatározását, mivel részletes tipológiát nyújt, amely segít mélyebben megérteni ezeknek a platformoknak a különféle funkcióit. A szerző öt különböző típust különít el, amelyek révén pontosabb képet kaphatunk a közösségi média sokrétű szerepéről. Az első kategóriába tartoznak a blogok, amelyek lehetőséget adnak az egyéni gondolatok és vélemények közzétételére, akár írott, akár videós formában. Olyan platformok, mint a Tumblr vagy a WordPress, lehetőséget biztosítanak arra, hogy a felhasználók saját identitásukat és nézőpontjukat megosszák a nyilvánossággal. Ebbe a csoportba sorolhatók a mikroblogok is, mint például az X, korábbi nevén Twitter, amelyek a rövid és tömör közlésekre épülő kommunikációs formát részesítik előnyben. [44]

A második kategória a közösségi hálózatoké, amelyek talán a legismertebb képviselői a közösségi médiának. Ilyen platformok például a Facebook, a LinkedIn vagy a TikTok. Ezek a hálózatok lehetővé teszik a személyes profilok létrehozását, ahol a felhasználók tartalmakat oszthatnak meg, kapcsolatokat építhetnek és közösségeket hozhatnak létre az azonos érdeklődésű emberek között. Ezen platformok egyik legfontosabb jellemzője az interakció lehetősége, legyen szó hozzászólásokról, megosztásokról vagy az azonnali üzenetküldésről. Ez az interaktív jelleg az, ami a közösségi hálózatokat igazán vonzóvá teszi. [44]

A harmadik kategóriát Klausz a tartalom alapú közösségi felületeknek nevezi. Ezek a platformok az azonos érdeklődésű felhasználók számára kínálnak lehetőséget a közös tartalomgyártásra. Ez a kategória különösen izgalmas, mivel nemcsak a tartalom megosztására, hanem annak közös fejlesztésére is alkalmas. A videók, képek vagy dokumentumok megosztása és szerkesztése új dimenziót nyit a közösségi média használatában. [44]

A fórumok, mint a Reddit vagy a Quora, Klausz negyedik kategóriáját képezik. Ezek a platformok az ötletek és információk megosztására szolgálnak, miközben lehetőséget nyújtanak arra, hogy az azonos érdeklődésű felhasználók csoportokat alkossanak. A fórumok egyik különlegessége, hogy a beszélgetések gyakran tematikusak, így a felhasználók mélyebb, tartalmasabb párbeszédeket folytathatnak egy adott témáról. [44]

Az utolsó kategória a tartalomgenerátoroké, amelyek közé olyan eszközök tartoznak, mint az RSS-alapú alkalmazások[3], például a Microsoft Flow vagy az Integromat. Ezek a platformok automatizálják a tartalomkészítést és -megosztást, megkönnyítve a felhasználók számára a folyamatos jelenlét fenntartását a közösségi médiában. Bár ezek a platformok kevésbé interaktívak, fontos szerepet játszanak az információ áramlásának biztosításában. [44]

Klausz kategorizálása nemcsak a közösségi média sokszínűségét mutatja meg, hanem azt is, hogy ezek a platformok hogyan szolgálhatják a különböző felhasználói igényeket. A közösségi média tehát nem egy homogén jelenség, hanem egy rendkívül komplex ökoszisztéma, amelyben különböző típusú platformok és funkciók találkoznak. [44] Nagy (2012) és Klausz (2016) meglátásai együtt egy átfogó képet nyújtanak arról, hogy a közösségi média miként formálja a kommunikációt, az interakciót és a tartalomfogyasztást a modern társadalomban.

Ezek az elemzések nemcsak a közösségi média jelenlegi helyzetét segítenek megérteni, hanem a jövőbeni fejlődési irányok felvázolásához is hozzájárulnak. A közösségi média folyamatosan változik, ahogy a technológiai lehetőségek bővülnek és a felhasználói szokások alakulnak. Az interakció és a visszacsatolás, amelyeket Nagy (2012) kiemel, továbbra is központi szerepet játszik, míg Klausz (2016) kategorizálása segít abban, hogy jobban megértsük a különböző platformok funkcióit és jelentőségét a digitális világban.

1.6. Részkövetkeztetések

A közösségi média alapvetően átalakította a modern társadalmi és katonai kommunikációs környezetet. Az online platformok nem csupán a hétköznapi kapcsolattartás eszközei, hanem **stratégiai jelentőségű terekké váltak**, amelyek új lehetőségeket és kihívásokat is teremtenek. A **közösségi média** szabályozatlansága és globális elérhetősége révén **különösen fontos szerepet játszik az információs műveletekben**, ahol állami és nem állami szereplők tájékoztatási és befolyásolási célokra egyaránt alkalmazzák. A platformok egyszerre nyújtanak lehetőséget az információs fölény megszerzésére, valamint az ellenség manipulációjára és destabilizálására.

[3] Az **RSS alapú alkalmazások** (gyakran RSS-olvasók vagy feed-olvasók) olyan szoftverek, webes szolgáltatások vagy mobilapplikációk, amelyek lehetővé teszik a felhasználók számára, hogy egy központi felületen kövessék, rendszerezzék és olvassák különböző weboldalak, blogok, hírportálok friss tartalmait (RSS feedjeit). [147]

A fejezetben bemutattam és elemeztem, hogy a közösségi média olyan dinamikus eszközként működik, amely a gyors információáramlást, az interaktivitást és a széleskörű tájékoztatást támogatja. A katonai alkalmazás során a közösségi média segíthet a nyilvánosság informálásában, a morális támogatás fenntartásában, ugyanakkor jelentős kiberbiztonsági kockázatokat is hordoz. Az ellenséges szereplők adathalászatot, álhírek terjesztését és érzékeny információk kiszivárogtatását végezhetik a platformokon keresztül.

A közösségi média alkalmazása a modern hadviselésben továbbá számos etikai kérdést is felvet, például a dezinformációs kampányok és a propaganda igazságosságát és hatását illetően. Az etikus kommunikáció elvei – az átláthatóság és a hitelesség – kulcsszerepet játszanak a közösségi média katonai alkalmazásának szabályozásában. Megállapítottam, hogy az **átfogó stratégiák kidolgozása** és az **innovatív technológiai megoldások alkalmazása** elengedhetetlen ahhoz, hogy a **közösségi média előnyeit maximalizálják, miközben a kockázatokat minimalizálják**.

2. FEJEZET
KÖZÖSSÉGI MÉDIA SZEREPE AZ INFORMÁCIÓS MŰVELETEKBEN

A közösségi média napjainkban nem csupán a hétköznapi kommunikáció egyik legfontosabb eszköze, hanem stratégiai jelentőségű platformként is működik a modern információs hadviselésben. Az online tér folyamatosan bővülő lehetőségei az információs műveletek minden aspektusában, a hírszerzéstől kezdve a befolyásolási kampányokig, kulcsszerepet kaptak. A közösségi média dinamikája – gyors információáramlás, széleskörű elérhetőség, valamint az interakció és az adaptáció lehetősége – új dimenziókat nyitott az információs műveletekben. Mindezek révén az állami és nem állami szereplők számára is hatékony eszközzé vált a stratégiák megvalósításában.

A fejezet célja, hogy bemutassa a közösségi média szerepét az információs műveletek különböző területein. A közösségi média hírszerzési és felderítési alkalmazásai például a nyílt forrású információk (OSINT) gyűjtésétől kezdve az adatelemzésig terjednek, amelyek a stratégiai döntéshozatalt támogatják. Emellett vezetés és irányításiban (C2) betöltött szerepe is egyre hangsúlyosabb, hiszen a platformok lehetővé teszik az azonnali információmegosztást és koordinációt.

A befolyásolási műveletek során a közösségi média a narratívák formálásának és az ellenséges célpontok pszichológiai gyengítésének eszköze. Ugyanakkor az olyan területeken, mint a célmegjelölés és célravezetés, valamint a kibertér műveletek, a platformok hatékonysága megkérdőjelezhetetlen. Az aktív védelem koncepciója, amely magában foglalja a veszélyek és fenyegetések időben történő felismerését és kezelését, szintén egyre inkább integrálódik a közösségi média felhasználási területei közé.

E fejezet nemcsak az alkalmazási területek részletes vizsgálatára vállalkozik, hanem rávilágít a közösségi média kínálta lehetőségek és veszélyek közötti finom egyensúlyra is. Az elemzések célja, hogy megértsük, hogyan használható a közösségi média az információs műveletek során, és milyen kihívásokat kell leküzdeni ahhoz, hogy ezeket az eszközöket hatékonyan és biztonságosan lehessen alkalmazni a modern hadviselésben.

2.1. Közösségi média és a hírszerzési/felderítési műveletek

A közösségi média napjainkban a globális kommunikáció és adatáramlás egyik legfontosabb platformjává vált. Az olyan népszerű felületek, mint a Facebook, az X vagy az Instagram, lehetővé teszik az információk valós idejű megosztását, ezáltal hozzájárulva egy határok nélküli kommunikációs tér kialakulásához. [42] Ezek a technológiai eszközök nemcsak a mindennapi életünkre gyakorolnak hatást, hanem a nemzetbiztonság és a hadviselés területén is új lehetőségeket és kihívásokat teremtenek.

A hírszerzés és a felderítési műveletek szempontjából a közösségi média kettős szerepet játszik. Egyrészt óriási adatforrást biztosít a nyílt forrású hírszerzés (OSINT) számára, amely révén a szakemberek nyilvánosan elérhető információk alapján készítenek elemzéseket és következtetéseket. Például a felhasználói aktivitások, helymeghatározási adatok vagy a kapcsolati hálók vizsgálata rendkívül értékes betekintést nyújthatnak egy adott célcsoport viselkedésébe vagy szándékaiba. [32] Másrészt a közösségi média gyakran válik célponttá különböző kiberbiztonsági fenyegetések és információs hadviselési taktikák számára. Az álhírek terjesztése, a dezinformációs kampányok és a pszichológiai műveletek mind olyan stratégiák, amelyek a közösségi média sebezhetőségét használják ki. [5]

A modern hírszerzési műveletekben a közösségi média alkalmazása különösen a big data és a mesterséges intelligencia által vezérelt eszközök fejlődésével vált kiemelt jelentőségűvé. Az automatizált rendszerek képesek hatalmas mennyiségű adat gyors feldolgozására és elemzésére, így az információgyűjtés hatékonyságát nagymértékben növelik. [4] Az ilyen technológiák ugyanakkor etikai és jogi kérdéseket is felvetnek, különösen a személyes adatok védelme és a magánszféra tiszteletben tartása terén.

A közösségi média a nyílt forrású hírszerzés (OSINT) egyik legértékesebb területévé vált az elmúlt években, köszönhetően annak, hogy hatalmas mennyiségű, nyilvánosan elérhető adatot biztosít. Az olyan platformok, mint a Facebook, az X, az Instagram vagy a LinkedIn, nemcsak személyes információkat tartalmaznak, hanem a felhasználók tevékenységére, kapcsolataira és preferenciáira vonatkozó adatokat is, amelyeket megfelelő elemzéssel hírszerzési célokra lehet hasznosítani. Az OSINT eszközei lehetővé teszik ezen nyílt forrású adatok összegyűjtését, rendszerezését és elemzését, amelyeket mind kormányzati, mind magánszervezetek széles körben használnak a nemzetbiztonsági és üzleti célok érdekében. [5]

Az adatgyűjtés során a közösségi média különféle aspektusait veszik figyelembe. Egyik kiemelt terület a felhasználói viselkedési minták elemzése, amely során a platformokon végzett aktivitásokból következtetnek az egyének vagy csoportok szokásaira, érdeklődési körére és viselkedési dinamikájára. [45] A helymeghatározási adatok (geolokáció) szintén fontos szerepet játszanak a hírszerzésben, hiszen ezek alapján pontosan beazonosítható, hogy a felhasználók mikor és hol tartózkodtak. Az ilyen információk különösen értékesek válsághelyzetek, például konfliktuszónák elemzésekor. [46] A kapcsolati hálók feltérképezése pedig lehetővé teszi a befolyásos szereplők azonosítását egy adott közösségen belül, amely stratégiai előnyt jelenthet például terrorista sejtek vagy bűnszervezetek elleni fellépés során. [47]

A kulcsszavak és metaadatok elemzése révén a hírszerzők pontosabb képet alkothatnak a közösségi média aktivitásokról. Az ilyen elemzések során speciális algoritmusokat alkalmaznak az információk feldolgozására és osztályozására, amelyek segítségével azonosítani lehet azokat a mintázatokat vagy anomáliákat, amelyek potenciális fenyegetésekre utalhatnak. [48] Ez a technológiai megközelítés a nagy adathalmazok kezelésének hatékony módszere, amely gyors és precíz döntéshozatalt tesz lehetővé.

Az adatgyűjtés és elemzés hatékonyságát nagymértékben növelik az automatizált eszközök és a mesterséges intelligencia (AI) technológiák. Az automatizált adatgyűjtés, például scraping technológiák[4] alkalmazása lehetővé teszi a nagy mennyiségű információ gyors összegyűjtését és rendszerezését. A chatbotok és más mesterséges intelligencia alapú rendszerek nemcsak az adatgyűjtést segítik, hanem az elemzési folyamatokat is támogatják azáltal, hogy képesek az információk összefüggéseinek gyors felismerésére. [49] A gépi tanulási algoritmusok például hatékonyan azonosítják a különböző mintázatokat, előrejelzéseket készítenek, és az anomáliák felismerésével segítenek a potenciális fenyegetések azonosításában. [50]

A közösségi média által biztosított adatok és az ezeket feldolgozó technológiák kombinációja tehát kiemelt jelentőségűvé vált az OSINT területén. Ezek az eszközök nemcsak a hagyományos hírszerzési módszereket egészítik ki, hanem új dimenziókat is

[4] A scraping, vagy web scraping egy olyan technológiai folyamat, amelynek során automatizált eszközökkel adatokat gyűjtenek le weboldalakról. Ez az eljárás lehetővé teszi, hogy strukturálatlan adatokat (például egy honlap HTML-kódját) strukturált formába (például táblázatokba, adatbázisokba) rendezzünk további elemzés vagy felhasználás céljából. (Columbia University, n.d.)

nyitnak a fenyegetések felismerésében és kezelésében, hozzájárulva ezzel a nemzetbiztonság és az üzleti döntéshozatal hatékonyságához.

A közösségi médián alapuló hírszerzés számos lehetőséget kínál, azonban komoly kihívásokkal is szembesül. Az egyik legfontosabb akadályt az adatvédelem és a jogi korlátok jelentik. A személyes adatok védelme egyre hangsúlyosabb kérdés, különösen az Európai Unió által bevezetett Általános Adatvédelmi Rendelet (General Data Protection Regulation - GDPR) hatálybalépése óta, amely szigorú előírásokat fogalmaz meg az adatok gyűjtésére és kezelésére vonatkozóan. Az ilyen szabályozások komoly etikai dilemmákat is felvetnek, hiszen a hírszerzők számára gyakran nehéz egyensúlyt találni az adatok felhasználása és a magánszféra tiszteletben tartása között. [51] Továbbá, az adatgyűjtés jogszabályi keretei jelentős eltéréseket mutatnak különböző országokban, ami bonyolultabbá teszi a globális hírszerzési műveletek végrehajtását és az információk feldolgozását. [52]

A dezinformáció és félrevezetés szintén súlyos problémát jelent a közösségi médián alapuló hírszerzésben. Az álhírek és hamis információk terjedése nemcsak a közvélemény befolyásolását célozza, hanem gyakran a hírszerzési műveletek hatékonyságát is aláássa. Az ilyen jellegű dezinformációs kampányok célja gyakran a döntéshozók és elemzők félrevezetése, amely stratégiai hibákhoz vezethet. [53] A deepfake technológiák további veszélyt jelentenek, mivel rendkívül hitelesnek tűnő, ám hamis vizuális és audió tartalmak előállítását teszik lehetővé, amelyek a manipuláció új dimenzióját nyitják meg. Ezek a technológiák nemcsak a közösségi médiát, hanem a hagyományos hírszerzési folyamatokat is kihívás elé állítják. [5]

Az adatok hitelességének és relevanciájának ellenőrzése szintén kulcsfontosságú probléma a közösségi médiából származó információk esetében. Az ilyen forrásokból származó adatok sokszor pontatlanok, hiányosak vagy irrelevánsak, ami megnehezíti az elemzési folyamatot és növeli a hamis pozitív vagy hamis negatív eredmények előfordulását. [32] Ez különösen kritikus olyan helyzetekben, ahol az időérzékeny döntéshozatal elengedhetetlen, például válságkezelés vagy terrorizmus elleni műveletek során. Az adatok hitelességének biztosítása ezért elengedhetetlen, és olyan fejlett technológiák alkalmazását igényli, mint a mesterséges intelligencia és a gépi tanulás, amelyek képesek az anomáliák gyors felismerésére és az adatok minőségének ellenőrzésére. [4]

A közösségi médián alapuló hírszerzés hatékonyságának növelése érdekében ezekre a kihívásokra átfogó és innovatív megoldásokra van szükség. Az adatvédelem és az etika tiszteletben tartása mellett a fejlett technológiák és módszertanok alkalmazása kulcsfontosságú annak érdekében, hogy az ilyen típusú hírszerzés fenntartható és eredményes maradhasson.

A közösségi média adatainak integrálása a modern hírszerzési rendszerekbe jelentős előrelépést hozott a nemzetbiztonság és a konfliktuskezelés területén. Az olyan technológiák, mint a big data és a mesterséges intelligencia (MI), lehetővé teszik a hatalmas mennyiségű közösségimédia-adat hatékony feldolgozását és elemzését, amelyekből értékes információk nyerhetők. A hírszerző rendszerek egyre inkább támaszkodnak ezekre az eszközökre, hogy az információgyűjtés gyorsabb és pontosabb legyen. Az MI-alapú rendszerek képesek automatizált mintázatfelismerésre, anomáliaészlelésre és előrejelzések készítésére, miközben a big data analitika továbbfejlesztése lehetőséget nyújt a még komplexebb adathalmazok kezelésére. [54]

A jövőbeli innovációk között fontos szerepet játszanak az olyan technológiák, mint a metaverzum, az AR (kiterjesztett valóság) és a VR (virtuális valóság). Ezek a platformok újabb dimenziókat nyitnak a hírszerzésben, különösen a szimulációs környezetek, a valós idejű adatelemzés és a kiképzési programok területén. [55] A decentralizált platformok, például a blokklánc-technológiák, azonban új kihívásokat is jelentenek, mivel ezek az adatok titkosítását és elérhetetlenségét eredményezhetik, ami megnehezíti a hagyományos hírszerzési módszerek alkalmazását. A decentralizált rendszerek és a teljes anonimitás iránti növekvő igény új stratégiák kidolgozását teszi szükségessé a hírszerzési közösség számára. [56]

A közösségi média hírszerzésben betöltött stratégiai jelentősége vitathatatlan, hiszen lehetőséget kínál a gyors és hatékony információgyűjtésre, az adatvezérelt döntéshozatalra, valamint a fenyegetések előrejelzésére. Ugyanakkor elengedhetetlen, hogy az adatgyűjtési és -feldolgozási folyamatok során nagy hangsúlyt kapjon az etikai és jogi szempontok figyelembevétele. A személyes adatok védelme, a magánszféra tiszteletben tartása, valamint az átlátható szabályozások kialakítása kulcsfontosságú a közösségi média hírszerzésben való fenntartható alkalmazásához. [57]

A jövőben az innováció és az adatvédelem közötti egyensúly megteremtése lesz a legnagyobb kihívás. A technológiai fejlődés lehetővé teszi a hírszerző rendszerek

számára, hogy hatékonyabban működjenek, azonban a túlzott adatgyűjtés és a visszaélések kockázata veszélyezteti a közbizalmat. Az új technológiák bevezetése és alkalmazása során elengedhetetlen az átláthatóság, az etikus magatartás, valamint a jogszabályi megfelelőség biztosítása. Csak így lehet a közösségi média hírszerzésben betöltött szerepét hosszú távon fenntarthatóvá és elfogadhatóvá tenni.

2.2. Közösségi média és C2

A C2 (Command and Control) rendszerek a modern hadviselés és hírszerzési műveletek központi elemei, amelyek lehetővé teszik a katonai egységek és hírszerzési operatív csapatok számára, hogy hatékonyan koordinálják tevékenységeiket a különböző hadszíntereken, vagy műveleti területeken. Ezek a rendszerek az információgyűjtés, -feldolgozás és -megosztás folyamatát foglalják magukban, miközben biztosítják a gyors döntéshozatal és az azonnali reagálás képességét. Az új technológiák, mint például a big data, a mesterséges intelligencia és a valós idejű kommunikáció, radikálisan átalakították a C2 rendszerek működését, különösen a konfliktusok során. A közösségi média megjelenése azonban új dimenziót adott ezeknek a rendszereknek, egyszerre kínálva lehetőségeket és kihívásokat a modern hadviselés számára. [5]

A közösségi média forradalmasította a kommunikációt, és lehetőséget teremtett a C2 rendszerek számára, hogy valós idejű információkat szerezzenek be a konfliktuszónákból. A különböző platformokon keresztül gyűjtött adatok, például a felhasználók által megosztott képek, videók és geolokációs információk, értékes információkkal szolgálhatnak a katonai döntéshozók számára. Ezek az adatok nemcsak a helyzetismeret javítására használhatók, hanem a döntéshozatal támogatására is, lehetővé téve a gyors és hatékony műveleti koordinációt. [58]

Ugyanakkor a közösségi média integrációja a C2 rendszerekbe jelentős biztonsági kockázatokat is rejt magában. Az információk kiszivárgásának veszélye és a hamis információk terjedése alááshatja a rendszerek megbízhatóságát, miközben a dezinformációs kampányok célzottan zavarhatják meg a katonai műveleteket. [59] Az orosz-ukrán konfliktus példája rávilágít arra, hogy a közösségi média miként válhat a hibrid hadviselés eszközévé, amikor az ellenséges erők célzott pszichológiai és információs műveleteket hajtanak végre a közösségi médián keresztül. [58]

A C2 rendszerek jövője szorosan összefügg a közösségi média folyamatos fejlődésével és az új technológiák integrációjával. A mesterséges intelligencia és a gépi

tanulás lehetőséget kínál arra, hogy a C2 rendszerek hatékonyabban kezeljék a közösségi médiából származó adatokat, miközben minimalizálják a hamis információk hatását. Az új generációs technológiák, mint az AR/VR, tovább növelhetik a műveleti hatékonyságot és a valós idejű helyzetismeretet, azonban az adatvédelem és a kibertámadások elleni védelem továbbra is kritikus szempontok maradnak. [60]

A közösségi média jelentős hatást gyakorolt a modern C2 rendszerek működésére, különösen a valós idejű információmegosztás, helymeghatározás és hálózati együttműködés területén. A különböző platformok lehetővé tették a gyors információáramlást, amely alapvetően átalakította a katonai és hírszerzési műveletek végrehajtásának dinamikáját. [61]

A közösségi média, mint gyors információáramlási felület, új dimenziót nyitott a valós idejű kommunikációban a C2 rendszereken belül, hiszen a felhasználók által létrehozott tartalmak, például fényképek, videók vagy szöveges bejegyzések azonnal hozzáférhetők és hatékonyan felhasználhatók a helyzetek gyors értékeléséhez. Ez a lehetőség különösen nagy jelentőséggel bír az operatív és stratégiai szintű döntéshozatal során, mivel elősegíti a gyorsabb és pontosabb reagálást olyan helyzetekben, amelyek folyamatosan változnak. A közösségi média eszközei lehetőséget adnak arra, hogy a parancsnokok és az elemzők friss és időérzékeny információkra támaszkodva hozzák meg döntéseiket, miközben csökken az információk késedelmes eljutásából eredő kockázat. [62]

A helymeghatározás és a helyzetismeret területén a közösségi média használata szintén alapvető változásokat hozott. A geolokációs adatok, amelyeket a felhasználók által készített bejegyzések vagy a készülékek GPS-adatai révén érhetők el, lehetővé teszik az egyének és események pontos helyének azonosítását. Ezek az adatok hasznosak a katonai műveletek tervezésében és végrehajtásában, különösen olyan helyzetekben, ahol a gyors helyzetismeret kritikus fontosságú. Emellett a közösségi média lehetőséget teremt valós idejű térképek és adatelemzések készítésére, amelyek segítségével a parancsnokok pontos képet kaphatnak a műveleti területekről, és hatékonyabban oszthatják ki az erőforrásokat. [63]

A hálózati együttműködés terén a közösségi média a decentralizált kommunikáció egyik alapvető eszközévé vált a C2 rendszerekben. A platformok lehetőséget kínálnak a különböző katonai egységek és szövetséges erők közötti azonnali

információmegosztásra, amely elősegíti a koordinációt és az együttműködést. A decentralizált kommunikáció különösen fontos a modern konfliktusokban, ahol a gyorsan változó helyzetek és a különböző érdekelt felek közötti hatékony együttműködés elengedhetetlen. A közösségi média lehetővé teszi, hogy a résztvevők közvetlenül kapcsolódjanak egymáshoz, megoszthassák a helyi információkat, és valós időben reagáljanak a fenyegetésekre. [64]

A közösségi média integrálása a C2 rendszerekbe számos előnnyel jár, ugyanakkor jelentős kockázatokat és kihívásokat is magában hordoz. Az információk kiszivárgása és a kibertámadások veszélye komoly fenyegetést jelentenek a C2 rendszerek működésére, miközben a dezinformáció és a manipulált tartalmak alááshatják azok hatékonyságát. [65]

Az információk kiszivárgása a közösségi médián keresztül a C2 rendszerek egyik legnagyobb biztonsági kockázata. A nyilvánosan elérhető platformok és a felhasználók által megosztott tartalmak lehetőséget adhatnak érzékeny információk megszerzésére, amelyeket ellenséges szereplők kihasználhatnak. Például katonai mozgásokkal, operatív tervekkel vagy műveleti pozíciókkal kapcsolatos információk könnyen nyilvánosságra kerülhetnek, ha azokat nem megfelelően védik. [5] Ez különösen igaz olyan helyzetekben, ahol a közösségi média eszközei valós idejű helyzetjelentések készítésére szolgálnak, hiszen ezek a jelentések ellenőrizhetetlen forrásokból származhatnak, és potenciális kockázatot jelentenek a műveleti biztonságra.

A kibertámadások szintén komoly veszélyt jelentenek a C2 rendszerekre. Az ellenséges szereplők, beleértve állami és nem állami csoportokat, a közösségi médiát használhatják kiberfegyverek bevetésére, például adathalász támadások vagy rosszindulatú szoftverek telepítésére. Ezek a támadások megbéníthatják a kommunikációs csatornákat, torzíthatják az információkat, vagy akár teljesen leállíthatják a C2 rendszerek működését, amely komoly veszteségeket eredményezhet a katonai műveletek során. [65]

A dezinformáció és a félrevezetés szintén jelentős kihívásokat jelent a C2 rendszerek számára. A hamis információk terjesztése a közösségi médián keresztül célzottan zavarhatja meg a döntéshozatali folyamatokat. Például az ellenséges szereplők szándékosan terjeszthetnek félrevezető tartalmakat, amelyek torzíthatják a valóságot, és helytelen döntésekhez vezethetnek. Az ilyen típusú információs támadások hatása

különösen nagy lehet válsághelyzetekben, ahol az időérzékeny döntéshozatal kulcsfontosságú. [58]

A deepfake technológiák és manipulált tartalmak további kihívást jelentenek a C2 rendszerek számára. Ezek a technológiák lehetővé teszik hamis vizuális és audio tartalmak előállítását, amelyek rendkívül meggyőzőek lehetnek. Az ilyen tartalmak alkalmazásával az ellenséges erők képesek megtéveszteni a katonai vezetőket, manipulálni a közvéleményt, vagy aláásni a bizalom légkörét a C2 rendszereken belül. Ez különösen veszélyes a modern konfliktusok során, ahol a gyors és megbízható információáramlás elengedhetetlen. [66]

A jövőben a mesterséges intelligencia (MI) és az új technológiák integrációja alapvetően alakíthatja át a C2 rendszereket, különösen a közösségi média által generált adatok feldolgozásában és a műveleti koordinációban. Az MI-alapú elemzések már most is jelentős szerepet játszanak a nagy mennyiségű adat gyors és hatékony feldolgozásában, de a technológia további fejlődése új távlatokat nyithat meg. Az MI alkalmazásával lehetővé válik a közösségi médiában található mintázatok azonosítása, valamint a szokatlan vagy anomális tevékenységek felismerése, amelyek segíthetik a katonai vezetők döntéshozatali folyamatait. Ez a technológia képes automatizálni az adatok elemzését, minimalizálva az emberi hibák lehetőségét, és gyorsabb, megalapozottabb döntéseket tesz lehetővé. [67]

Az új technológiák integrációja, mint például az AR (augmented reality, kiterjesztett valóság) és VR (virtuális valóság), szintén alapvető változásokat hozhat a C2 rendszerekben. A közösségi média adatainak integrálása a C2 rendszerekbe lehetővé teszi a valós idejű helyzetfelismerést és koordinációt, miközben az AR/VR technológiák vizuális és interaktív környezeteket biztosítanak a műveletek megtervezéséhez és végrehajtásához. Ezek az eszközök lehetővé teszik, hogy a parancsnokok és csapatok közvetlenül, vizuálisan és intuitívan dolgozzanak együtt, javítva a kommunikáció hatékonyságát és a műveleti reakcióidőt. [60]

A közösségi média a modern C2 rendszerek kulcselemévé vált, amely jelentős mértékben hozzájárulhat a műveletek sikerességéhez. Ugyanakkor a jövőbeli fejlesztések során kiemelt figyelmet kell fordítani az adatbiztonságra, a hitelességre és az integrációra. Az adatok biztonságos kezelése elengedhetetlen a rendszerek megbízhatóságának fenntartásához, miközben a hitelesség biztosítása segíti a hamis információk és

manipulációk elleni védekezést. Az integráció során az új technológiák megfelelő alkalmazásának és a hagyományos rendszerekkel való kompatibilitásnak is kulcsszerepe lesz. [60]

A jövőbeli fejlesztési irányok között szerepel a mesterséges intelligencia és a gépi tanulás további fejlesztése, valamint az AR/VR technológiák katonai alkalmazásának kiterjesztése. Ezen eszközök hatékony implementációja azonban kihívásokkal járhat, különösen a technológiai infrastruktúra kiépítése és a használathoz szükséges képzés terén. A közösségi média és a C2 rendszerek közötti szinergia optimalizálása kulcsfontosságú lesz a hatékonyság növelése és a jövőbeni kihívások kezelése érdekében. [60]

2.3. Közösségi média és a befolyásolási műveletek

A közösségi média forradalmasította az információs hadviselés és a befolyásolási műveletek (influence operations) eszköztárát. Míg az információs műveletek évezredek óta a hadviselés részét képezik, a digitális korszak új dimenziót adott ezeknek a tevékenységeknek. [19] Az internet globális elérése és a közösségi platformok interaktív természete korábban soha nem látott sebességű és hatósugarú információterjesztést tesz lehetővé. Svetoka megállapítja, hogy a legutóbbi líbiai, szíriai és ukrajnai konfliktusokban a közösségi média vált az egyik fő kommunikációs csatornává, ahol széles körben használták akciók koordinálására, hírszerzés gyűjtésére, de legfőképpen a célközönség meggyőzésére és mozgósítására. [5] Ez azt jelenti, hogy a közösségi média mára nem pusztán kiegészítője, hanem központi színtere lett a befolyásolási műveleteknek.

A befolyásolási műveletek során állami és nem állami szereplők egyaránt igyekeznek a közösségi médiát fegyverként használni a politikai és katonai céljaik elérésére. Ennek egyik oka, hogy a közösségi platformok szabályozatlansága és anonim jellege megkönnyíti a manipulatív tartalmak terjesztését. Bárki globális hallgatóságot érhet el csekély erőforrással, és a hamis profilok mögé rejtőzve szinte következmények nélkül indíthat dezinformációs kampányokat. [68] A közösségi médiában zajló befolyásolás lehet nyílt, vagy rejtett. Az utóbbi jellemző formái lehet az az álhírek (fake news) terjesztése, a troll-hadseregek és automatizált botnetek alkalmazása a közvélemény torzítására, illetve a célzott pszichológiai műveletek a közösségi médián keresztül. [69]

Az orosz befolyásoló műveletek az utóbbi években különösen látványos példákkal szolgáltak a közösségi média erejére. A 2014-ben kezdődött orosz–ukrán konfliktus során Oroszország kiterjedt dezinformációs kampányt folytatott, ami során hamis hírek és összeesküvés-elméletek tömkelegével árasztotta el a Facebookot, X-et és orosz nyelvű közösségi oldalakat azért, hogy a konfliktus természetét eltorzítása. Céljuk egyrészt a nemzetközi közvélemény megosztása és bizonytalanságban tartása volt, másrészt az ukrán lakosság és a katonák pszichológiai megtörése. Az orosz információs hadviselés egyik fő törekvése a társadalmi bizalom megingatása és a döntéshozók befolyásolása az ellenséges oldalon. Ennek eszközei közé tartoznak az álhírek mellett a megfélemlítő narratívák (pl. eltúlzott történetek az ukrán erők atrocitásairól), valamint az olyan hamis online személyiségek, akik látszólag ukrán állampolgárokként kritizálják saját kormányukat. Oroszország emellett ipari méretekben üzemeltetett „trollgyárakat”, ahol több száz alkalmazott gyártotta és terjesztette a propagandaposztokat a nap 24 órájában. Ezek a trollok és botok mesterségesen felnagyították az orosz narratívákat, hogy azok organikus közvéleménynek tűnjenek. Az oroszok e módszerekkel radikalizálni is igyekeztek bizonyos célcsoportokat, illetve megnyerni a támogatásukat saját geopolitikai céljaikhoz. Például Kelet-Ukrajnában a szakadár érzelmek szítása érdekében oroszbarát közösségi média oldalakon terjesztettek híreket, amelyek démonizálták az ukrán kormányt és hősként állították be a szeparatistákat. A Kreml irányítása alatt álló médiagépezet a digitális térben olyan alternatív valóságot alakított ki, amelynek hatására elvesztette bizalmát a hivatalos információk iránt, és fogékonnyá vált az orosz narratívára. [70]

A nyugati hatalmak számára komoly kihívást jelent ez a fajta hibrid hadviselés. A NATO és tagállamai az elmúlt években fokozott figyelmet fordítanak a közösségi médiában zajló ellenséges befolyás elleni védekezésre. Svetoka (2016) rámutat, hogy az államoknak fel kell készülniük arra, miként azonosítsák és lépjenek fel a közösségi médiával való visszaélésekkel szemben. Ennek részeként számos ország hozott létre speciális stratégiai kommunikációs egységeket, amelyek feladata az álhírek monitoringja és cáfolata, valamint a saját hiteles üzenetek terjesztése. Emellett a nyugati országok egyre nagyobb hangsúlyt fektetnek a digitális műveltség növelésére, a lakosság és a katonák képzésére, hogy felismerjék a manipulált tartalmakat.

A terrorista és lázadó szervezetek szintén mesterien aknázták ki a közösségi médiát a befolyásolásra. Az ISIS propagandagépezete hírhedten hatékony volt a 2014–

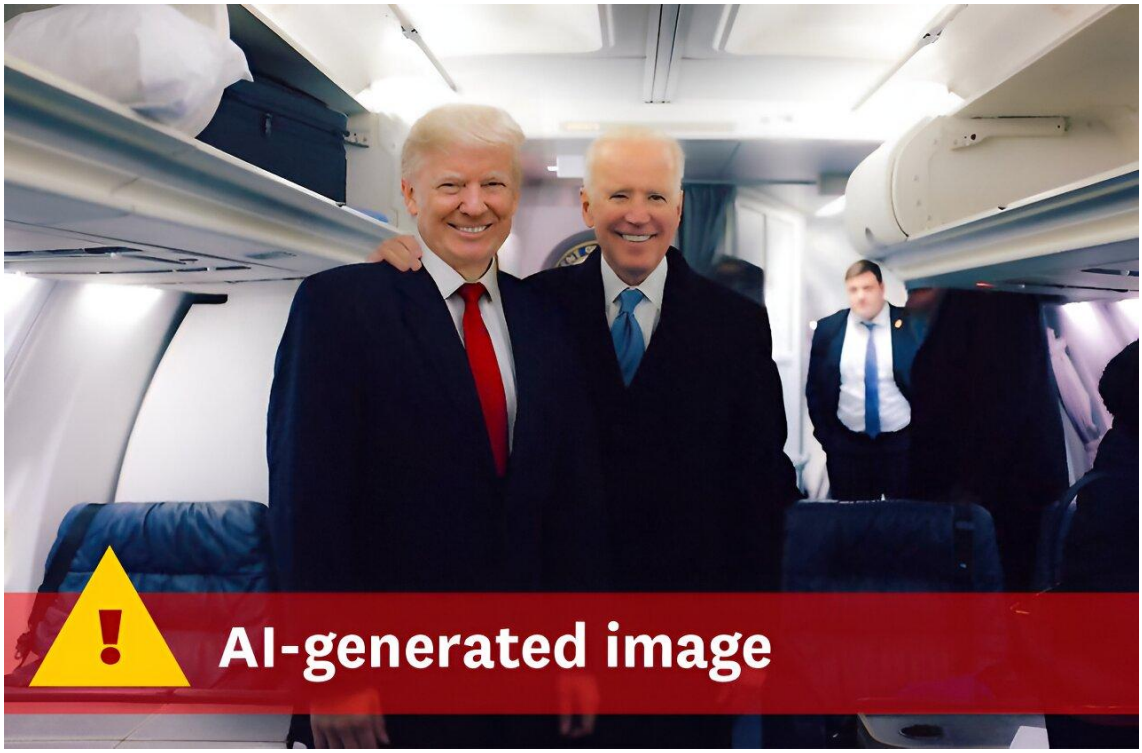
2017 közötti időszakban. Ekkor profin szerkesztett toborzó videókat és sokkoló erőszakos tartalmakat tettek közzé, amelyek vírus módjára terjedtek. Az X-en és a Telegramon több tízezer szimpatizáns terjesztette az Iszlám Állam üzenetét, egyszerre rémisztve el ellenfeleit brutalitásának demonstrálásával és vonzva a radikalizálódó fiatalokat egy látszólag hősies ügyhöz. Egy 2015-ös kongresszusi meghallgatáson elhangzott adatok szerint az ISIS propagandaanyagai több mint 200 000 felhasználót értek el az X-en, napi átlagban 90 új kampányhoz kapcsolódó üzenetet posztoltak a szimpatizánsok. Az ISIS ennek révén nem csupán harcosokat toborzott a világ számos pontjáról, de sikerült félelmet keltenie a nemzetközi közvéleményben is, például az online lefejezésekről készült videók például pszichológiai hadviselési eszközként szolgáltak. Ugyanakkor ez a nyílt kommunikáció sebezhetővé is tette őket, mert az amerikai légierő hírszerzése egy esetben egy ISIS-tag dicsekvő Facebook-posztja alapján 22 órán belül azonosította és lebombázta a szervezet egyik parancsnoki központját. [71]

E tapasztalatok hatására az ISIS vezetése később megpróbálta korlátozni harcosainak online jelenlétét, mivel ráébredtek, hogy a közösségi média kétélű fegyver, mert amennyire segíti a propagandát, annyira információforrás az ellenfélnek is. A közösségi médiában folyó befolyásolási műveletek hatása nehezen mérhető, de bizonyos esetekben közvetlen következményekkel járt. Gondoljunk az úgynevezett Arab Tavasz 2011-es eseményeire, ahol a Facebookon és X-en szerveződő tiltakozások több országban is forradalmi változásokat indítottak el. Itt a befolyásolás inkább pozitív értelemben, a szabadság mobilizálásában jelent meg. [72] Ugyanakkor a 2016-os amerikai elnökválasztás vagy a 2016-os Brexit-népszavazás kapcsán kimutatták, hogy a közösségi médiában terjedő célzott dezinformációk és „microtargeting” kampányok hozzájárulhattak a választók véleményének befolyásolásához. Mindez rámutat, hogy a közösségi média algoritmusai ún. visszhangkamrákat (echo chamber) hoznak létre, amelyekben az emberek hajlamosak csak a saját nézeteiket megerősítő információkat látni. [73] Ezt a jelenséget az információs hadviselés irányítói könnyen kihasználhatják és tudatosan célozzák meg az egyes csoportokat az őket leginkább fogékonnyá tevő üzenetekkel. A pszichográfiai profilalkotás és a nagy adattömegek elemzése révén személyre szabott propagandát lehet előállítani. Ily módon a közösségi média nem csupán a tömegek, hanem az egyének befolyásolásának eszközévé is vált.

Az utóbbi években jelentősen átalakult a közösségi médián keresztüli dezinformációs kampányok módszertana. Míg korábban szöveges posztok, manipulált

hírek és szándékosan félrevezető bejegyzések jellemezték ezeket a műveleteket, mára egyre inkább az AI által generált képek és vizuális tartalmak kerülnek a dezinformációs stratégiák középpontjába. Ezek az eszközök nemcsak az információs káosz fokozását szolgálják, hanem hatékonyan kihasználják a közösségi média vizuális orientáltságát és az emberek csökkent vizuális kritikai érzékenységét.

A mesterséges intelligenciával generált képek meggyőző részletességgel képesek hamis, de valósághű jeleneteket alkotni, amelyeket gyakran politikailag érzékeny kontextusban használnak fel. Ezt szemlélteti alább az 1. ábra. A cél az emberek gyors érzelmi reakciójának kiváltása, amely megelőzi a racionális gondolkodást, és így növeli a tartalom terjedésének esélyét.



2. ábra: Mesterséges Intelligencia által generált fotó Joe Biden-ről és Donald Trump-ról [74]

Ez a tendencia egybevág az úgynevezett „low-effort, high-impact” megközelítéssel, amelyet sok dezinformációs aktor alkalmaz. Az AI segítségével gyártott vizuális tartalmak ugyanis minimális technikai tudással is előállíthatók, miközben drámai hatást fejtenek ki. Ráadásul ezek a képek sokszor kikerülik a platformok szokásos fact-checking mechanizmusait is, mivel nem klasszikus, álhíres szövegek, hanem újonnan generált, egyedi tartalmak. A Harvard Kennedy School kutatása szerint az AI által

generált vizuális dezinformációt az emberek nagy része nem tudja megkülönböztetni valós fényképektől, még akkor sem, ha figyelmeztetik őket a manipuláció lehetőségére. [75]

A jelenség nem csupán információs hadviselési szempontból jelent kihívást, hanem bizalmi és társadalmi stabilitási szempontból is. Egyes magas követőszámú oldalak előszeretettel alkalmazzák ezeket a technológiákat. Eleinte összeesküvés-elméleteket kezdtek terjeszteni, mára viszont célzottan alkalmaznak AI-tartalmakat a dezinformáció hitelesítésére, például hamis háborús képeket vagy kreált személyeket használnak érvek alátámasztására.

A „hallgatag algoritmus" jelensége tovább fokozza a problémát. A közösségi platformok algoritmusai jellemzően az érzelmileg intenzív, sok interakciót kiváltó posztokat emelik előtérbe, így a dezinformációs tartalmak nagyobb láthatóságot kapnak. Ezzel szemben a cáfolatok vagy tényellenőrzések sokkal ritkábban érik el ugyanazt a közönséget. [76]

Egyes országokban már észlelhetők államilag szervezett kampányok, amelyek AI-alapú képek és videók segítségével terjesztenek dezinformációt geopolitikai célból. Az orosz-ukrán háború kapcsán több elemzés is rámutatott arra, hogy hamis képeket és mélyhamisított (deepfake) videókat használtak a háborús bűnök „dokumentálására" vagy éppen az ukrán vezetők lejáratására. [77] Az ilyen tartalmak képesek elbizonytalanítani a közvéleményt, relativizálni a tényeket, és végső soron aláásni a demokratikus rendszerek alapjait.

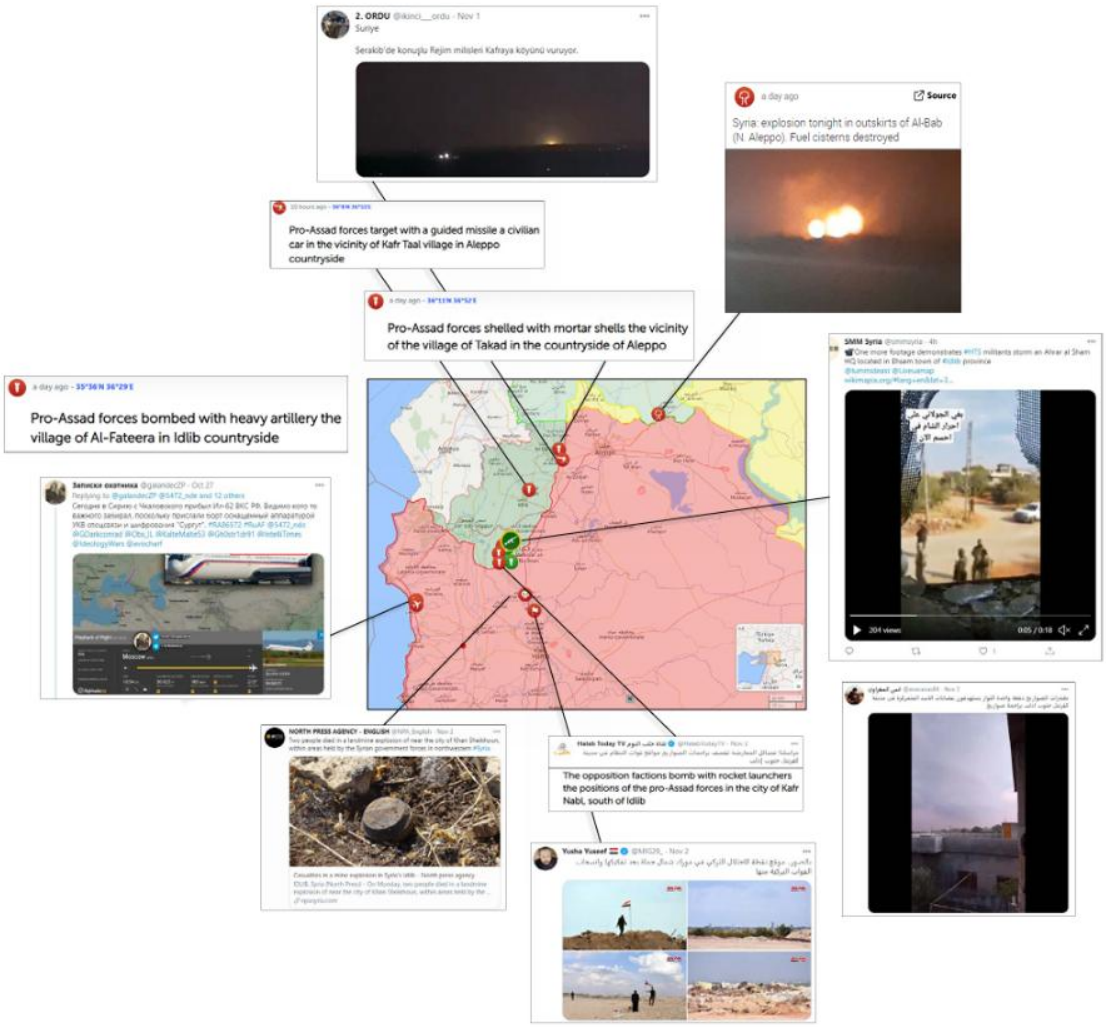
A hatékony védekezés érdekében egyre fontosabbá válik a vizuális forráshitelesség ellenőrzése, az ún. visual literacy[5] fejlesztése, valamint a közösségi média platformok technológiai megoldásainak fejlesztése. Ugyanakkor ezen rendszerek csak részben képesek követni az AI-technológiák gyors fejlődését, így a társadalmi tudatosság növelése továbbra is kulcsfontosságú marad.

[5] Visual literacy (vizuális műveltség): annak a képessége, hogy az egyén képi és vizuális információkat (például fotókat, videókat, grafikákat, térképeket vagy infografikákat) tudatosan értelmezzen, kritikus szemmel elemezzen, valamint felismerje azok mögöttes jelentéseit, manipulációs elemeit és kommunikációs céljait.

2.4. Közösségi média, mint a célmegjelölés és célravezetés eszköze

A közösségi média nem csupán a narratívák csataterét jelenti, hanem konkrét hírszerzési és célkijelölési feladatokban is egyre fontosabb szerepet kap. A nyílt forrású információk felhasználása révén a katonai erők új módszereket fejlesztettek ki a célpontok felderítésére és megjelölésére. A modern precíziós csapásmérés alapja a pontos célazonosítás. Ebben a folyamatban a közösségi média egyfajta érzékelő hálózatként működhet, ahol a civil felhasználók akaratlanul is információkat szolgáltatnak a harctéri helyzetről. Mára azt mondhatjuk, hogy minden állampolgár szenzorrá vált, hiszen az emberek okostelefonjaikkal folyamatosan fotókat, videókat töltenek fel és bejelentkeznek helyszínekről, s ez az adathalmaz felbecsülhetetlen értékű lehet a hírszerzés számára. [78]

A hadseregek világszerte felismerték, hogy a közösségi média adatai a célleküzdési ciklus első lépésében, a felderítésben és azonosításban komoly erőnyerőt jelentenek. Rasak (2021) szerint a fegyveres erők egyre inkább a közösségi médiát használják a célkeresési folyamat első lépéseként, azaz a leendő célpontok felderítésére. Előfordul, hogy egy parancsnoki központ térképfalai mellett valós időben futnak a releváns X-bejegyzések vagy Telegram-csatornák, hogy az elemzők azonnal lássák, ha a helyi lakosok például ellenséges csapatmozgásról számolnak be. A geotaggel ellátott posztok különösen értékesek, hiszen egy harci övezetben közzétett fénykép metaadatai elárulhatják a pontos koordinátákat. Az algoritmusok ma már képesek tömegesen begyűjteni és térképre vetíteni az ilyen nyilvános posztokat, felfedve például egy ellenséges konvoj útvonalát vagy egy tüzérségi üteg pozícióját. A Live Universal Awareness Map (2. ábra) és hasonló online eszközök nyíltan demonstrálják, hogy az X-en megosztott információkból akár valós idejű „háborús térkép” állítható össze.



3. ábra: Szíriában, 2020. november 3-án készült Live Universal Awareness Map-je [78]

A szíriai konfliktus során civilek ezrei jelentették Facebook-csoportokban és X-en a légicsapások helyszíneit, ami alapján a segélyszervezetek és olykor a harcoló felek is tájékozódtak az eseményekről. Például 2015-ben amerikai hírszerzők egy ISIS-fegyveres öntelt „selfie” -jéből szerezték meg egy parancsnoki létesítmény helyét. A terrorista egy háttérben látható épület előtt pózolt és büszkélkedett a csoport képességeivel a Facebookon, az amerikai elemzők pedig e nyilvános poszt alapján beazonosították a helyszínt, és 22 órán belül légicsapást mértek rá, teljesen megsemmisítve az objektumot. [78] Ez az eset bizonyította, hogy a felelőtlen közösségimédia-használat halálos következményekkel járhat az ellenségre nézve. Az ISIS azóta igyekezett korlátozni harcosai online tevékenységét, de a nyomok így is gyakran fellelhetők és a koalíciós erők számos dzsihadista vezetőt lokalizáltak azáltal, hogy azok titokban használt X-fiókjait vagy Telegram-csatornáit lekövették. A

hagyományos reguláris hadseregek szintén profitálnak a közösségi média OSINT adataiból a célkijelölésben. Az orosz–ukrán háború során Ukrajna innovatív módon fordította saját javára a nyílt információkat. Ukrán hacktivisták és OSINT-szakértők csoportjai rendszeresen elemzik az orosz katonák közösségi médiás jelenlétét. 2022. október 12-én egy orosz katona, Alekszej Lebegyev a VKontaktye oldalon közzétett egy fotót, amelyen egy fehér sátorban guggol. Arcát ugyan maszk takarta, de nem vette észre, hogy a poszthoz automatikusan társult a földrajzi helymeghatározás, ami a Donyeck megyei Szvobodne falu volt. Az ukrán Molfar elemzői azonnal felfigyeltek erre a bejegyzésre, és néhány órán belül kidolgoztak egy célpont-profilt. Más nyilvános fotókat is találtak ugyanarról a helyszínről más orosz katonák fiókjain, valamint műholdfelvételekkel azonosították a sátortábort, amelyről kiderült, hogy az orosz csapatok egyik kiképző bázisa. Miután ezt kiderítették, az információt átadták az ukrán katonai hírszerzésnek. [79] Ez egyike volt azon eseteknek, amikor egy katona Facebook posztja végzetes célravezető információnak bizonyult.

Az ukrán hatóságok tudatosan ösztönzik a polgári lakosságot is az információmegosztásra és létrehoztak például hivatalos Telegram-botokat, amelyekkel a civilek névtelenül beküldhetik észleléseiket az ellenséges mozgásokról. Ezt a fajta tömeges társadalmi érzékelést a 21. századi hadviselés új elemének tekinthetjük, ahol a polgárok telefonjai érzékelőhálózatba szerveződve segítik a célfelderítést. Természetesen az így nyert adatok megbízhatósága változó, ezért a katonai elemzőknek mindig több forrásból kell megerősíteniük egy-egy értesülést, mielőtt csapásmérés alapjául használják. De a digitális korszakban ezt is támogatja a technológia, például egy adott térségből származó posztok szentimentelemzése megmutathatja, ha a lakosság pánikjelei nőnek, az akár harci cselekményre utalhat, vagy ha hirtelen rengeteg bejegyzés jelenik meg egy bizonyos helynévvel, az akár valós harci eseményt jelezhet. Az ilyen módszerek összevethetők a hagyományos felderítés adataival, növelve a célkijelölés pontosságát. [80]

A közösségi média emellett a célravezetés támogatására is használható a harctéren, például a tüzérségi vagy rakétacsapások koordinálása során. 2020-ban a hegyi-karabahi háborúban az azeri erők drónfelvételeket és közösségi médiás jelentéseket kombinálva találták meg és semmisítették meg az örmény légvédelmi ütegeket. Az azeri védelmi minisztérium az X-en rendszeresen publikált drónvideókat az éppen megsemmisített célpontokról, ami pszichológiai hadviselésnek is beillett, de egyben arra

is utalt, hogy valószínűleg a közösségi médiát is figyelik valós időben. Ha egy civil szemtanú jelezte a Facebookon, hogy egy adott faluban rakétatalálat érte az elektromos hálózatot, arra az örmény fél reagálhatott, és az azeri hírszerzés következtethetett belőle a tartalék generátorok helyére vagy a javítóalakulat mozgására. [81] Bár ezek finom jelek, a „big data" elemzés a közösségi médiában hatalmas mennyiségű ilyen apró adatpontot képes összegyűjteni és értékelni. Ennek eredményeként például egy mintafelismerő algoritmus észreveheti, hogy egy adott térségben rendszerint nő a civil posztok száma közvetlenül egy rakétakilövés előtt, amelynek oka lehet, hogy a lakosság hallja a rakétaindítás zaját. Ha ezt korrelálják a katonai szenzoradatokkal, pontosabb riasztásokat adhatnak a saját csapatoknak.

Természetesen a közösségi média adta előnyök mellett komoly kihívások is jelentkeznek a célmegjelölés terén. Az ellenség is tudatában van annak, hogy posztjai leleplezőek lehetnek, ezért egyre gyakoribb a megtévesztés (deception) ebben a térben. Ez lehet például hamis helyszíni fotók posztolása, vagy akár szándékosan félrevezető információk kiszivárogtatása az online platformokon. Például orosz katonák a Donbászban több esetben szándékosan régi vagy máshol készült fotókat osztottak meg, hogy megtévesszék az ukrán felderítést a csapatok elhelyezkedéséről. Az is előfordul, hogy egy katonai járművet feltűnően hagynak civil környezetben fotózni, majd a poszt nyomán oda irányuló támadásra csapdát állítanak. Emiatt a közösségi médiára építő célfelderítést mindig óvatos szkepticizmussal kell kezelni. Többforrású hitelesítés szükséges annak érdekében, hogy csak akkor váljon egy közösségi poszt alapú értesülés célmegjelöléssé, ha más forrás is alátámasztja. A hadseregek ezért integrálják az OSINT-elemzőket a célfelderítő csoportokba, hogy azok szakértelmükkel kiszűrjék a hamis nyomokat és aggregálják a valódikat. [78]

2.5. Közösségi média és a kibertér műveletek

A fentiekből is kitűnik, hogy a közösségi média a kibertér egyik meghatározó eleme, így a kibertér műveletek során is kulcsszerepet játszhat támadási felületként, támadási eszközként és a műveletek célpontjaként egyaránt. A katonai doktrínák a kibertér műveleteket gyakran defenzív, offenzív és felderítő kategóriákra osztják. [25] Mindhárom területen megfigyelhető a közösségi média integrációja. Egyrészt, a közösségi platformok infrastruktúrája maga is célpont lehet az offenzív kibertámadások során, másrészt a közösségi médiát használhatják a támadók eszközként a műveleteik végrehajtására. Végül, harmadrészt pedig a közösségi médián zajló tevékenységek

információs műveleti szempontból is relevánsak a kibertérben. Offenzív kibertér műveletek során a közösségi médiát többféleképpen ki lehet használni. Az egyik módszer a kiber-felderítés és social engineering[6] támadások támogatása. A nyílt profilokról begyűjthető személyes adatok aranyat érnek egy ellenfélnek, aki mondjuk adathalász támadást tervez egy katonai szervezet ellen. Például egy ellenséges hacker megnézheti a LinkedIn-en, kik a célszervezet rendszergazdái, majd ezekre a személyekre szabott megtévesztő üzeneteket küldhet, hivatkozva közös ismerősökre vagy érdeklődési körre, amit a közösségi médiáról tudott meg. Így a közösségi média, mint támadási felület jelenik meg: az emberi tényező kihasználását (social engineering) nagyban megkönnyíti, hogy a célpontok önként osztanak meg magukról információkat online. [82]

A közösségi média platformjai maguk is lehetnek az offenzív kibertér műveletek célpontjai. Az ellenség megpróbálhatja feltörni a fontosabb közösségi fiókokat vagy szolgáltatásokat, hogy azokon keresztül okozzon káoszt vagy kárt. Ilyen volt például a 2013-as hírhedt Twitter-incidens, amikor a Szíriai Elektronikai Hadsereg feltörte az Associated Press Twitter-fiókját, és hamisan közzétette, hogy robbanás történt a Fehér Házban és Obama elnök megsérült. A posztot pár perc alatt cáfolták, de az ál hír pillanatok alatt kb. 136 milliárd dolláros átmeneti tőzsdei veszteséget okozott, mivel automatizált kereskedési algoritmusok és pánikba esett befektetők reagáltak rá. [83]

Ez az eset megmutatta, hogy a közösségi média infrastruktúra elleni támadása igenis felér egy kibertámadással, amely fizikai következményekkel járhat. Hasonló incidens történt 2015 áprilisában, amikor ismeretlen hackerek megbénították a francia TV5Monde televíziót, egyszerre törölték elérhetetlenné a tévécsatorna adását és vették át az irányítást a közösségi média-fiókjaik felett, hogy azon keresztül az Iszlám Állam nevében propagandát tegyenek közzé. [84]

Látható, hogy a közösségi média-fiókok elleni sikeres támadás azonnal globális hírré válik és az így terjesztett dezinformáció sok emberhez eljut, mielőtt fellépnek a támadók ellen. Így tehát a kibertámadás és az információs támadás hatása összeadódik. Ezért a hadviselő felek ma már stratégiai fontosságúnak tekintik a közösségi platformok védelmét. A nagy tech cégek kormányokkal együttműködve igyekeznek fejleszteni a

[6] A **social engineering** (szociális manipuláció) olyan pszichológiai manipuláción alapuló támadási módszer, amelynek során a támadó az emberi tényezőt kihasználva próbál bizalmas információkhoz hozzáférni, vagy a célpontot meghatározott műveletek végrehajtására rávenni, például jelszavak megadására, káros szoftver telepítésére vagy biztonsági szabályok megszegésére [145]

biztonsági protokolljaikat, különösen választások vagy válságok idején, amikor megnő a hackelések és beavatkozások kockázata.

A defenzív kibertér műveletek vonatkozásában a közösségi média főként korai jelzőrendszerként és információmegosztó felületként hasznosul. A védelmi oldal számára a közösségi média figyelése fontos része a kiberveszélyek időbeni felismerésének. Például a kibervédelemmel foglalkozó egységek monitorozzák a hackercsoportok által használt nyilvános csatornákat, hogy észleljék, ha támadási szándékot kommunikálnak vagy sikeres behatolással dicsekednek. Gyakori, hogy egy támadó csoport a közösségi médián vállal felelősséget egy kibertámadásért, vagy éppen előre figyelmeztet egy közelgő akcióra. A kibervédelmi szakemberek számára tehát az X és a dark web fórumai éppúgy megfigyelendők, mint a hálózati forgalmi logok. Emellett a közösségi média segíthet a kárenyhítésben is, ugyanis egy kibertámadás esetén a hatóságok a közösségi média platformjain keresztül tudják gyorsan tájékoztatni a nyilvánosságot a szükséges lépésekről. A védekező oldal tehát kommunikációs csatornaként is használja e felületeket a kibertérben zajló műveletek során. [85]

A kibertér és a közösségi média összefonódása különösen nyilvánvaló a hibrid hadviselésben, ahol a technikai és információs támadások egyszerre jelennek meg. Az ellenfél egy jól megtervezett műveletben kombinálhat egy technikai kibertámadást és egy dezinformációs kampányt. Például előfordulhat, hogy egy kritikus infrastruktúra ellen indított hackertámadást kísér a közösségi médiában terjesztett pánikkeltő üzenet, amely felnagyítja a károkat vagy hamis híreket közöl további meghibásodásokról. Így a technikai hatás és az információs hatás összeadódik, és a védelemnek mindkettőre reagálnia kell. 2017-ben például Ukrajnában egy orosz malware (NotPetya) bénította meg a kormányzati és üzleti IT-rendszereket, miközben az oroszbarát közösségi oldalak hamis híreket terjesztettek arról, hogy Kijevben összeomlott a bankrendszer és általános káosz van. Ez is mutatja, hogy a kibertámadások elleni aktív védekezés nem csak technikai kérdés, hanem kommunikációs is. Ha a hatóságok gyorsan tudnak posztolni a hivatalos csatornáikon megnyugtató, pontos információkat, akkor a támadók információs hatása tompítható. [86]

Az offenzív oldalon a fejlett kiberhadviselő nemzetek már azt is megtehetik, hogy aktívan visszavágnak a közösségi média frontján. Az Egyesült Államok például 2018-ban a hírek szerint egy titkos kiberművelettel ideiglenesen megbénította az orosz „trollgyár”

internet-hozzáférését a félidős választások napján, hogy megakadályozza a választási beavatkozásukat. Ezt a lépést tekinthetjük a közösségi médiában zajló ellenséges befolyás elleni aktív védekezésnek, ugyanis a kibertérben semmisítették meg átmenetileg az ellenség online propagandafegyverét. [69] Hasonlóképpen, az amerikai Cyber Command 2016-ban indított Glowing Symphony hadművelete során behatolt az Iszlám Állam online hálózataiba, törölte vagy módosította a propagandavideóikat és posztjaikat, s ezzel megzavarta a terrorcsoport globális kommunikációját. [87]

Ezek a példák azt mutatják, hogy a kibertér műveletek és a közösségi média frontja nem választható el egymástól, hiszen a tiszta hackelés mellett a hadviselés immár magában foglalja a platformok feletti uralomért vívott küzdelmet is. Aki le tudja kapcsolni az ellenség Facebook-oldalait, hamis üzenetekkel tudja elárasztani a csatornáit, vagy éppenséggel fel tudja törni a kommunikációs appjait, az komoly stratégiai előnyre tehet szert.

Ugyanakkor ez a tendencia etikai és jogi kérdéseket is felvet. A közösségi média globális szolgáltatások hálózata, többnyire amerikai székhelyű magánvállalatok tulajdonában. Egy katonai kiberművelet, amely ezek infrastruktúráját érinti, könnyen érinthet civileket és semleges feleket is. Például egy Meta elleni támadás zavarhatja a platform általános működését, sértheti a felhasználók adatait. A nemzetközi jog jelenleg is keresi a választ arra, hogy a közösségi médián keresztül indított kibertér műveletek mennyiben tekinthetők fegyveres támadásnak vagy beavatkozásnak. A Tallinn Manual 2.0 (2017) kimondja, hogy a kibertérben végrehajtott műveletek is sérthetik az államok szuverenitását, ha jelentős hatásúak. Ugyanakkor a megkülönböztetés civil és katonai között elve ebben a nem fizikai térben nehezen alkalmazható. Emiatt a katonai tervezők fokozottan ügyelnek arra, hogy a közösségi média bevonásával tervezett kibertér műveletek politikai felhatalmazása egyértelmű legyen, és minimalizálják a mellékhatásokat.

2.6. Közösségi média és az aktív védelem

Aktív védelem alatt általánosságban olyan proaktív, kezdeményező védelmi intézkedéseket értünk, amelyek nem csupán passzívan hárítják el a fenyegetéseket, hanem előre felismerik, sőt semlegesítik azokat, mielőtt kárt okozhatnának. A közösségi média esetében az aktív védelem azt jelenti, hogy a katonai és nemzetbiztonsági szervezetek folyamatosan figyelik a platformokon zajló diskurzust a potenciális veszélyek kiszűrése

céljából, és proaktívan fellépnek a fenyegetést jelentő tartalmakkal vagy tevékenységekkel szemben. [88]

Ennek egyik fontos eleme a valós idejű monitoring és elemzés. A védelmi oldal aktív hozzáállása megkívánja, hogy ne várja meg, amíg egy dezinformációs kampány teljesen kibontakozik vagy egy közösségi médiás híresztelés pánikot kelt, hanem már a korai jeleknél beavatkozzon. Például egy katonai hírszerző egység algoritmusai jelezhetik, ha hirtelen szokatlan aktivitás indul egy kulcsfontosságú témában. Ha azt látják, hogy gyanús profilok tömegesen kezdenek posztolni egy adott hashtaggel, azonnal elemezhetik a tartalmat és eredetet, így akár még azelőtt megállapítható, hogy egy ellenséges narratíva készül kibontakozni, mielőtt az tömeges elérést nyerne. Az aktív védelem részeként ilyenkor a védők kezdeményező lépéseket tesznek, például felveszik a kapcsolatot a platform üzemeltetőivel a gyanús bot-hálózat felszámolása érdekében, vagy előre figyelmeztetik a potenciális célközönséget, hogy hamis információk várhatók egy bizonyos témában. Jól mutatja ezt a 2022-es ukrajnai háború alatt megjelent Zelenszkij-deepfake esete is. Mivel az ukrán hatóságok hetekkel korábban jelezték, hogy az oroszok ilyen hamis videóval próbálkozhatnak, a megjelenő deepfake-et a közönség nagy része azonnal gyanakodva fogadta, és a platformok gyorsan le is vették. [58]

Az aktív védelem tehát a fenyegetések előrejelzését és megelőzését jelenti a közösségi médiában. Az aktív védelem további eleme a gyors reagálás és cáfolat. Ha egy ellenséges narratíva vagy álhír mégis utat tör magának, az aktív védekezést folytató fél haladéktalanul ellensúlyozza. Például, ha a közösségi médiában elterjed, hogy egy katonai művelet során civil áldozatok voltak, akkor a katonai kommunikációs csatornákon perceken-belül közzéteszik a tényszerű helyzetjelentést, fotókkal és hiteles bizonyítékokkal. A NATO stratégiája szerint a "First with the truth" (Légy első az igazsággal) elv érvényesítése az egyik legjobb ellenszere a dezinformációnak. [89]

Az aktív védelem ennek jegyében a közösségi médiában is igyekszik tematizálni a beszélgetést, nem átengedni a teret a hazugságoknak. Ha például egy hamis hír jelenik meg arról, hogy egy ország katonai vezetése kapitulálni készül, akkor a kormányzati profilok azonnal kiadják a tagadó nyilatkozatot, és megerősítik a lakosságot a folytatásról, ezzel elejét véve a pániknak. 2022 márciusában, amikor hackerek egy ukrán híroldalt feltörve deepfake videót tettek közzé Zelenszkij állítólagos megadásáról, Zelenszkij rövid

időn belül a saját hivatalos Telegram-csatornáján válaszolt egy videóüzenetben, kijelentve: „*Nem tesszük le a fegyvert".* [58]

Az aktív védelem kiterjed a platformszintű együttműködésre is. A közösségi média cégekkel való kapcsolattartás ma már a kormányzati szervek feladatai között szerepel, különösen választások és válságok idején. Az aktív védelem jegyében számos ország (köztük Magyarország is) szorgalmazza, hogy a nagy platformok vezessenek be hatékonyabb moderációs és átláthatósági intézkedéseket. [90]

A közösségi médiában megvalósuló aktív védelem másik aspektusa a megelőző műveletek végrehajtása az információs térben. Bizonyos esetekben a védekező fél nem elégszik meg a védekezéssel, hanem támadó jellegű, de védelmi célú lépéseket tesz. Ilyen lehet az ellenséges propagandisták leleplezése és hiteltelenítése. Például, ha egy NATO-ellenes álhírkampány mögött sikerül beazonosítani konkrét orosz ügynököket vagy trollfarmokat, akkor a védők nyilvánosságra hozhatják ezek adatait, bemutatva a közönségnek, hogy manipuláció áldozatai. Ezt tette az Egyesült Államok is, amikor 2018-ban szankciókkal sújtott és név szerint megnevezett orosz személyeket az IRA trollgyárból, elrettentő céllal. Szintén ide sorolható a „honeypot" műveletek alkalmazása, amikor védelmi hírszerzők hamis terrorista- vagy hacker-csoportnak adják ki magukat a közösségi médiában, hogy magukhoz vonzzák az ellenséges szereplőket, és így megfigyelhessék vagy félrevezethessék őket. Ezt a módszert a bűnüldözésben régóta használják, és a kibertérben is megjelent aktív védelmi technikaként („social engineering active defense"). [91] Bár kockázatos, mégis eredményes lehet, hiszen a védők értékes információhoz jutnak az ellenfél szándékairól, és akár elő is idézhetnek olyan ellenfél-lépéseket, amelyekből tanulni tudnak.

2.7. Részkövetkeztetések

A fejezetben megvizsgáltak alapján azt a következtetést vonom le, hogy **a közösségi média a 21. századi katonai műveletek minden szintjét és területét áthatja**. A vezetés és irányítás (Command and control, C2) terén a közösségi média új lehetőségeket nyit a valós idejű helyzetismeret bővítésére és a stratégiai kommunikációra, ugyanakkor új kihívásokat is támaszt a műveleti biztonság és a döntéshozatal terén. A parancsnokok számára a digitális tér dinamikus, de veszélyekkel teli információforrássá vált, ahol a gyors reagálás és a kritikus gondolkodás kulcsfontosságú. A befolyásolási műveletekben a közösségi média a modern információs hadviselés fő fegyverévé lépett elő. Legyen szó

állami propaganda-hadjáratokról, választásokba való beavatkozásról vagy terrorcsoportok toborzó kampányairól, mindezeket a platformokat használják a célcsoportok véleményének alakítására. A globális elérés, az interaktivitás és az algoritmusok által vezérelt tartalomterítés olyan erővel ruházza fel a közösségi médiát, amelyet a hadviselésben korábban elképzelni sem lehetett.

A fejezetben elvégzett vizsgálataim szintén rávilágítanak arra, hogy **a közösségi média konkrét harci előnyöket teremthet a célmegjelölés és célravezetés területén**. Az OSINT-forradalom révén ma már civil posztok alapján lehet felderíteni és nyomon követni ellenséges erőket, ami jelentős mértékben támogatja a precíziós csapásokat és a gyors reagálású műveleteket. Ugyanakkor fontos kiemelni, hogy ami egyik oldalon hírszerzési kincs, az a másik oldalon fatális OPSEC-hiba. A hadviselés során számos példát láttunk arra, hogy a felelőtlen közösségi média használat végzetes következményekkel járt. Ez hangsúlyozza a képzés és a szabályozás fontosságát, ugyanis a katonáknak meg kell tanulniuk fegyelmezetten bánni a közösségi médiával, tudva, hogy az ellenség is figyel.

Megvizsgáltam, hogy a közösségi platformok egyaránt lehetnek a támadás eszközei, a támadás célpontjai és a védelmi erőfeszítések komponensei. Ennek alapján arra a következtetésre jutottam, hogy a kibertérben zajló konfliktusokban a technikai és információs műveletek egyre inkább összeforrnak és a közösségi média pedig az a színpad, ahol ez a szinergia látványosan megmutatkozik. A 2010-es évek végére a nemzetállamok felismerték, hogy a kibervédelem nem működhet elszigetelten az információs tér védelmétől, a kettőt integráltan kell kezelni.

Elemzéseim rávilágítanak arra, hogy **az aktív védelem koncepciója összegzi mindazt, amire a közösségi média katonai alkalmazásában szükség van, azaz proaktivitás, gyorsaság, rugalmasság és együttműködés**. Az aktív védelem lényege, hogy ne hagyjuk magunkat meglepni vagy sarokba szorítani az információs térben, hanem előzzük meg és törjük meg a fenyegetéseket. A közösségi médiában ez a gyakorlatban folyamatos jelenlétet, monitoringot és szükség esetén ellentámadást jelent a dezinformációval és kibertámadásokkal szemben. Ahogy a dolgozat több példája is bemutatta, a közösségi médiában zajló aktív védelem konkrét eredményekhez vezethet, mert a társadalom kevésbé dől be az álhíreknek, az ellenfél elveszíti

kezdeményezőkészségét az információs térben, és végső soron a katonai műveletek zavartalanabbul folyhatnak.

Mindazonáltal fontos kiemelni, hogy a **közösségi média szerepe a hadviselésben egy dinamikusan változó terület**. A technológia fejlődésével új kihívások fognak jelentkezni. A katonai stratégiáknak folyamatosan alkalmazkodniuk kell ehhez. A fejezet alapján azonban egyértelmű, hogy a közösségi média meghatározó tényező marad a konfliktusokban és befolyásolja a harcmezőn kívüli és belüli eseményeket, hat az emberek gondolkodására és a katonák cselekvéseire egyaránt. Éppen ezért a katonai tervezésben és doktrínákban immár elengedhetetlen figyelembe venni ezt a dimenziót. A siker kulcsa az lesz, hogy a fegyveres erők képesek-e integrálni a közösségi média adta lehetőségeket a saját hadműveleti ciklusukba, miközben védettek maradnak az abból eredő fenyegetésekkel szemben.

3. FEJEZET
A KÖZÖSSÉGI MÉDIA ÉS AZ INFORMÁCIÓS MŰVELETEK KAPCSOLATA ESETTANULMÁNYOKON KERESZTÜL

A modern orosz kiberműveletek és a közösségi médiában megvalósuló információs műveletek jelenségének átfogó megértése érdekében elengedhetetlen azok konkrét esettanulmányokon alapuló vizsgálata. Az empirikus példák lehetővé teszik azon módszerek, eszközök és stratégiai célok feltárását, amelyek az orosz államhoz köthető kiberműveleteket és információs befolyásolási tevékenységeket jellemzik, továbbá rávilágítanak arra a folyamatra, amelynek során a közösségi média a modern konfliktusok egyik meghatározó műveleti környezetévé vált.

A fejezet időrendi megközelítést alkalmazva elsőként a 2020 előtti, állami támogatással végrehajtott orosz kiberműveletek jellegzetes eseteit vizsgálja, amelyek megalapozták a későbbi, komplexebb információs és kiberműveleti stratégiák kialakulását, kezdve a 2014-es krími annexió eseményeinek elemzésére kerül sor, amely mérföldkőnek tekinthető a kibertér és az információs műveletek integrált, összehangolt alkalmazása szempontjából. Az elemzés ezt követően az orosz–ukrán fegyveres konfliktus (2022-) során megfigyelhető, úgynevezett „virálissá vált hadviselés” jelenségére tér ki, amelyben a közösségi média platformjai kulcsszerepet játszanak az információk valós idejű terjesztésében, a stratégiai narratívák formálásában, valamint a hazai és nemzetközi közvélemény befolyásolásában.

Végezetül a legújabb fegyveres konfliktusok információs dimenziója kerül bemutatásra, amelyeket a közösségi média meghatározó szerepe miatt, az általam„Jom Kippur 2.0”-ra keresztelt eseménnyel zárom az esettanulmányok bemutatását.

E példák rávilágítanak arra, hogy a közösségi média platformjai a modern hadviselés során már nem csupán kommunikációs eszközként, hanem önálló műveleti térként jelennek meg, amely jelentős hatást gyakorol a konfliktusok dinamikájára, az információs fölény megszerzésére, valamint a stratégiai és műveleti célok elérésére.

3.1. 2020 előtti orosz államilag szponzorált kibertámadások

A 2000-es évek végétől kezdődően Oroszország számos, államilag támogatott kibertámadással bizonyította, hogy a kibertér a geopolitikai konfliktusok új frontvonala lett. Az egyik első ismert eset 2007-ben történt Észtországban, amikor egy szovjet emlékmű eltávolítása miatti diplomáciai vita nyomán Észtország súlyos, 22 napig tartó kibertámadás-sorozatot szenvedett el. Elosztott túlterheléses (Distributed Denial of Service, DDoS) támadások formájában bénították meg észt kormányzati, pénzügyi és média honlapok tucatjait, részben megbénítva az ország információs infrastruktúráját. Bár a támadások mögött közvetlenül egyetlen szervezet sem vállalta a felelősséget, számos közvetett bizonyíték utalt orosz kötődésre. Szakértők szerint a jelek egy összehangolt információs hadműveletre utaltak, melyben orosz állami szereplők legalábbis támogatták a nacionalista hackercsoportokat. [92]

Az észt támadás hatására a NATO létrehozta Tallinban az Együttműködési Kibervédelmi Kiválósági Központot (Cooperative Cyber Defence Centre of Excellence, CCDCOE), felismerve, hogy a tagállamok ellen indított ilyen jellegű támadások komoly biztonsági fenyegetést jelentenek. Az észtországi kibertámadás precedenst teremtett és rámutatott, hogy egy kis, erősen digitalizált ország infrastruktúráját a kibertérből érkező csapások is megbéníthatják, különösebb hagyományos fegyveres beavatkozás nélkül. [93]

Ezt követte 2008 augusztusában a Grúzia elleni háború, amelynek során a hagyományos fegyveres műveleteket összehangolt kibertámadások támogatták. A Dél-Oszétia körüli fegyveres összecsapással párhuzamosan orosz kötődésű hackerek bénították meg a grúz elnöki hivatal, parlament és több médiaportál honlapját, valamint közzétettek oda nem illő, propagandacélú üzeneteket. A támadások során mintegy 54 kormányzati és híroldalt értek el, és Grúzia internetforgalmának mintegy harmada akadozott vagy állt le a legintenzívebb napokon. A kibercsapások időzítése egybeesett az orosz csapatok előrenyomulásával augusztus 8-10. között, ami azt mutatja, hogy a kibertámadások szinkronban voltak a hagyományos katonai műveletekkel, mely a kiber- és konvencionális hadviselés összehangolt alkalmazásának egyik első gyakorlati példája . Bár a grúziai kibertér műveletek nem döntötték el a konfliktust, mégis világosan jelezték, hogy Oroszország új információs hadviselési modellt alkalmaz. Ennek keretein belül hazafias hackerek laza hálózatát mozgósították, akik az orosz állam hallgatólagos vagy közvetlen ösztönzésére támadták az ellenfél információs infrastruktúráját. [94]

A 2010-es években az orosz kibertér műveletek egyre kifinomultabbá és sokrétűbbé váltak. A korai, látványos bénító akciók mellett megjelent a hosszabb távú, rejtettebb kiberkémkedés és a kritikus infrastruktúrák elleni szisztematikus támadások sora. 2014-ben, a kelet-ukrajnai háború és a krími események idején Oroszország nem csupán a harctéren, hanem a kibertérben is aktív volt. Májusban az ukrán elnökválasztást célzó hackertámadási kampány zajlott, ami során egy oroszbarát hackercsoport több napon át tartó akciókkal próbálta megzavarni a választást. Például feltörték és kiszivárogtatták bizonyos jelöltek e-mailjeit, DDoS-támadásokkal lassították az eredmények közzétételét, sőt megpróbálták manipulálni a választási bizottság rendszerét . Utóbbi keretében egy kártékony programot juttattak a Központi Választási Bizottság hálózatába, amely a tervek szerint hamis eredményként a szélsőjobboldali Dmitro Jaros képét és győzelmét jelenítette volna meg a hivatalos honlapon. Az ukrán szakembereknek alig egy órával a szavazóhelyiségek zárása előtt sikerült eltávolítaniuk ezt a malware-t. Mindezek ellenére az orosz állami televízió, az Pervij Kanal még aznap este bemutatta a hamis Jaros-győzelmet hirdető grafikát, mint „az ukrán választási bizottság honlapján megjelent” eredményt, noha valójában soha nem került ki oda. Ezt a dezinformációt nyugati elemzők egyértelműen úgy értékelték, mint az orosz narratíva részét, amely azt hivatott alátámasztani, hogy „a kijevi forradalmat szélsőséges nacionalisták, neonácik vezették”. A 2014-es ukrán választási incidens így rávilágít a „hack-and-leak” műveletek és a propaganda összefonódására: orosz hackerek beavatkoztak a demokratikus folyamatba, majd a lopott vagy hamisított információt az orosz médiagépezet felhasználta a kívánt politikai narratíva terjesztésére. [95]

2015-ben Oroszország tovább fokozta az ukrajnai kibertérben folytatott hadviselést, immár az ország kritikus infrastruktúráját is célba véve. 2015. december 23-án példátlan kibertámadás érte Ukrajna három regionális áramszolgáltatóját. A támadók betörtek az áramszolgáltató vállalatok SCADA-irányító rendszereibe, és több kapcsolóállomást lekapcsoltak, mintegy 225 ezer fogyasztónál okozva áramszünetet, amely órákig tartott a téli hidegben. [96] A támadás módszeres volt és a behatolók először hónapokon át kémkedtek a hálózatokon, majd egy előre telepített rosszindulatú kód aktiválásával távoli vezérléssel lekapcsolták az áramot, miközben DDoS-támadással a hibabejelentő központokat is túlterhelték, hogy nehezítsék a reagálást. Az ukrán biztonsági szolgálat szerint az akció mögött az orosz hírszerzés állt, a műveletet pedig az úgynevezett Sandworm hacker-csoport hajtotta végre, amelyről köztudott, hogy orosz

katonai hírszerzéshez köthető. [97] Később az Egyesült Államok kiberbiztonsági hatóságai is megerősítették, hogy az eset egy államilag szponzorált támadás volt: a 2015-ös ukrán áramszünet volt az első dokumentált eset, amikor egy kibertámadás fizikai infrastrukturális kiesést – áramkimaradást – idézett elő, és ezt a nyugati kormányok egyértelműen Oroszország számlájára írták. A 2015-ös támadást 2016 végén egy hasonló, bár kisebb volumenű akció követte Kijevben, ismét az elektromos hálózat ellen, amivel világossá vált, hogy Oroszország stratégiai célpontként tekint az ukrán energetikai infrastruktúrára, és képes azt időről időre megbénítani kifinomult kiber-fegyverekkel. [98]

Az orosz kibertér műveletekben rejlő valós veszélyre a 2016-os események mutattak rá, amikor is az amerikai elnökválasztásba avatkoztak bele az orosz hackerek. Az amerikai hírszerző közösség 2017 elején nyilvánosságra hozott értékelése szerint Oroszország hírszerző szolgálatai kiterjedt kibertér műveleteket hajtottak végre a 2016-os amerikai elnökválasztás befolyásolása érdekében. [99] Ezek keretében orosz hackerek behatoltak az amerikai Demokrata Párt országos bizottságának és vezető kampánystábtagok e-mail fiókjaiba, és onnan nagy mennyiségű belső kommunikációt és dokumentumot loptak el. Ezt követően a GRU a "Guccifer 2.0" fedőnevű online személyiségen, illetve a DCLeaks weboldalon keresztül szivárogtatta ki a megszerzett adatokat, majd együttműködve a WikiLeaks-szel, ütemezetten nyilvánosságra hozta azokat. Az ellopott és kiszivárogtatott levelek számos kellemetlen vagy kompromittáló információt tartalmaztak a demokraták kampányáról, és az orosz dezinformációs kampány ezeket felnagyítva igyekezett megosztani az amerikai közvéleményt. Az amerikai hírszerzés „nagy valószínűséggel" arra a következtetésre jutott, hogy ezt a műveletet nagy valószínűséggel személyesen Vlagyimir Putyin utasítására hajtották végre, s célja az volt, hogy aláássa Hillary Clinton esélyeit és elősegítse egy oroszbarátabb jelölt, Donald Trump megválasztását. [100] Fontos kiemelni, hogy ez a beavatkozás egyrészt klasszikus kibertámadás, másrészt információs hadviselés volt. Ezzel Oroszország egy új szintre emelte a kibertér műveleteket és egy idegen hatalom belpolitikájának befolyásolására használta fel a kibertér adta eszközöket.

2017-ben Oroszország ismételten bizonyította offenzív kiberképességeit egy globális kibertámadással, amely „NotPetya" néven vált hírhedtté. 2017 júniusában, az ukrán alkotmány napján egy malware fertőzte meg ukrán intézmények és vállalatok százainak számítógépes hálózatait. A kártevő kezdetben zsarolóprogramnak álcázta

magát (a “Petya” továbbfejlesztett változataként), azonban valójában a titkosított állományok visszaállítására nem volt lehetőség, tehát a támadás célja nem a pénzszerzés, hanem az adatmegsemmisítés és megbénítás volt. A fertőzés Ukrajnából hamar tovább terjedt világszerte, nagy multinacionális vállalatok (Maersk, Merck, FedEx stb.) rendszereit is lebénítva. A támadás okozta anyagi kár globális szinten becslések szerint meghaladta a 10 milliárd dollárt, így ezt tartják minden idők legpusztítóbb kibertámadásának. [97] 2018 februárjában a nyugati országok egyhangúlag Oroszországot tették felelőssé a NotPetya támadásért: a Fehér Ház hivatalos közleményében kijelentette, hogy „2017 júniusában az orosz katonai erők indították a történelem legpusztítóbb és legköltségesebb kibertámadását”, amely Ukrajna destabilizálását célozta, ám végül szerte a világon féktelen pusztítást végzett. [101]

A NotPetya incidens megmutatta, hogy Oroszország kész a kibertérben is eszkalálni konfliktusait, akár úgy is, hogy a kontroll alól kikerülve globális károkat okoz. A támadásért közvetlenül a GRU, annak is a „Sandworm” néven ismert csoportja felelt. Ez az eset stratégiai üzenettel bírt, ugyanis jelezte, hogy egy államilag irányított kibertámadás akár fizikai gazdasági károkat is okozhat világszerte, és a nemzetközi normák hiányában nehéz az agresszort felelősségre vonni. A NotPetya után a NATO is deklarálta, hogy bizonyos kibertámadások akár aktiválhatják a kollektív védelem 5. cikkét, elismerve a kiberakciók potenciális pusztító hatását. [102]

3.2. 2014: a Krím annexiója

A 2014-es Krím-félsziget elfoglalása és annektálása gyakran szerepel példaként az orosz „újgenerációs hadviselés” sikerére. Moszkva ebben a műveletben ötvözte a katonai erőt a nem-hagyományos eszközökkel, hogy ellenállás nélkül ragadjon el egy területet egy szuverén államtól. A krími események egyúttal rávilágítottak arra, hogyan fonódik össze a kiber- és információs hadviselés a helyi politikai tényezőkkel és pszichológiai műveletekkel.

A Kijevben kitört 2014. februári forradalom eredményeként Oroszország számára kedvezőtlen helyzet alakult ki, ugyanis Ukrajnában nyugatbarát vezetés került hatalomra, miközben a Krím félszigeten jelentős orosz katonai jelenlét és orosz ajkú lakosság volt. Moszkva stratégiai érdeke az volt, hogy megakadályozza Ukrajna nyugati integrációját és megtartsa befolyását a térségben. E cél elérése érdekében az orosz vezetés hibrid hadviselést alkalmazott, amelyben a közvetlen katonai beavatkozást információs

hadműveletek készítették elő és támogatták. Az orosz hibrid háború lényege éppen az, hogy a katonai és nem katonai eszközök összehangolt kombinációjával törjék meg az ellenfél ellenállóképességét anélkül, hogy nyílt, nagy léptékű háború bontakozna ki. Krím esetében pontosan ez történt: a fegyveres akciók villámgyorsan, szinte vérontás nélkül zajlottak le, részben azért, mert az ukrán állam addigra politikailag és információs szinten is destabilizálódott. [103]

A krími művelet 2014 február végén indult, amikor megjelentek a zöld egyenruhás, azonosító nélküli katonák és ellenőrzésük alá vonták a stratégiai pontokat a félszigeten. A sikerükhöz azonban nagyban hozzájárult az, hogy az ukrán erők koordinációját és kommunikációját megzavarták. Orosz részről kibertámadások és elektronikai hadviselési eszközök bevetésére is sor került, amikkel a hackerek megtámadták az Ukrtelekom krími hálózatát, elvágva a félszigetet az Ukrán szárazföldi távközlési hálózattól, és átirányítva a kommunikációt orosz infrastruktúrára. Emellett beszámolók szerint orosz erők blokkolták a mobiltelefon-forgalmat is. A kijevi parlament egy bizottsági elnöke például arról számolt be, hogy február 27-én ismeretlen eszközökkel tömegesen zavarták az ukrán parlamenti képviselők telefonjait nyilvánvalóan annak érdekében, hogy akadályozzák a válság idején a kommunikációjukat. Ugyanekkor a krími terület védelméért felelős ukrán katonai egységek parancsnokai sem kaptak időben utasításokat Kijevből, melynek okai részben a kommunikációs zavarok, részben a politikai fejetlenség volt. Az orosz erők viszont biztosították a saját kommunikációjukat és C2-rendszereiket, így információs fölénybe kerültek helyben. [11]

A NATO StratCom szerint a Krím elfoglalása során ún. kétirányú cyber-hadviselés zajlott. Egyrészt a telekommunikációs eszközöket és médiacsatornákat ért támadások kommunikációs „blackout”-ot idéztek elő, másrészt pedig más kibertámadások a belföldi és nemzetközi közvélemény befolyásolását célozták. [104]

A Krím információs elszigetelését szolgálta az is, hogy az oroszbarát erők átvették a helyi médiát. Fegyveresek foglalták el a krími állami televíziót és rádiót, az ukrán tévécsatornákat pedig lekapcsolták, helyükön orosz állami tévét kezdtek sugározni. Ezzel párhuzamosan gombamód szaporodtak a közösségi médiában és internetes fórumokon a Kreml narratíváit terjesztő üzenetek. Az orosz állam már korábban létrehozott egy ún. troll hadsereget, melynek tagjai hamis profilok ezreivel posztoltak oroszpárti

kommentárokat és álhíreket. 2014 elején Szentpéterváron egy Internet Research Agency (IRA) nevű cégben több száz fizetett alkalmazott dolgozott napi 12 órás műszakokban azon, hogy online fórumokon és közösségi oldalakon befolyásolják a véleményeket. [105] A krími válság során Moszkva legalább 600 fős koordinált hacker csapatot vetett be, mintegy 19 millió dolláros ráfordítással, hogy folyamatosan kommenteljenek, blogoljanak és posztoljanak az annexiót támogató tartalmakat. A céljuk egyrészt a helyi lakosság meggyőzése volt arról, hogy a félsziget visszatérése Oroszországhoz történelmi igazságszolgáltatás, másrészt a nemzetközi közvélemény befolyásolása, hogy elhiggyék, hogy a krímiek többsége önként, örömmel csatlakozik Oroszországhoz. [106] A közösségi médiában terjedő üzenetek gyakran félelem- és gyűlöletkeltő rémhírek voltak, melyek az ukrán erőket igyekeztek démonizálni. Elhíresült példa egy álhír, miszerint ukrán katonák Szlovjanszk főterén egy oroszajkú hároméves kisfiút keresztre feszítettek az édesanyja szeme láttára – ezt a rémtörténetet az orosz Pervij Kanal televízió is leadta 2014 júliusában. Később független tényellenőrzők egyértelműen cáfolták, hogy ilyesmi történt volna, de addigra a hír futótűzként terjedt a közösségi hálókon, tovább szítva a haragot az ukránok ellen. Hasonló dezinformáció volt egy kitalált orvos, bizonyos Igor Rosovszkij története, aki azt állította a Facebookon, hogy szemtanúja volt: az odesszai zavargások során ukrán nacionalisták oroszbarát aktivistákat égettek el élve egy épületben, és még az életben maradt sebesülteket is hagyták meghalni, miközben antiszemita megjegyzéseket tettek. E hamis bejegyzést 24 óra alatt több mint 5000-szer osztották meg orosz közösségi oldalakon. [106]

Noha az ilyen történeteket később lebuktatták, a válság forró szakaszában erőteljesen formálták a közhangulatot.

A Krím elfoglalásának információs műveletei nem csak a dezinformáció terjesztését jelentették, hanem a pszichológiai hadviselést is. Az orosz média folyamatosan azt sugallta, hogy Ukrajnában káosz és fasiszta fenyegetés uralkodik, ami elől a krími oroszoknak Oroszország védelmet nyújt. Ugyanakkor azt is kommunikálták, hogy az ukrán erők tömegesen adják meg magukat és állnak át. A krími lakosság oroszbarát részét Moszkva tudatosan mozgósította. A helyi orosz szervezetek és médiafelületek már a válság előtt terjesztették a szeparatizmus gondolatát, így mire az orosz katonák megjelentek, egy részben fogékony közeget találtak. Ennek csúcspontja a 2014. március 16-án megrendezett népszavazás volt, amelyet az orosz narratíva a népek önrendelkezéseként mutatott be, holott azt fegyveres jelenlét és nemzetközileg illegitim

keretek között tartották meg néhány héttel a terület elfoglalása után. A népszavazás hivatalos eredménye (a szavazók 96%-a a csatlakozásra voksolt) kétségkívül manipulált volt, de a propaganda sikerét mutatja, hogy ezt az eredményt sok orosz és krími elhitte, és a nemzetközi közvélemény egy része is bizonytalan volt a krímiek valódi akaratát illetően. [104]

A fentiekből azt a következtetést vonom le, hogy a krími annexió esettanulmánya egyértelműen megmutatja, mennyire fontos az információs fölény és a kibertér kontrollja a modern hadviselésben. Oroszország a hadművelet során elérte, hogy az ukrán vezetés vak és béna legyen a krími terepen, mert sem kommunikálni, sem reagálni nem tudott hatékonyan. Ezzel párhuzamosan Moszkva felépített egy legitimációs narratívát a saját lakossága és a világ felé, amely a történteket nem agresszióként, hanem a hazatérésként keretezte. Kibertér műveletek járultak hozzá a fizikai műveletek és információs műveletek biztosították a politikai sikerhez szükséges narratív környezetet. Bár katonailag az orosz erőfölény nyilvánvaló volt, a váratlan fordulatot nagymértékben segítette, hogy az ukrán társadalom megosztottá vált a propaganda által, a nemzetközi reakció pedig késlekedett a bizonytalan információk közepette. [104]

3.3. Virális háború: az orosz-ukrán háború a közösségi médiában

Az orosz-ukrán konfliktus 2014-től zajló folyamata, különösen a 2022 februárjában kezdődött nyílt háború, gyakran kapta a „első közösségi média-háború" vagy a „TikTok-háború" jelzőt. Noha nem ez volt az első konfliktus, melyről valós időben értesülhetett a világ, a digitális platformok soha nem látott módon és mértékben váltak a harctér kiterjesztésévé. A háború virális jellege több szempontból is megnyilvánult. Egyrészt a konfliktusról szóló hírek, videók, mémek és narratívák vírus módjára terjedtek a globális közösségi hálózatokon, másrészt a hadviselő felek tudatosan alkalmazták a közösségi médiát pszichológiai hadviselési és propagandacélokra. [58]

Már a 2022-es invázió első napjaiban világossá vált, hogy a közösségi média kulcsszerepet kap a fegyveres konfliktusban. Az ukrán kormányzat proaktív kommunikációba kezdett, amely során Volodimir Zelenszkij ukrán elnök rendszeresen jelentkezett okostelefonos videóüzenetekkel a megtámadott fővárosból. Ezek a személyes hangvételű videoüzenetek a Facebookon és X-en percek alatt bejárták a világot, óriási hatást gyakorolva a nemzetközi közvéleményre és a morálra. Zelenszkij és kabinetje a közösségi médián keresztül mozgósította a nyugati támogatást is: a #StandWithUkraine,

#ArmUkraineNow és hasonló kampányok révén empátiát és segítséget kértek, amihez civil aktivisták milliói csatlakoztak online. Ez egy új jelenség volt, ami során egy megtámadott ország vezetője közvetlenül, közvetítők nélkül tudott kommunikálni a külföldi népekkel és döntéshozókkal, mozgósítva a nemzetközi közvéleményt. Ennek eredményeként a nyugati kormányokra nagy nyomás nehezedett, hogy támogassák Ukrajnát – részben a közösségi médiában kifejeződő erős szolidaritási hullám miatt. [107]

Az ukrán lakosság és civil társadalom is fegyverként használta a közösségi hálózatokat. A frontvonalról és a megszállt területekről számtalan civil által rögzített videó és kép került fel a netre valós időben, dokumentálva a háború eseményeit. Ezek a tartalmak egyrészt bizonyítékul szolgáltak az orosz háborús bűnökre másrészt a közösségi médiás posztok egy része közvetlen hírszerzési értékkel bírt. Az ukrán katonai hírszerzés és a nyugati szakértők is felhasználták az OSINT keretében a TikTokon, Telegramon közzétett videókat az orosz csapatmozgások nyomon követésére. Ismert példa, hogy már 2022 elején, még az invázió indulása előtt egy orosz tankokat szállító vasúti szerelvény videója felkerült a TikTokra Belaruszban, ezzel idő előtt jelezve a csapatösszevonást. [108] A háború kitörése után az ukrán hatóságok még egy okostelefonos alkalmazást is indítottak, amelyen keresztül a civilek bejelenthették az észlelt ellenséges erőket, járműveket. Így a lakosság digitális partizánhálózatként segítette a honvédelmet. Ez a fajta ún. crowdsourcing korábban nem látott módon kapcsolta be a civil lakosságot a hadviselésbe, ugyanis okostelefonjaik révén szinte bárki hírszerzővé vagy propagandistává válhatott.

Oroszország eközben saját információs offenzíváját folytatta a közösségi médiában, bár jelentős kihívásokkal szembesült. A Kreml 2022-ben is arra törekedett, hogy dezinformációval és propaganda-narratívákkal igazolja a háborút és megtörje az ukrán ellenállást. Az orosz állami média és a hozzá kötődő online hálózatok számos hamis narratívát terjesztettek. Azt állították például, hogy Ukrajnában náci junta uralkodik, amely népirtást követ el az oroszajkúak ellen, hogy az Egyesült Államok biológiai fegyverlaborokat működtet Ukrajnában, vagy hogy az ukrán vezetés valójában nem is létezik. Az orosz dezinformáció három fő keretben igyekezett tálalni a háborút: a Donbasz mint áldozat és az ott élőket érő vélt sérelmek, az ukrán vezetés és nacionalizmus, mint ellenség, amely fenyegeti Oroszországot és a ruszin kisebbséget, valamint Ukrajna mint a Nyugat bábja amelyben Oroszország a NATO és EU ellen harcol. Ezeket a narratívákat a Kreml évek óta sulykolta, de a teljes invázió idején még

intenzívebben jelentek meg, különösen az orosz nyelvű közegben. 2022-ben az orosz propaganda-csatornák soha nem látott mennyiségű hamis hírt generáltak. Független elemzők egy év alatt több mint 160 különféle hamis narratívát azonosítottak az orosz–ukrán háború kapcsán, és legalább 460 olyan weboldalt találtak, amelyek rendszeresen terjesztettek orosz dezinformációs tartalmakat a háborúról. [109]

Fontos hangsúlyozni, hogy a 2022-es invázió információs csataterén Oroszország nem ért el olyan egyértelmű fölényt, mint 2014-ben Krímben. Ennek több oka volt. Egyrészt, a nyugati technológiai platformok sokat tanultak a 2016-os és utáni beavatkozásokból. Az invázió nyomán a Meta például letiltotta az RT és a Szputnyik orosz állami csatornákat az EU-ban, és figyelmeztető címkékkel látta el az orosz állami média tartalmait világszerte. Az X 2022-ben szintén korlátozta az állami média elérését. A YouTube globálisan blokkolta az orosz állami propagandacsatornákat. Ezek a lépések jelentősen szűkítették a Kreml dezinformációs hálózatának mozgásterét a mainstream platformokon. [110] Oroszország ezért alternatív utakat keresett. Előtérbe került a Telegram mint kvázi-szabályozatlan platform, valamint az olyan nyugati szélsőséges weboldalak és fórumok, ahol a tartalommoderáció gyenge. Emellett Moszkva igyekezett technikai eszközökkel is manipulálni a közösségi médiát és botnetek, ill. automata profilok segítségével próbálták felnagyítani a saját narratíváikat. A háború kezdeti szakaszában az X-en a háborúhoz kapcsolódó tartalmak mintegy 10-15%-át automatizált fiókok generálták. [111] Az orosz oldalon a botok főként azokat az üzeneteket erősítették fel, amelyek megosztottságot szítottak a nyugati közvéleményben, illetve az összeesküvés-elméleteket terjesztették. Az ukrán oldalon a botok jellemzően információt próbáltak szerezni vagy cáfolni az orosz narratívákat, de a két fél tevékenysége nem volt egyensúlyban és az orosz dezinformáció terjedése sokkal szervezettebb és bőségesebb volt. [112] A háború előrehaladtával a Twitter/X moderációs változásai tovább rontották az online információs környezetet és 2023-ra jelentősen leépítették a platform Trust and Safety csapatát, így az erőszakos tartalmak és félrevezetések kiszűrése akadozot Az Európai Unió 2023 végén vizsgálatot is indított az X ellen, mivel az októberi közel-keleti konfliktus kapcsán is rengeteg hamis hír terjedt a platformon. [113]

Mindeközben a közösségi média nem csupán a dezinformáció, de a kreatív ellenállás terepe is lett. Az ukrán és nemzetközi támogatók humorral és mémekkel vették fel a harcot az orosz propagandával szemben. Megalakult a NAFO (North Atlantic Fellas Organization) nevű internetes jelenség, ami ez egy laza, X-en szerveződő közösség,

amely kutyás mémeket használva gúnyolja és fárasztja az orosz hivatalos fiókokat, trollkodva válaszol az orosz dezinformációra. A NAFO afféle „mém-hadseregként” vált ismertté, amely hatékonyan terelte el a figyelmet az orosz propagandisták bejegyzéseiről és közben adománygyűjtéseket is szervezett az ukrán hadsereg javára. [114] Ez jól példázza, hogy a közösségi médiában nem csak állami szereplők és automatizált fiókok tevékenykednek, hanem spontán alulról jövő kezdeményezések is formálják az információs teret. A háború eddigi tapasztalatai arra utalnak, hogy bár Oroszország továbbra is magas szinten űzi az információs hadviselést, a nyílt demokratikus társadalmak is megtalálhatják az ellenszer egy részét azáltal, hogy közösségeik ellenállóbbak a hamis narratívákkal szemben, és a tényellenőrző szervezetek, civil aktivisták gyorsan reagálnak a terjedő hazugságokra.

A 2022–2023-as orosz-ukrán háború tehát kettős képest mutat a közösségi média-hadviselésről. Egyrészt a háborút jóformán élőben közvetítik a platformokon, hiszen a világ közvéleménye a telefonjai képernyőjén napi rendszerességgel szembesül a konfliktus képeivel, legyen szó rakétacsapások videóiról, frontkatonák sisakkamerás felvételeiről vagy menekültek személyes történeteiről. Ez az eddigi legdokumentáltabb háború a nyilvánosság előtt. Másrészt soha nem volt ennyire éles az információs hadviselés sem. Mindkét fél igyekszik a valóságot a maga képére formálni a digitális térben. A közösségi média tehát egyszerre a tanúságtétel eszköze és a manipuláció terepe. Emiatt a nézőknek, olvasóknak kritikusabbnak kell lenniük, a platformoknak pedig felelősséget kellene vállalniuk a tartalmak kezelésében. Az eddigi tapasztalatok alapján kijelenthetjük, hogy az ukrajnai háború során formálódik a közösségi média-hadviselés új kora, ahol a digitális műveltség és az ellenőrzött információk szerepe kulcsfontosságú. [115]

3.4. Jom kipur 2.0.: háború testközelből a közösségi médiában

2023 októberében egy, az orosz-ukrán háborútól független, de annak tanulságaihoz mégis szorosan kapcsolódó esemény sokkolta a világot, méghozzá a Hamasz váratlan támadása Izrael ellen. A 2023. október 7-i offenzíva az 1973-as jóm kippúri háború óta a legsúlyosabb meglepetésszerű csapásként érte Izraelt, ennek okán többen „Jom kipur 2.0”-nak kezdték nevezni a történteket. Az analógia nem csupán a váratlanságra utal, hanem arra is, ahogyan a modern technológia révén a háború borzalmai testközelbe kerültek a civil lakosság számára. A közösségi média itt is kulcsszerepet játszott és a

támadók és az áldozatok szemszögéből egyaránt valós időben jelentek meg brutális tartalmak az online térben, precedens nélküli módon.

A Hamasz fegyveresei a támadás napján nem csak fizikai atrocitásokat követtek el, hanem tudatosan fegyverként használták a közösségi médiát a terror pszichológiai keltésére. Több esetben az történt, hogy a terroristák az általuk meggyilkolt vagy túszul ejtett izraeli civilek okostelefonjait felhasználva élőben közvetítették vagy feltöltötték a gyilkosságok felvételeit az áldozatok saját közösségi profiljaira. Egy ilyen dokumentált esetben egy izraeli nagymama meggyilkolását a támadók lefényképezték/videózták, majd az ő Facebook-fiókján keresztül posztolták, így a nő családtagjai és ismerősei saját hírfolyamukban szembesültek szerettük kegyetlen kivégzésével. [113]

Mire a platform moderátoraihoz eljutott ez az esemény, addigra a videó sokakhoz eljutott a világ számos pontján. Ez a döbbenetes módszer rámutatott arra, hogy a gyilkosok direkt célja volt nemcsak a fizikai pusztítás, de a távol lévő emberek traumatizálása és megfélemlítése is a social media eszközeivel, ami új kihívás elé állítja a platformokat is. [113]

A támadás és az azt követő háború során a közösségi média elárasztódott brutális és felkavaró tartalommal. A Telegram csatornákon és az X felületén perceken belül terjedni kezdtek a képek a megtámadott izraeli fesztiválról, a kibucokban elkövetett mészárlásokról, valamint a Gázából Izraelbe hurcolt túszokról. Sok felvétel hiteles volt és a valós eseményeket mutatta be, mások azonban manipuláltak vagy kontextusukból kiragadottak voltak. A dezinformáció is gyorsan megjelent és egyes felhasználók régi háborús videókat osztottak meg friss eseményekként, vagy éppen hamis vádakat terjesztettek. Ugyanígy, amikor néhány nappal később robbanás történt egy gázai kórháznál, a közösségi médiában percek alatt futótűzként terjedtek egymásnak ellentmondó narratívák. Palesztin források 500 halottról beszéltek egy izraeli légicsapás miatt, míg izraeli források azt állították, hogy egy eltévedt iszlamista rakéta csapódott be a parkolóban. Az X-en és más platformokon számtalan kétes hitelességű fotó és videó keringett a helyszínről, ami világszerte tüntetéshullámot indított el, mire a hivatalos vizsgálatok napokkal később sokkal alacsonyabb áldozatszámot és a Hamaszt sejtető felelősséget valószínűsítettek. Ez az eset is rávilágított arra, hogy a háború első narratívája immár a közösségi médiában formálódik, gyakran megelőzve a tényszerű valóság

feltárását. A jelenséget súlyosbította, hogy néhány nagy platform a moderátor-csapatok csökkentése miatt nem tudta hatékonyan kezelni a helyzetet. [116]

Ami a lélektani hatásokat illeti a közösségi médián terjedő, testközelből származó háborús tartalmak erőteljes érzelmi reakciókat váltottak ki világszerte. Egyrészt növelték az együttérzést és szolidaritást az áldozatok iránt, másrészt azonban a megrázó képsorok gyűlölethullámokat is generáltak. Nyugaton megugrott mind az antiszemita, mind az iszlamofób incidensek száma, ahogy a háború képei polarizálták a társadalmakat. Megfigyelhető volt egyfajta visszacsapó hatásról, ami értelmében az erőszakos tartalmak terjedése a közösségi médiában radikalizálhatja a nézőket, bosszúra vagy gyűlöletre sarkallva őket. A Hamasz épp erre játszott, hiszen brutalitásuk fitogtatásával és annak online terítésével a megfélemlítés mellett azt is el akarták érni, hogy izraeli reakcióként minél erősebb legyen a megtorlás. [117]

A Jom kipur 2.0 kifejezés egyrészt utal arra, hogy 50 évvel az 1973-as háború után Izrael hasonló sokkot élt át, másrészt arra is, mennyire megváltozott a háború természete a technológia által.

1973-ban a világ csak napokkal-hetekkel később értesült a háború borzalmairól és diplomáciai bonyodalmairól, míg 2023-ban emberek milliárdjai valós időben követték az eseményeket a X-en, YouTube-on, TikTokon. A távolságot a digitális kor eltörölte és a háború testközelből ér mindenkit, aki okostelefonnal rendelkezik. Ez egyszerre jelenti azt, hogy nem lehet elhallgatni a háborús bűnöket, de azt is, hogy a háborúk emberi szenvedése felerősítve hat a társadalmakra, potenciálisan további erőszakot gerjesztve. A közösségi média tehát etikai és gyakorlati dilemmákat vet fel a konfliktusok bemutatásában. Hogyan lehet megakadályozni, hogy a terrorcselekmények elkövetői ingyen propaganda-platformként használják e szolgáltatásokat? Miképp védjük meg a civil felhasználókat a traumatizáló tartalmaktól anélkül, hogy a tájékoztatás csorbulna? Hogyan kezeljük a valós idejű dezinformációt egy háborús krízis során? Ezek a kérdések égetően aktuálisak lettek.

Az EU 2023 végén már a Digital Services Act (DSA) új eszközeivel figyelmeztette a nagy platformokat a felelősségükre, jelezve: kötelezettségük proaktívan fellépni a háborús dezinformáció és erőszakos tartalmak ellen, különben jogi következményekkel néznek szembe. [118]

3.5. Részkövetkeztetések

A fenti esettanulmányok elemzésével azt a megállapítást teszem, hogy Oroszország élen jár a hibrid hadviselésben, azt már-már művészi szintre emelte, melynek lényege a **katonai, kiber- és információs eszközök integrált alkalmazása**. A 2020 előtti kibertámadások során Oroszország demonstrálta, hogy képes az ellenfelek kritikus infrastruktúráit megbénítani, titkos adatokat eltulajdonítani és fegyverként felhasználni, valamint dezinformációs kampányokkal megingatni demokratikus folyamatokat. E támadások nem elszigetelten jelentkeztek, hanem minden esetben egy geopolitikai cél szolgálatába álltak.

A bemutatott esettanulmányokból levont nagyon fontos következtetésem, hogy a 2014-es krími válság példája rámutatott, hogy **a hagyományos katonai sikerek mögött sokszor az információs fölény és a kibertérben vívott harc áll**. Krímben az oroszok azért tudtak szinte ellenállás nélkül teret nyerni, mert előbb megbénították az ukrán fél kommunikációját és narratíváját és a „hard power" hatását a „soft power" műveletei többszörözték meg. Ez lényegében Geraszimov (az orosz vezérkari főnök) által 2013-ban felvázolt nem-lineáris hadviselés doktrínájának sikeres alkalmazása volt, ahol a nem-katonai eszközök azonos súlyt kapnak a katonaiakkal. [119]

Harmadszor, az orosz-ukrán háború virális információs hadszíntere megmutatta, hogy **a közösségi média egyszerre erősítheti és gyengítheti a propaganda hatását**. Oroszország történelmi léptékű dezinformációs offenzívát indított, ám üzenetei a nyugati társadalmakban már kevésbé voltak hatékonyak a megnövekedett tudatosság és ellenintézkedések miatt. Ugyanakkor a közösségi média révén az ukrán fél is globális támogatói hálózatot építhetett és hatásosan kommunikálhatta saját narratíváját. A virális háború korában a percepciókért folytatott küzdelem szorosan összefonódik a fizikai harccal és a nyilvánosság megnyerése majdnem olyan fontos, mint egy csata megnyerése a terepen. [106]

Negyedszer, a „Jom kipur 2.0" esete általános tanulságokkal szolgál a háború média-árnyékáról. A **közösségi média valós időben közvetíti a háború borzalmait** a világ minden pontjára, ami **egyrészt növelheti a nemzetközi nyomást a konfliktusok lezárására**, másrészt **eszkalálhatja is az erőszakot azáltal, hogy szélsőséges reakciókat vált ki**. A háború virtualizálódása dilemmák elé állítja a nemzetközi közösséget. Például, hogy hogyan egyensúlyozható a szabad információáramlás és a

káros tartalmak korlátozása, miként vonhatóak felelősségre az online térben is tevékeny háborús bűnösöt, és hogyan védhetőek meg a civileket ebben az új környezetben.

Megállapítom, hogy **az információs hadviselés és a kibertér műveletek immár nem különülnek el a hadviselés főáramától, hanem annak integráns részét képezik.** Az orosz példák stratégiai racionalitást mutatnak, bármennyire is elítélendők némely cselekedetek morális vagy jogi szempontból. A kibertérben folytatott hadviselés aszimetriája Oroszországnak kedvez, hiszen hagyományos katonai ereje elmarad a NATO mögött, de a kiber- és információs térben viszonylag olcsón és tagadható módon tudott eredményeket elérni. Ugyanakkor a legújabb fejlemények azt jelzik, hogy az ilyen műveletek hatásfoka csökkenhet, amint az ellenfelek alkalmazkodnak. Az ukrajnai háború azt bizonyította, hogy a nyílt társadalmak is tudnak rezilienciát építeni, hiszen az aktív tényellenőrzés, a civil ellen-narratívák és a diplomáciai-digitális együttműködés képes részben kivédeni a Kreml manipulációit. Mindazonáltal a kihívás óriási, mert a jövő háborúiban valószínűleg még kifinomultabb kibertámadásokkal és még alattomosabb közösségi média-manipulációkkal kell számolnunk. A nemzetközi közösség feladata lesz olyan normák és védelmi mechanizmusok kialakítása, melyek korlátok közé szorítják az állami és nem állami szereplők pusztító tevékenységét a kibertérben.

A fejezet esettanulmányai együttesen arra hívják fel a figyelmet, hogy a 21. századi háború fogalmát újra kell gondolnunk. Már nem csupán tankokkal, rakétákkal és katonákkal vívják, hanem bitekkel, narratívákkal és tweetekkel is. Az orosz gyakorlat jól példázza, milyen hatékony és veszélyes lehet ez a komplex hadviselés, hiszen képes romba dönteni gazdaságokat egy malware segítségével, választásokat eldönteni e-mailek kiszivárogtatásával, vagy épp harc nélkül elfoglalni területeket az információs tér manipulálásával. Ugyanakkor a nyílt információs környezet hosszabb távon vissza is üthet az agresszorra, mert a valóság előbb-utóbb felszínre kerül, mint ahogy a hosszan tartó ukrajnai háború esetében a nemzetközi közösség fokozatosan átlát az orosz dezinformáción, és a támogatás nem lankad.

4. FEJEZET
ELLENINTÉZKEDÉSEK A KIBERTÉRI KÖZÖSSÉGI MÉDIÁN KERESZTÜLI BEFOLYÁSOLÁS ELLEN ÉS AZ ELLENÁLLÓKÉPESSÉG NÖVELÉSÉNEK LEHETŐSÉGEI

Az információs műveletek és a kibertér műveletek által jelentett fenyegetések globalizálódásával párhuzamosan világszerte megjelent az igény a hatékony ellenintézkedések kidolgozására és a társadalmak ellenállóképességének növelésére. Míg az előző fejezet a dezinformációs és kibertevékenységek gyakorlati sajátosságait vizsgálta, addig e fejezet átfogó, nemzetközi nézőpontból elemzi, hogyan reagálnak a demokratikus társadalmak ezekre a kihívásokra. Az alábbiakban sorra veszem a szabályozási megközelítéseket és kihívásokat, a digitális műveltség és oktatás szerepét, a technológiai megoldásokat, a társadalom ellenálló képességének erősítését különös tekintettel a kritikus gondolkodás fejlesztésére, valamint a nemzetbiztonsági és kiberbiztonsági aggályokat. A célom egy globális és kiegyensúlyozott áttekintés nyújtása, ahol nem csupán egyetlen állam szemszögéből, hanem általános nemzetközi példákon és gyakorlatokon keresztül vizsgálom a válaszlépéseket.

4.1. Szabályozási megközelítések és kihívások

A dezinformáció és a rosszindulatú kibertevékenységek elleni küzdelem egyik alappillére a megfelelő szabályozási keretek kialakítása. Számos ország és nemzetközi szervezet próbál választ adni arra a kérdésre, hogy a jog eszközeivel hogyan lehet gátat vetni az online térben terjedő káros információknak anélkül, hogy aláásnánk a szólásszabadságot és a nyílt kommunikáció alapelveit. A szabályozási megközelítések terén azonban komoly kihívások mutatkoznak, mivel a jogalkotóknak egy rendkívül gyorsan változó és globális jelenségre kell reagálniuk. Az alábbiakban áttekintem a különböző szabályozási stratégiákat és a velük kapcsolatos dilemmákat.

4.1.1. Állami szerepvállalás és nemzetközi iránymutatások

Nemzetközi szinten egyre több kormányzat ismeri fel, hogy az online dezinformáció problémája átlépi az országhatárokat, ezért összehangolt szabályozási lépésekre van szükség. Az Európai Unió az elmúlt években úttörő szerepet vállalt a platformszabályozásban. 2018-ban önszabályozó jelleggel megszületett az EU dezinformáció visszaszorítását célzó magatartási kódexe, amelyben nagy online platformok vállaltak önkéntes kötelezettségeket a hamis tartalmak terjedésének visszaszorítására. [120] Ez a megközelítést az önszabályozás és társszabályozás elemeit ötvözte, melyet később továbbfejlesztettek. Az EU 2022-ben elfogadott átfogó digitális szabályozási csomagja, a Digital Services Act (DSA, A digitális szolgáltatásokról szóló rendelet) már jogilag kötelező erővel ír elő kockázatértékelési és -mérséklési kötelezettségeket a nagy online platformok számára, kifejezetten említve az olyan rendszerszintű kockázatokat, mint a dezinformáció terjedése. [118] A DSA keretében az önkéntes kódex egyfajta társszabályozási eszközzé vált, amelynek betartását a szabályozó hatóságok is figyelemmel kísérik. [121]

Mindemellett több nemzetközi szervezet próbál iránymutatást nyújtani a kormányok számára. Az UNESCO 2023-ban több szakterület bevonásával globális útmutatót tett közzé a digitális platformok szabályozásáról, amely hét alapelvet fogalmaz meg annak érdekében, hogy a platformok felelősségre vonhatók legyenek a káros tartalmak kezelésében, miközben a felhasználók szabad véleménynyilvánításhoz való joga sem csorbul. Az UNESCO hangsúlyozza a többszereplős megközelítést, amely keretein belül a kormányok, a technológiai cégek, a civil szféra és a nemzetközi szervezetek együttműködését hangsúlyozzák annak érdekében, hogy globális normákat alakítsanak ki a digitális térben. [122] Hasonlóképpen, az ENSZ emberi jogi mechanizmusai is állást foglaltak és az ENSZ, ill. más nemzetközi szervezetek különleges rapportőrei már 2017-ben közös nyilatkozatban figyelmeztettek, hogy az álhírek elleni büntetőjogi fellépés könnyen a szólásszabadság indokolatlan korlátozásához vezethet, és ezért kerülendő. Az ENSZ emberi jogi főbiztosának hivatala 2021-ben átfogó jelentésben elemezte a dezinformáció jelenségét, és rámutatott: a kormányoknak elsősorban nem tiltó szabályokkal, hanem pozitív intézkedésekkel – átláthatóság, oktatás, média támogatása – kell az információs ökoszisztéma egészségét javítaniuk. [123]

4.1.2. Jogalkotási példák és dilemmák

Egyes országok önálló jogszabályokkal próbálkoztak az online tér szabályozására. Németország már 2017-ben elfogadta a NetzDG néven ismert törvényt, amely kötelezi a közösségi média szolgáltatókat, hogy a jogellenes gyűlöletkeltő tartalmakat 24 órán belül távolítsák el. Bár a NetzDG közvetlenül nem a dezinformációra irányult, precedenst teremtett a platformok felelősségének szabályozására és vitákat váltott ki a szólásszabadság lehetséges korlátozása miatt. [124] Franciaország 2018-ban kifejezetten a választások idején terjesztett álhírek ellen hozott törvényt, amely lehetővé teszi bírói úton bizonyos tartalmak eltávolítását a választási kampányok alatt. Ennek hatékonysága azonban korlátozottnak bizonyult, és a kritikusok szerint nehéz meghúzni a határt politikai vélemény és szándékos dezinformáció között. [125] Litvánia és Lettország a nemzetbiztonság részeként tekint az információs tér védelmére, és jogszabályokkal, valamint operatív testületekkel lép fel a külföldi félretájékoztatás ellen, beleértve a bizonyos weboldalak vagy bot-hálózatok blokkolásának lehetőségét is. [121]

Ugyanakkor a jogalkotási megközelítés számos dilemmát rejt magában. Az egyik legfőbb kihívás a fogalmak meghatározása. Mit tekintsünk dezinformációnak vagy káros tartalomnak? A túl tágan vagy homályosan megfogalmazott törvényi definíciók könnyen visszaélésekhez vezethetnek, illetve öncenzúrára késztethetik a platformokat. A jogszerű, de káros online tartalmak szabályozása különösen problémás demokratikus keretek között, mivel az állami cenzúra tilalma mellett ezen tartalmak kiszűrését többnyire a magáncégekre hárítja, amelyek azonban nem kötődnek közvetlenül az alkotmányos szólásszabadság normáihoz. Ebből következik, hogy ha a kormányok erősen ösztönzik vagy kötelezik a platformokat a határesetnek minősülő tartalmak eltávolítására, az könnyen a véleménynyilvánítás közvetett cenzúrájához vezethet. [124] Erre példa volt az Egyesült Királyság Online Biztonsági Törvénytervezete, ami eredetileg bevezette a legális, de káros tartalom fogalmát a felnőttekre nézve is, amelyet a platformoknak korlátozniuk kellett volna, ám a tervezet ezen részét 2022 végén kivették a javaslatból és inkább a platformok átláthatósági kötelezettségeire helyezték a hangsúlyt. [126]

A másik fontos kihívás a joghatóság kérdése. Az internet globális természete miatt egy adott ország törvényei nehezen érvényesíthetők egy nemzetközi platformon vagy külföldön működő szereplővel szemben. Például hiába tilt be egy ország egy külföldi dezinformációs weboldalt, az könnyen új domain alatt vagy más szervereken tovább

működhet. A nemzetközi együttműködés ezért kulcsfontosság az Európai Unió 2019-ben létrehozta a Rapid Alert System-et a tagállamok közötti információmegosztásra a választási beavatkozásokkal kapcsolatban, valamint rendszeresen egyeztet az USA-val és más partnerekkel a külföldi információs befolyás visszaszorításáról. [127]

4.1.3. Ön- és társszabályozás, platformfelelősség

A kormányzati szabályozás mellett megjelentek az önszabályozói kezdeményezések és az iparági gyakorlatok is a dezinformáció elleni küzdelemben. A nagy technológiai vállalatok az elmúlt években kénytelenek voltak reagálni a társadalmi és politikai nyomásra. Számos platform vezetett be saját szabályzatot a hamis információk terjesztésének tilalmára, fejlesztett ki tényellenőrző programokat és jelentési felületeket a felhasználók számára. Az ilyen önkéntes lépések fontosak, de önmagukban nem tudják kezelni a probléma méretét és sebességét, hiszen a többmilliárdnyi napi poszt kézi moderálása lehetetlen, az automatikus szűrők pedig gyakran pontatlanok, ezért a jelenlegi rendszer sokszor „túl kevés, túl későn” alapon reagál a terjedő álhírekre. [128]

Az önszabályozás ezért sok helyen átfordul a hatóságok bevonásával történő társszabályozásba. Ennek lényege, hogy az iparági szereplők kidolgozzák a normákat és technikai megoldásokat, de egy állami szerv felügyeli vagy jóváhagyja azokat, biztosítva az elszámoltathatóságot. [121] Az említett EU dezinformációs kódex 2022-es megerősítése is ebbe az irányba mutat. A kódex aláírói, köztük a nagy platformok és online hirdetési szereplők vállalták, hogy átláthatóbbá teszik algoritmusaikat kutatók számára, és rendszeresen beszámolnak a dezinformáció elleni lépéseikről, mindezekért cserébe pedig az EU Bizottság nyomon követi és értékeli e vállalások teljesítését. [120] Hasonló elképzelés formálódik az Egyesült Királyságban is. A szigetországban az Online Biztonsági Törvény 2023-as verziója elsősorban kötelező átláthatósági jelentéseket és felhasználói védelempolitikákat ír elő a platformoknak, de nem definiál új tiltott tartalomkategóriát a káros dezinformációra. Ehelyett a hangsúly a platformok felelősségén és a felhasználók képessé tételén van. [129]

Fontos kiemelni, hogy a túlzottan szigorú vagy büntető jellegű állami fellépést a szakértők többsége ellenzi a demokratikus berendezkedésű országokban. Az eredményes szabályozás inkább arra törekszik, hogy növelje a digitális tér átláthatóságát és integritását, nem pedig arra, hogy egyszerűen kriminalizálja a félrevezető tartalmakat. [123]

4.2. Digitális műveltség és oktatási kezdeményezések

A dezinformáció elleni küzdelemben kulcsszerepe van a társadalom tudatosságának és felkészültségének. A tapasztalatok szerint minél képzettebbek a polgárok a digitális média használatában, és minél jobban értik az online tartalmak keletkezésének, terjedésének módját, annál kevésbé válnak a manipuláció áldozataivá. [121] Éppen ezért az utóbbi években számos ország indított digitális és médiaműveltségi oktatási programokat, hogy megerősítse a lakosság ellenálló képességét a félrevezető információkkal szemben.

4.2.1. Média- és digitális műveltségi programok világszerte

Finnországot gyakran emlegetik jó példaként, ahol már a 2010-es évek közepétől stratégiai prioritásként kezelték a médiaműveltség oktatását a formális iskolarendszerben. A finn tanterv része a kritikus gondolkodás, forráskritika és a digitális tartalmak értékelésének képessége, melynek köszönhetően Finnország rendre az élen végez a dezinformációval szembeni társadalmi reziliencia felméréseken. Hasonló kezdeményezések indultak a balti államokban is, például Észtországban "Média és manipuláció" címmel vezettek be középiskolai kurzust, amely interaktív módon tanítja a diákokat a propaganda és álhírek felismerésére. Franciaországban a médiatudatosság erősítésére 2015 óta működik a CLEMI nevű központ, amely tanároknak nyújt képzéseket és tananyagokat a sajtó és digitális média oktatásához, valamint országos projekteket koordinál. [121]

Az Európai Unió intézményi szinten is segíti e területet. 2019-ben létrehozta az Európai Digitális Média Megfigyelőközpontot (EDMO), amely kutatóintézeteket, fact-checkereket és médiaműveltségi szakértőket hálózatba szervezve egyrészt monitorozza a dezinformáció trendjeit, másrészt erősíti a tagállamok médiatudatossági kezdeményezéseit. Az EDMO égisze alatt számos nemzeti kezdeményezés alakult, amelyek programokat dolgoznak ki a helyi igényekre szabva. Emellett az EU Demokrácia cselekvési terve (2020) hangsúlyozza a polgárok képessé tételét a digitális korban, és anyagi forrásokat különített el médiaműveltségi projektek támogatására. [130]

A digitális műveltség erősítésének fontosságát a nemzetközi szervezetek is kiemelik. Az UNESCO régóta szervez Médiaműveltség és Információs Műveltség (MIL) programokat világszerte, és minden évben megtartják a Global MIL Week-et, amely során jó gyakorlatokat osztanak meg és tudatosító kampányokat folytatnak. Az UNESCO

anyagai hangsúlyozzák, hogy a digitális korban a médiaértés állampolgári alapkészséggé vált, amely nélkülözhetetlen a demokrácia fenntartásához. [122]

4.2.2. Kritikus gondolkodás és kognitív ellenálló képesség a dezinformációval szemben

Az oktatási kezdeményezések mögött meghúzódó egyik alapelv, hogy megelőző jelleggel növeljék a társadalom immunitását a félrevezető információkkal szemben. E megközelítés gyakran az ún. inokulációs elméletre támaszkodik, amelyet a pszichológia területén eredetileg már az 1960-as években megfogalmaztak. Ennek lényege, hogy ha az embereket előre felkészítjük a várható megtévesztő érvelési trükkökre vagy manipulációkra, mintegy "oltást" adva nekik kis dózisú hamis információ és annak cáfolata révén, akkor később, amikor szembe találkoznak egy ilyen jelenséggel sokkal ellenállóbbak lesznek azokkal szemben. [131]

Az inokulációs megközelítést az utóbbi években konkrét oktatási eszközökre ültették át. Ilyenek például a digitális játékok és interaktív tréningek, amelyek szórakoztató formában tanítják meg a dezinformáció felismerését. A Cambridge Egyetem kutatói által kifejlesztett Bad News játékban a játékos maga válik fake news gyártóvá és így tapasztalja meg a manipuláció módszereit, majd a kísérő magyarázatok segítik felismerni ezeket a valóságban. Ez a játék bizonyítottan növelte a résztvevők szkepticizmusát a megtévesztő tartalmakkal szemben. [132] Ugyanez a kutatócsoport a COVID-19 pandémia idején kifejlesztette a Go Viral! nevű minijátékot, amely néhány perc alatt "beoltja" a játékost a járványhoz kötődő gyakori félrevezető narratívák ellen; ennek hatékonyságát egy nemzetközi kísérlet is alátámasztotta. [133]

Az oktatási programok eredményességével kapcsolatban egyre több empirikus kutatás lát napvilágot. Ezek általában biztató, bár árnyalt képet festenek. Egy friss elemzés szerint a médiaértés-oktatás és a kritikus gondolkodás fejlesztése az egyik leghatékonyabb hosszú távú eszköz a dezinformáció ellen, ugyanakkor azonnali áttörést nem várhatunk tőle és nehéz széles körben gyorsan kiterjeszteni. (Bateman, Jackson, 2024) A Carnegie Endowment 2024-es szakpolitikai összegzése rámutatott, hogy a média- és digitális műveltségi programok hatása jelentős, de az implementációjuk nehéz és erőforrás-igényes, különösen idősebb korosztályok esetén, akiket már nem érnek el az iskolai programok. [134] Kutatások kimutatták, hogy az idősebb felnőttek (különösen a 65 év feletti korosztály) hajlamosabbak felelőtlenül megosztani álhíreket a közösségi médiában részben digitális szocializációjuk hiányosságai miatt, ezért a médiatudatossági

erőfeszítéseket rájuk is ki kell terjeszteni például közösségi foglalkozásokkal vagy nyugdíjas klubok bevonásával. [135]

4.3. Technológiai megoldások

A modern információs környezetben a kihívást sok tekintetben maguk a technológiai platformok és eszközök teremtik, ugyanakkor a megoldásoknak is részben technológiai jellegűeknek kell lenniük. A nagy mennyiségű online tartalom emberi erővel történő moderálása és ellenőrzése gyakorlatilag kivitelezhetetlen, így az utóbbi években egyre nagyobb hangsúly helyeződik az automatizált, mesterséges intelligencia vezérelte megoldásokra a dezinformáció felismerésében és visszaszorításában. [136] Emellett a kibertér műveletek elleni védekezésben is új technológiák jelennek meg, beleértve az olyan fejlett védelmi rendszereket, amelyek képesek azonosítani és elhárítani a támadásokat még azelőtt, hogy komolyabb károkat okoznának.

4.3.1. Mesterséges intelligencia és automatizált tartalomszűrés

A közösségi médiaplatformok első generációs válasza a problémára a moderátorok és tényellenőrök alkalmazása volt, emberi munkaerővel kiszűrve a legkirívóbb félrevezető tartalmakat. Gyorsan kiderült azonban, hogy ez a megközelítés nem skálázható. Például a Facebook több ezer moderátort foglalkoztat világszerte, mégsem képes minden álhír vagy manipuláció gyors kiszűrésére, ráadásul komoly késéssel reagál sok esetben. [134] Ezért a platformok párhuzamosan fejlesztenek algoritmikus szűrőket is. A mesterséges intelligencia (MI) lehetőséget ad arra, hogy a rendszer automatikusan azonosítson gyanús mintázatokat.

Egy innovatív közelítés az érzelemelemzés alkalmazása a félrevezető tartalmak detektálására. Ahogy a NATO egy elemzése is kiemelte, az online terjedő álhírek gyakran erős érzelmi reakciókat váltanak ki, míg a valós hírek jellemzően kevésbé szenzációs érzelmekhez kapcsolódnak. E felismerés alapján MI-algoritmusok próbálják előre jelezni, hogy egy adott poszt tartalmaz-e olyan érzelmi indikátorokat, amelyek a dezinformáció jellemzői. Egy kísérleti projektben a Johns Hopkins Egyetem kutatói olyan modellt hoztak létre, amely az érzelmi profil alapján szűri a posztokat, és az eredmények ígéretesek voltak és az algoritmus sok esetben előbb kiszűrte a potenciális álhírt, minthogy az tömegesen elterjedt volna. Fontos ugyanakkor kiemelni, hogy az efféle automatizált szűrés csupán valószínűségekkel dolgozik, és nem tévedhetetlen, így

általában emberi felülvizsgálattal együtt alkalmazzák, különösen, amikor súlyos következményekkel járó döntésekről van szó. [136]

4.3.3. Új fenyegetések: deepfake és AI által generált tartalom

A technológiai fronton nem csak a védekezés, de a támadás eszközei is fejlődnek. Az elmúlt években komoly aggodalom övezi az ún. deepfake technológia terjedését, vagyis amikor mesterséges intelligencia segítségével valósághű hamis videókat vagy hangfelvételeket állítanak elő, mintha egy közszereplő mondott vagy tett volna valamit, ami sosem történt meg. A deepfake-ek és más AI-generált tartalmak új dimenziót adhatnak a dezinformációnak. 2022-2023-ban már előfordult, hogy hamis, generált képek vagy hangok megtévesztettek nagyközönséget, például deepfake videó jelent meg az ukrán elnökről, ahogy megadja magát, illetve hamis audiofelvételek keringtek politikusok nyilatkozatairól. [137]

A védekezés erre a fenyegetésre is technológiai jellegű lehet. Kutatók és vállalatok dolgoznak deepfake-detektorok fejlesztésén, amelyek az emberi szem számára láthatatlan digitális nyomokat képesek felismerni, és így automatikusan jelezni, ha egy médiafájl gyaníthatóan mesterséges. [138]

4.3.4. Kiberbiztonsági technológiák a védekezésben

A kiberműveletek és az információs műveletek sokszor kéz a kézben járnak. A kritikus infrastruktúrákat vagy informatikai rendszereket érő kibertámadások ellen a hagyományos IT-biztonsági megoldásokat kellett továbbfejleszteni, tekintettel arra, hogy az államilag támogatott támadók és a szervezett bűnözői csoportok egyre kifinomultabb módszereket alkalmaznak. A mesterséges intelligencia itt is megjelent: pl. fejlett anomáliaészlelő rendszerek figyelik a hálózati forgalmat és a bejelentkezéseket, hogy valós időben kiszúrják a szokatlan mintákat, amelyek betörésre utalhatnak. Az ilyen rendszerek önmaguktól tanulva képesek megkülönböztetni a legitim, de rendhagyó tevékenységet a valódi támadástól, így hatékonyabbak lehetnek a hagyományos, statikus tűzfalszabályoknál.

Továbbá, a nemzetállamok és nemzetközi szervezetek is fejlesztenek speciális technológiai képességeket a kibertér védelmére. A gépi tanulás segíthet a támadók módszereinek osztályozásában és gyors attribúciójában is. A kísérleti rendszerek próbálják automatikusan elemezni a támadás nyomait és korábbi adatbázisokkal

összevetve következtetnek arra, melyik ismert csoporthoz lehet köthető az incidens. [139] Bár a támadások megbízható forrásazonosítása továbbra is nagy kihívás, az automatizált elemző eszközök felgyorsíthatják az attribúciós folyamatot, amely kulcsfontosságú lehet a megfelelő politikai vagy jogi válaszlépések (pl. szankciók) meghozatalához.

4.4. A társadalmi ellenálló képesség kiépítése: a kritikus gondolkodás képességének erősítése

A technológiai és jogi-intézményi lépések mellett legalább ugyanolyan fontos a társadalmi szintű ellenálló képesség fejlesztése. Az, hogy a közösségek, a polgárok milyen mértékben képesek ellenállni a félrevezető propagandának, mennyire tudatosan fogyasztják az információkat, és milyen erős a társadalmi kohézió és bizalom, amely megnehezíti a külső vagy belső rosszindulatú befolyásolók dolgát. A dezinformáció ugyanis ott tud igazán romboló hatású lenni, ahol eleve mély törésvonalak, bizalmi válságok vagy információs vákuumok vannak a társadalomban.

4.4.1. Kritikus gondolkodás és kognitív immunitás

A társadalmi ellenálló képesség talán legnehezebben megfogható, de rendkívül lényeges eleme a kritikus gondolkodás kultúrája. Ez egyfajta mentális oltóanyag, amely nem feltétlenül konkrét tudásanyagot jelent, hanem egy attitűdöt és készséget, avagy a hajlandóságot és képességet arra, hogy a befogadott információkat az egyén megkérdőjelezze, több forrásból ellenőrizze, és tudatában legyen a saját kognitív torzításainakA pszichológiai kutatások igazolják, hogy az emberek gyakran nem azért hisznek el hamis híreket, mert nem tudnák a valóságot, hanem mert a hamis hír érzelmileg vagy világnézetileg rezonál velük, és nem fordítanak elegendő figyelmet a kritikai értékelésre. Ezért a kritikus gondolkodás fejlesztése részben arról szól, hogy megtanítsuk az embereket lelassítani és reflektálni, mielőtt egy tartalmat igaznak fogadnak el vagy továbbküldenek. [131]

A kritikus gondolkodás erősítése sokrétű feladat. Az oktatást már említettem, de e készség fejlesztése nem ér véget az iskolapadban. Gyakran szó esik a “nudging” (terelés) technikákról is. Például a közösségi médiában a platformok apró pszichológiai ösztönzőket építhetnek be, amelyek a felhasználót gondolkodásra késztetik. Egy kísérletben az X felhasználók egy részének megjelent egy üzenet, mielőtt megosztottak volna egy cikket, hogy “Olvasta a cikket? A megalapozott véleményhez érdemes átfutni,

mielőtt megosztja.” Ez az egyszerű emlékeztető bizonyítottan csökkentette az ellenőrizetlen cikkek megosztását. [134]

A civil társadalom és a média is sokat tehet a társadalmi immunitásért. Fontos a független sajtó megerősítése és a helyi közösségek információs ökoszisztémájának támogatása. A helyi újságírás és közösségi média hiánya sokszor vákuumot teremt, amit könnyen töltenek be külső manipulátorok, ezért a helyi hírek és információk hiteles csatornáinak fenntartása az ellenálló képesség része. [134]

A társadalmi kohézió erősítése is kritikus tényező. A dezinformációs kampányok gyakran rájátszanak meglévő társadalmi megosztottságokra, az etnikai, vallási, politikai törésvonalakra. Ha egy társadalom tagjai között erősebb a párbeszéd és az empátia, kevésbé válnak polarizált narratívák foglyává.

4.5. Nemzetbiztonsági és kiberbiztonsági aggályok

Az információs műveletek és a kibertámadások elleni küzdelem nem csupán civil vagy technológiai kérdés, hanem a nemzetbiztonság szerves része is lett a 21. században. A kormányok és védelmi intézmények felismerték, hogy a kibertérben zajló fenyegetések közvetlen hatással lehetnek egy ország szuverenitására, politikai stabilitására és végső soron fizikai biztonságára.

4.5.1. A fenyegetés nemzetbiztonsági keretezése

A hidegháború után sokáig a nyugati nemzetbiztonsági gondolkodás perifériáján voltak az információs műveletek. Az utóbbi bő évtized azonban gyökeresen megváltoztatta ezt a szemléletet. Ma már általánosan elfogadott, hogy a kiber- és információs támadások hibrid hadviselési eszközként jelennek meg, és ezek akár egy fegyveres konfliktus előkészítését is szolgálhatják. Ennek megfelelően a NATO 2014-ben elismerte, hogy egy jelentős kibertámadás akár a kollektív védelemre vonatkozó 5. cikkelyt is aktiválhatja, vagyis a kiberteret immár a hadviselés lehetséges terepeként kezelik. [20]

Szintén a NATO keretében 2019-ben megalakult az Európai Unióval közösen az Egyesített Hibrid Fenyegetések Elleni Kiválósági Központ (Hybrid CoE) Helsinkiben, amely kutatja és tréningezi az ilyen jellegű fenyegetések elleni védekezést. Számos ország frissítette nemzetbiztonsági stratégiáját vagy védelmi doktrínáját, hogy beillessze az információs hadviselést, mint fenyegetési kategóriát. Az USA védelmi minisztériuma is kiadott egy kiberstratégiát, amelyben külön fejezet foglalkozik az előretolt

védekezéssel (Defend Forward), amely lényege, hogy az amerikai kiberparancsnokság már a kibertérben igyekszik aktívan zavarni és akadályozni az ellenséges információs műveleti kapacitásokat, még mielőtt azok az USA-ban célba érnének. [140]

Ennek keretében például amerikai kiberműveleti szakemberek 2018-ban sikeresen bénították meg egy időre az orosz trollgyár szervereit a félidős választások idején, hogy megakadályozzák a dezinformációs kampányokat. [141]

Bár az efféle offenzív intézkedések részletei titkosak, létezésük jelzi, hogy a deterrencia és zavarás a nemzetbiztonsági eszköztár részévé vált az információs hadviselés ellen. Európában is számos ország emelte be a stratégiai dokumentumaiba e fenyegetéseket. Egyesült Királyság 2021-es Integrált Felülvizsgálata az ország kül-, védelem- és biztonságpolitikai jövőképét vázolja és kiemelten foglalkozik a "state-based threats" között a dezinformációval és kibertevékenységgel, és bejelentette egy új Nemzeti Kiberműveleti Központ felállítását, amely a hírszerzéssel karöltve akár támadó kibertér műveleteket is végrehajthat az ilyen fenyegetést jelentő aktorok ellen. [142]

4.5.2. Védelmi és hírszerző együttműködések

Mivel a dezinformációs fenyegetések gyakran határokon átnyúlóak, a nemzetbiztonsági dimenzió elválaszthatatlan az szövetségesi és nemzetközi együttműködésektől. A NATO nem csak közös doktrínát alkotott, de gyakorlatokat is tart a tagállamoknak: pl. a Steadfast Defender hadgyakorlatok kiegészültek szimulált információs műveleti helyzetekkel, hogy a parancsnokok és civilek is gyakorolják, miként kezeljenek egy helyzetet, ha a hagyományos katonai fenyegetés mellett a médiában és online is álhírek árasztják el a közvéleményt. [25] Az EU keretében a tagállamok 2019 óta működtetik a Rapid Alert System-et, amely a külügyi szolgálat (EEAS) szervezésében heti jelentésekkel és eseti riasztásokkal informálja a kormányokat a felmerülő dezinformációs kampányokról, és javasol ellenlépéseket. [120] Az EU továbbá létrehozta a Hibrid Fenyegetések Elleni Európai Központot (EU Hybrid Fusion Cell), amely az uniós intézményeken belül gyűjti a hírszerzési információkat a tagállamoktól a hibrid hadviselés jelenségeiről, beleértve az információs műveleteket is, és összképet alkot a fenyegetési trendekről. [143]

4.5.3. Dilemmák a biztonsági válaszokban

Miközben a nemzetbiztonsági szemlélet erősödik, fontos dilemmák is felmerülnek. Az egyik ilyen a belső, ill. külső fenyegetés kérdése. Sok demokratikus ország alkotmánya

és jogrendszere szigorúan elválasztja a külső hírszerző tevékenységet a belső, avagy az állampolgárokra irányuló megfigyeléstől. Az információs hadviselés azonban gyakran belső csatornákon zajlik és egy külföldi narratívát belföldi szereplők is átvesznek és terjesztenek. Ez felveti annak igényét, hogy a nemzetbiztonsági szervek valamilyen módon figyeljék a belföldi információs terepet is, hiszen a külföldi befolyás e csatornákon át ér célt. Ugyanakkor ez könnyen összeütközésbe kerülhet a polgári szabadságjogokkal és adatvédelmi normákkal. Általános konszenzus, hogy az átláthatóság és jogi kontrollok kulcsfontosságúak, hiszen minden ilyen erőfeszítésnek világos mandátummal, civil felügyelettel és csak a valódi külföldi fenyegetésre fókuszálva szabad működnie. [123]

Másik dilemma a katonai és a civil vezetés kérdése. Egyes országoknál a kibervédelmi képességek a hadsereghez kerültek, míg máshol polgári ügynökségek felelnek értük. Hasonlóan, az információs műveletekre adott reakció lehet stratégiai kommunikáció vagy pszichológiai hadviselés. A NATO országok jellemzően arra törekszenek, hogy a civilek kezében maradjon a lakossági tájékoztatás és média, még válság idején is, és a katonaság csak támogató vagy hírszerzési szerepet töltsön be. Ez azért fontos, mert ha a narratívaformálás átcsúszik a katonai logika alá, az akár hitelteleníthetí is a kormányzati kommunikációt békeidőben. Így a legtöbb helyen kétpilléres megoldás van, azaz civil válságkommunikációs struktúrák a nyilvánosság felé, és katonai/civil hírszerzési együttműködés a háttérben az információs fenyegetések elemzésére és közvetítésére a döntéshozók felé. [144]

Végül meg kell említeni, hogy a nemzetbiztonsági fókusz erősödése nem vezethet a demokratikus értékek feladásához. Ez önellentmondás lenne, hiszen pont ezek védelmében lépünk fel a hibrid fenyegetésekkel szemben. A nyugati nyílt társadalmak ereje éppen a rugalmasságukban és adaptív képességükben rejlik, amely azonban a szabad eszmecsere és átláthatóság talaján áll. Bármilyen ellenintézkedés, amely aláásná ezeket többet ártana, mint használna, mert saját demokratikus immunrendszerünket gyengítené. Éppen ezért a nemzetbiztonsági szervek egyre inkább a reziliencia fogalmára helyezik a hangsúlyt a “kontroll” helyett. Arra, hogy a társadalom képes legyen kiheverni egy-egy információs támadást, minimalizálni annak hatását, és tanulni belőle. [136]

4.6. Részkövetkeztetések

A fejezetben bemutattam és elemeztem a kiber- és információs fenyegetések elleni ellenintézkedések sokrétű rendszerét, rámutatva a globális gyakorlatokra és stratégiákra.

Megállapítottam, hogy a **probléma komplexitása miatt nincs egyedüli, mindenható megoldás**. Az **eredményes védekezés feltételezi a többdimenziós megközelítést**, amely magában foglalja a **jogi szabályozást**, a **technológiai eszközöket, az oktatást és a társadalmi tudatformálást** egyaránt.

A szabályozási keretek terén a világ országai a megfelelő egyensúly megtalálásával küzdenek és olyan törvényeket és irányelveket igyekeznek alkotni, amelyek gátat szabnak a legártalmasabb online tevékenységeknek, ugyanakkor nem fojtják el a szabad véleményáramlást és kreativitást, ami a demokratikus társadalmak alapja. A legfőbb kihívás továbbra is a joghatóság és a definíciók pontosítása, illetve a visszaélések elkerülése, azaz, hogy a dezinformáció elleni harc ne válhasson ürüggyé a legitim kritika elhallgattatására.

A digitális műveltség és oktatás fontosságát egyetlen komoly szakmai forrás sem vitatja. Míg a szabályozás és technológia inkább reaktív módon kezeli a tüneteket, addig az oktatás a gyökerénél próbál beavatkozni a problémába és tudatos, kritikus gondolkodású felhasználókat nevelni, akik kevésbé hiszékenyek a manipulációval szemben. Számos ország példaértékű médiaműveltségi programokat vezetett be, és a kutatások igazolják is ezek jótékony hatását. [133]

Ugyanakkor világos az is, hogy az oktatás hosszú távú befektetés, eredményei nem azonnal jelentkeznek, és nehéz a teljes lakosságot lefedni vele, különösen a már felnőtt korú generációkat. Ennek ellenére a társadalmi reziliencia építésének alapja marad a műveltség növelése, a kritikus gondolkodás normájának terjesztése, aminek az oktatási intézményektől a civil szervezeteken át a családokig minden szinten támogatottá kell válnia.

A technológiai megoldások nélkül a védekezés esélytelen volna a digitális korszak sebessége és volumene mellett. A mesterséges intelligencia és az automatizált rendszerek már most is segítik a platformokat és a hatóságokat a gyanús tartalmak és hálózatok kiszűrésében. [136] Fejlett algoritmusok fürkészik a botokat, elemzik a tartalmak nyelvezetét, sőt a terjedés dinamikáját is, hogy időben közbe lehessen avatkozni. Az innovációk azt mutatják, hogy kreatív ötletekben nincs hiány. A deepfake és más új fenyegetések megjelenése pedig arra sarkallja a védelmi oldalt, hogy mindig egy lépéssel előrébb járjon. Ugyanakkor a technológia kétélű kard, hiszen a támadók is mesterséges intelligenciához nyúlnak, és gyakran a védelem is csak annyira erős, amennyire az emberi

felhasználói láncszem az, ezért a tech megoldások sosem válthatják ki teljesen az emberi ítélőképességet és etikai normákat a folyamatból.

A társadalmi ellenálló képesség és a kritikus gondolkodás kultúrája voltaképp az oktatás és a közösségi szintű cselekvés metszete. Olyan közeg kialakítása a cél, ahol a polgárok maguk is aktív szereplői a védekezésnek. Felismerik és jelzik a dezinformációt, nem adják tovább, sőt akár ellen-narratívákat terjesztenek. Ide tartozik a civil gondolkodásmód és a független média szerepe is akár formálisan, akár informálisan. A bizalom építése a kulcseleme ennek. Ahol ez megvan, ott a külső rosszindulatú befolyásnak sokkal nehezebb gyökeret vernie. [131]

Végezetül a nemzetbiztonsági és kiberbiztonsági megközelítés integrálása arról gondoskodik, hogy az állam rendelkezzen a szükséges erőforrásokkal és felhatalmazással az ellencsapásokhoz és elhárításhoz. Ahogy a kibertámadásokat képesnek kell lenni gyorsan izolálni és visszaverni a kritikus infrastruktúrák védelme érdekében, úgy az információs hadviselésre is kellenek protokollok és felelős intézmények. A demokratikus országok e téren is lépéseket tettek: külön egységek, stratégiák, szankciók szolgálják a nemzetek szuverenitásának védelmét a kibertérben. Fontos azonban, hogy mindezt a nyílt társadalmak ne a szabadságjogok feláldozásával érjék el. Az ellenállóképesség lényege, hogy megtartjuk azon értékeinket, amelyeket a támadók elvennének.

5. FEJEZET

A KÉRDŐÍVES KUTATÁS BEMUTATÁSA

A disszertáció elméleti kereteinek gyakorlati alátámasztása érdekében egy saját szerkesztésű, online kérdőíves felmérést végeztem. **A kutatás elsődleges célja az volt, hogy felmérjem a civil lakosság – mint az információs műveletek elsődleges célpontja – tudatossági szintjét, valamint azt, hogy a felhasználók mennyire képesek felismerni a közösségi médiában megjelenő befolyásolási kísérleteket.** A kérdőívet úgy állítottam össze, hogy a válaszadók széles körét érjem el, így a célközönséget a magyarországi közösségi média-felhasználók alkották, tekintet nélkül azok szakmai hátterére.

A kérdőíves kutatás eredményeinek bemutatása során a felmérés kvantitatív adatait és a szakértői interjúkból származó kvalitatív megállapításokat egyaránt vizsgáltam. Ebben a fejezetben részletesen bemutatom a kérdőív eredményeit, melyeket összevetek a három szakértői interjú (Haig Zsolt, Bányász Péter és Kovács László) legfontosabb gondolataival, rávilágítva az egybecsengésekre és az esetleges eltérésekre. A fejezet második részében pedig javaslatokat fogalmazok meg az eddigi eredmények alapján.

A kérdőíves kutatás célja annak feltárása volt, hogy a válaszadók miként értékelik a közösségi média szerepét az információs műveletek és a kibertéri műveletek kontextusában, különös tekintettel annak alkalmazhatóságára, kockázataira és stratégiai jelentőségére. A vizsgálat célja továbbá annak meghatározása volt, hogy a közösségi média milyen mértékben tekinthető önálló műveleti eszköznek az információs környezet befolyásolásában, valamint milyen hatással van a műveleti biztonságra, a döntéshozatali folyamatokra és az információs fölény megszerzésére.

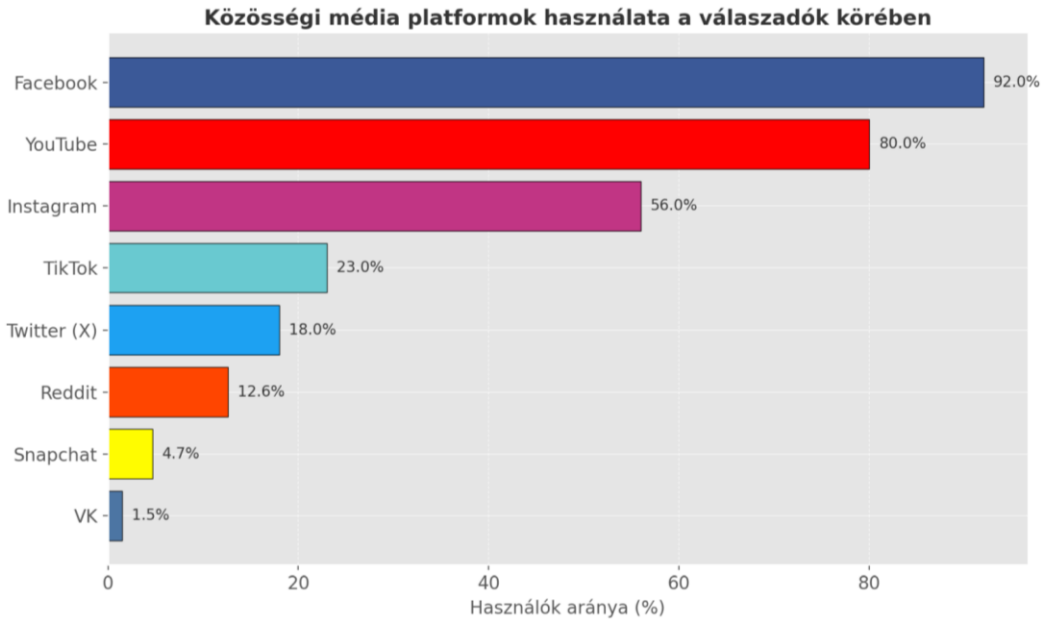
A kérdőíves adatfelvétel lehetőséget biztosított arra, hogy empirikus adatok álljanak rendelkezésre a közösségi média katonai és kiberbiztonsági vonatkozásainak megítéléséről, valamint a kapcsolódó fenyegetések és alkalmazási lehetőségek percepciójáról. A kutatás célja ezen túlmenően az volt, hogy a válaszadók tapasztalatain és véleményén keresztül alátámassza vagy árnyalja a szakirodalmi elemzés és az esettanulmányok alapján megfogalmazott elméleti megállapításokat, ezáltal hozzájárulva a kutatási hipotézisek empirikus vizsgálatához és a következtetések megalapozásához.

5.1. Az eredmények szintézise

A korábban online közétett online kérdőívet összesen 253 fő töltötte ki. A minta nemek szerinti megoszlása enyhén férfi többséget mutatott, ahol a válaszadók 57,7%-a férfi, 40,3%-a nő volt, míg ~2% (5 fő) nem kívánt válaszolni a nemére vonatkozó kérdésre. A válaszadók életkori összetétele vegyes képet mutatott, de enyhe eltolódás figyelhető meg az idősebb korosztályok felé. A legnagyobb korcsoportot az „50 év felettiek" alkották, de jelentős arányban képviseltették magukat a 46–50 éves és a 36–40 éves válaszadók is. A fiatalabb felnőttek (18–29 év között) összesen mintegy 14,6%-ot tettek ki.

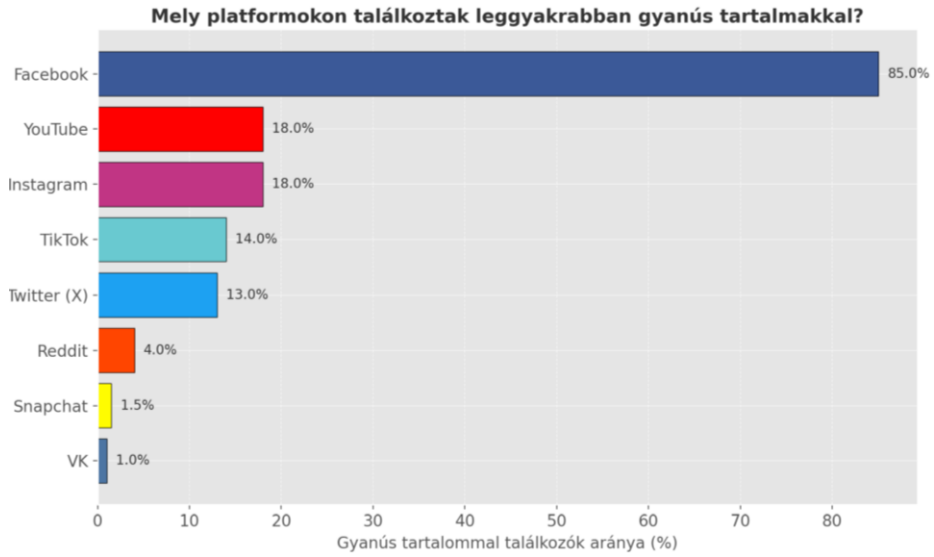
A lakóhely tekintetében a fővárosi válaszadók voltak a legtöbben (44,7%), ami érthető lehet egy online terjesztett kérdőív esetén, de jelentős volt a kisvárosok (22,5%) és nagyvárosok (20,6%) aránya is. Községekben vagy falvakban élők kisebb részt képviseltek (összesen kb. 12%). Ez az összetétel azért fontos, mert a demográfiai tényezők hatással lehetnek a közösségi média használati szokásokra és az információs műveletekkel kapcsolatos észlelésekre.

A kérdőív egyik alapvető kérdésblokkja a közösségi média használatának gyakoriságára és céljaira vonatkozott. Az eredmények szerint a válaszadók túlnyomó többsége rendszeresen és intenzíven használja a közösségi média platformokat. A kitöltők 69,2%-a napi több órát tölt a közösségi médián, további 23,7% pedig naponta legalább egy órát szán rá. Mindössze elenyésző hányad mondta azt, hogy hetente csak néhány órát vagy ennél is ritkábban használ közösségi médiát. Ezek az adatok arra utalnak, hogy a felmérésben résztvevők körében a közösségi média szerves része a mindennapoknak, ami megalapozza az információs műveletek kitettségét és hatását is. A közösségi médiát a válaszadók többféle célra használják, és gyakran párhuzamosan több funkciót is betölt számukra. Négy fő használati cél rajzolódott ki a feleletekből, méghozzá a kapcsolattartás családdal és barátokkal, érdeklődési körhöz tartozó csoportok és oldalak követése, hírfogyasztás, valamint egyéb szórakozás (például videók, mémek fogyasztása). A válaszadók 81,8%-a jelölte meg a személyes kapcsolattartást mint célt, és még ennél is többen (87%) használják arra a közösségi médiát, hogy hobbijukkal, érdeklődési területükkel kapcsolatos tartalmakat kövessenek. Figyelemre méltó, hogy a kitöltők több mint két harmada hírfogyasztásra is igénybe veszi e platformokat, azaz a közösségi média egyben hírfórumként is szolgál számukra. Ez a tény különösen fontos az információs műveletek szempontjából, hiszen a dezinformáció gyakran épp a híreknek álcázott tartalmak révén terjed.



4. ábra: Közösségi média platformok használata a válaszadók körében

A kérdőív rákérdezett arra is, mely konkrét közösségi média platformokat használják a válaszadók. A kérdésre érkezett eredményeket a 3. ábra szemlélteti, mely eredmények azt mutatják, hogy a Facebook toronymagasan a legelterjedtebb, hiszen a kitöltők mintegy 92%-a jelölte meg a Facebookot használt platformként. Ezt követi a YouTube, amelyet a válaszadók kb. 80%-a használ. Az Instagram is igen népszerű, a kitöltők körülbelül 56%-a aktív ott. A fiatalabb korosztályok körében globálisan rendkívül trendi TikTok platformot a válaszadók kisebb, de nem elhanyagolható része (kb. 23%) használja. A Twitter (új nevén X) itthon kevésbé elterjedt. A felmérésben résztvevők 18%-a jelölte, hogy használja. Ugyancsak kisebbségben vannak a Reddit (kb. 12,6%) és a Snapchat (kb. 4,7%) felhasználók a mintában, míg orosz kötődésű VKontakte (VK) oldalt mindössze 1-2% említette. A platformhasználat gyakoriságának ismerete azért lényeges, mert megmutatja, hol koncentrálódik leginkább a felhasználók figyelme, és így azt is, hogy potenciálisan milyen csatornákon érdemes keresni az információs műveletek nyomait. Ahogy Dr. Bányász Péter az interjúban hangsúlyozta, a közösségi média decentralizált, gyors és hatékony kommunikációs csatornákat biztosít különböző aktorok számára, beleértve az állami és nem állami szereplőket is, amit a fenti adatok is megerősítenek.



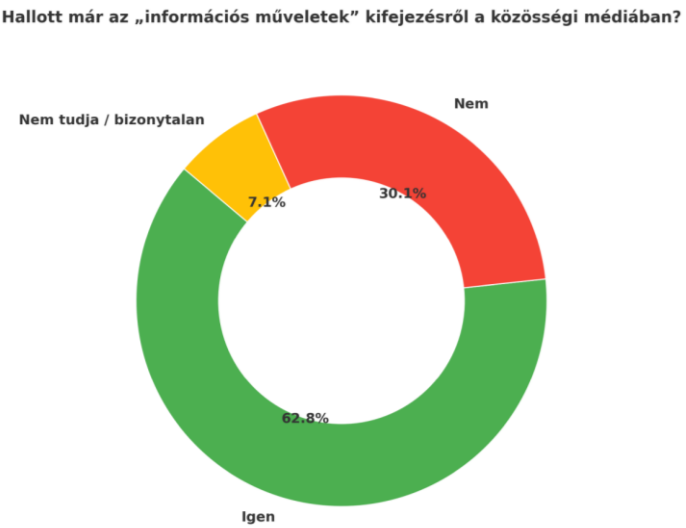
5. ábra: Mely platformokon találkoztak leggyakrabban gyanús tartalmakkal?

A széles elérésű platformok különösen vonzó eszközei az információs hadviselésnek, mivel egyszerre hatnak nagyszámú felhasználóra. A platformhasználat mellett kritikus kérdés, hogy hol találkoznak a felhasználók gyanús vagy manipulált tartalmakkal. A válaszadók több opciót is megjelölhettek arra a kérdésre, hogy melyik platformon szembesültek a legtöbb gyanús tartalommal. Az eredmények, melyeket a 4. ábra szemléltet, megerősítik azt a feltevést, hogy a kiterjedt használat és a gyanús tartalmak előfordulása között erős összefüggés van. A kitöltők döntő többsége, 85%-a, a Facebookot nevezte meg olyan platformként, ahol gyakran találkozik gyanús tartalommal. Ezzel a Facebook nemcsak a legnépszerűbb, de a felhasználói tapasztalatok szerint a legfertőzöttebb platform is ebből a szempontból. YouTube és Instagram egyaránt a válaszadók mintegy 18-18%-a szerint bővelkedik gyanús tartalmakban. Ez azért is figyelemreméltó, mert a YouTube-ot nagy arányban használják a megkérdezettek, az Instagramot pedig valamivel kevesebben, tehát mindkét platformon számottevő a potenciálisan félrevezető információ a megkérdezettek szerint. A TikTok-ot a válaszadók 14%-a említette problémás tartalmak forrásaként, a Twitter (X)-et pedig 13%-uk. Ez utóbbi arány a platformot használók körében meglehetősen magas, tükrözve a Twitter (X)nyíltabb, kevésbé moderált jellegét és azt, hogy ott gyakran terjed politikai dezinformáció. A kisebb közönségű oldalak közül a Reddit (4%) és a Snapchat (1-2%) kevésbé merültek fel, ami összefügg a csekély hazai felhasználói bázisukkal. Érdekes módon a kevesek által használt VKontakte-ot mind a 3 említő gyanúsnak ítélte, bár ez az adat a kis elemszám miatt csak jelzésértékű.

Mindezek alapján elmondható, hogy a Facebook messze a leginkább érintett platform a felhasználók szerint az információs műveletek terén, amit az is magyaráz, hogy a platform ökoszisztémája kedvez a dezinformáció terjedésének. Dr. Bányász Péter rámutatott, hogy a közösségi média algoritmusvezérelt tartalomterjesztési mechanizmusai visszhangkamrákat és szűrőbuborékokat hoznak létre, amelyek révén a felhasználók főként a saját világnézetükkel egyező tartalmakkal találkoznak. Ez a mechanizmus egyfelől magyarázza, miért érzékelnek sokan a Facebookon rengeteg manipulált információt, másfelől rávilágít a platform jelentette veszélyre: a torzított információs környezet megkönnyíti a sikeres információs műveleteket.

A fenti diagram szemlélteti, hogy a válaszadók hány százaléka jelölte egyes platformokon a legtöbb gyanús tartalom előfordulását. Jól látható, hogy a Facebook esetében kiemelkedően magas az arány, ami alátámasztja a platform központi szerepét a dezinformáció terjesztésében. A YouTube és az Instagram esetében a válaszadók közel ötöde számolt be gyakori gyanús tartalmakról. Dr. Bányász Péter az interjú során kiemelte, hogy a mesterséges intelligencia térnyerése a közösségi médiában tovább súlyosbítja a helyzetet, hiszen könnyebbé teszi valósághű hamis tartalmak (pl. deepfake videók) előállítását. Ugyan a válaszadók kisebb része említette csak a deepfake technológiát expliciten, az interjúk alapján a szakértők konszenzusa, hogy ezek a technikai eszközök az információs műveletek új hullámát jelentik. Mindazonáltal a kérdőív eredményei azt tükrözik, hogy a felhasználók főként a szöveges és hagyományos média tartalmak szintjén érzékelik a manipulációt, ugyanis a legnagyobb arányban választott platform is elsősorban ilyen jellegű tartalmak megosztásáról ismert.

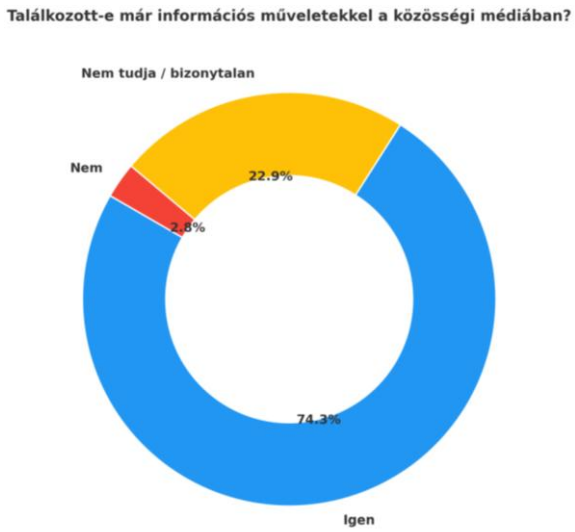
A szakértői interjúban Bányász Péter utalt arra, hogy a közösségi média alkalmas lehet politikai stabilitás aláásására és a közvélemény befolyásolására, akár választások kapcsán. Ezt a kutatás kérdőíves része közvetve igazolja azzal, hogy a felhasználók jelentős része észleli, hogy bizonyos platformokon mintha „töményebben” jelenne meg a manipulatív tartalom, ami jellemzően a politikailag túlfűtött közegekben figyelhető meg.



6. ábra: Hallott már az "információs műveletek" kifejezésről a közösségi médiában?

A kérdőívben rákérdeztem arra, hogy a válaszadók hallották-e már az „információs műveletek” kifejezést a közösségi médiában. A visszajelzések alapján (5. ábra) a kitöltők 62,8%-a válaszolt igennel, további 7,1% pedig bizonytalan volt abban, hogy találkozott-e a kifejezéssel, míg 30% határozottan nemmel felelt. Ez azt mutatja, hogy a fogalom a válaszadók többsége számára nem ismeretlen. Ez abból is fakadhat, hogy a vizsgált téma iránt fogékonyabbak tölthették ki a kérdőívet, illetve az elmúlt évek kapcsán a média is többször használt ilyen kifejezéseket. Ugyanakkor Dr. Bányász Péter rávilágított arra, hogy maga a terminológia sem egységes. Az interjú során megjegyezte, hogy ő nem tartja szerencsésnek az „információs hadviselés” terminust, mert azt inkább orosz és kínai kontextusban használják, míg NATO-oldalon az „információs műveletek” elnevezés terjedt el. Ez a terminológiai distinkció a válaszadók számára kevésbé volt releváns, hiszen a kérdőív magyar nyelven, köznyelvi megfogalmazásban kérdezett rá a jelenségre.

Fontos azonban hozzátenni, hogy a fogalom ismerete nem jelenti feltétlenül a mély megértést. A későbbi válaszokban látni fogjuk, hogy bár sokan érzékelik az információs műveletek jelenlétét, a jelenség árnyaltabb aspektusait nem biztos, hogy mindenki átlátja azok jelentőségét és összefüggéseit.

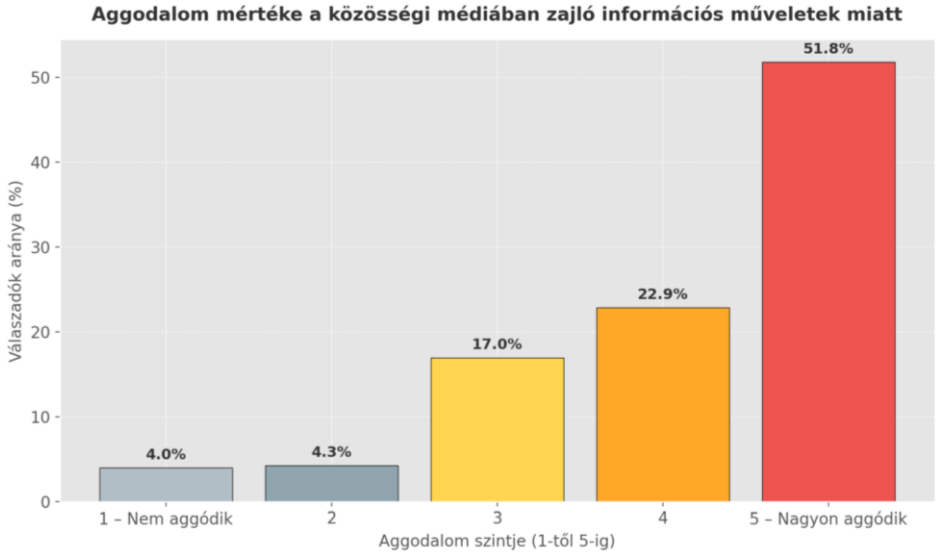


7. ábra: Találkozott-e már információs műveletekkel a közösségi médiában?

Arra a kérdésre, hogy találkozott-e már a közösségi médiában végrehajtott információs műveletekkel (6. ábra), a válaszadók még az előzőnél is magasabb arányban válaszoltak igennel. A kitöltők 74,3%-a úgy gondolja, hogy személyesen is találkozott már ilyen tevékenységgel, további 22,9% bizonytalan ebben, és mindössze 2,8% véli úgy, hogy soha nem találkozott ilyesmivel. Ez a megoszlás egyértelművé teszi, hogy a vizsgált minta nagy többsége érzékeli az információs műveletek jelenlétét a digitális terekben. Ezek az arányok akár aggasztóbbnak is tűnhetnek, mint a puszta fogalomismertség, ugyanis sokan azok közül is észleltek gyanús befolyásolási kísérleteket, akik amúgy a terminust nem is feltétlen tudnák pontosan meghatározni. Az észlelés magas aránya valószínűleg összefügg a mindennapi tapasztalatokkal is hiszen a felhasználók találkozhatnak nyilvánvaló propaganda-posztokkal, fake news cikkekkel, gyanús profilok aktivitásával stb. Dr. Bányász Péter is megerősítik, hogy ezek valóban létező jelenségek. Hangsúlyozta, hogy a közösségi média mára az információs műveletek egyik legmeghatározóbb eszközévé vált, mivel gyorsan és hatékonyan lehet rajta keresztül széles tömegeket elérni. Az, hogy a felhasználók háromnegyede személyes tapasztalattal bír ilyen befolyásolási kísérletekről, azt jelenti, hogy a probléma korántsem elméleti, mindinkább széles körben átélt valóság.

Ugyanakkor felmerül a kérdés, hogy pontosan mit tekintenek a válaszadók információs műveletnek? Lehetnek eltérések abban, ki mit azonosít be így? Például egyesek a nyilvánvaló politikai propagandát, mások a konteókat, megint mások a reklám jellegű megtévesztéseket is idesorolhatták. Az információs műveletek definíciója tág. Dr. Haig Zsolt szerint minden olyan tevékenység ide sorolható, amely a közvéleményt

befolyásolja és alakítja, különösen a modern hadviselés kontextusában. A NATO új doktrínája is ebbe az irányba mutat, ami szerint az információs fölény megszerzése és a közvélemény manipulálása a cél.



8. ábra: Aggodalom mértéke a közösségi médiában zajló információs műveletek miatt

A kérdőívben erre külön rákérdeztem, amit a 7. ábra mutat. Az adatok szerint a közösségi médiában zajló információs műveletek a felhasználók számára jelentős aggodalomra adnak okot. Egy ötfokú skálán értékeltem, ki mennyire aggódik a jelenség közösségi médiára gyakorolt hatása miatt. A válaszok átlaga 4 körül alakult, és a megoszlás erősen eltolódott a magas értékek felé. A kitöltők több mint fele a maximális 5-ös értéket választotta, további 22,9% pedig 4-est adott. Tehát összességében kb. 74-75% komoly aggodalmat érez a témával kapcsolatban. 17% körüli azok aránya, akik közepes szintű aggodalmat jeleztek, és csak elenyésző kisebbség van a skála alsó felén. Mindössze 4% jelölt 1-est és 4,3% 2-est. Ezek az eredmények világosan mutatják, hogy a közvélemény számára az információs műveletek potenciális veszélyforrásként jelennek meg, amelyek képesek negatív hatást gyakorolni a közösségi médiára és tágabb értelemben a társadalomra. Ezt az általános aggodalmat Bányász Péter is osztja, aki úgy fogalmazott, hogy az információs műveletek hosszú távon akár a demokratikus intézmények működését is destabilizálhatják és nem pusztán az ellenfél félretájékoztatásáról van szó. Külön kiemelte a COVID-19 világjárvány alatt terjedő álhírek példáját, amelyek révén a félelem- és pánikkeltés csökkentette a közegészségügyi intézkedések elfogadottságát, ezzel is aláásva a társadalmi bizalmat. Ez alátámasztja, hogy az információs műveleteknek kézzelfogható következményei lehetnek a

valóságban. A válaszadók szubjektív aggodalma tehát nem alaptalan és a modern történelmi példák mind arra utalnak, hogy ezek a jelenségek komoly hatással lehetnek közösségekre és nemzetekre.

A kérdőív kitért arra, hogy a válaszadók szerint mi lehet egy információs művelet célja. Erre a kérdésre több válaszlehetőséget is megadhattak, a leggyakoribb elképzeléseket listázva. Az eredmények alapján a közvélemény széleskörűen érzékeli az információs műveletek multidimenzionális célrendszerét. A legtöbben egyetértettek abban, hogy az információs műveletek egyik fő célja a közvélemény manipulálása. Szintén kiemelkedően sokan említették a politikai narratívák vagy ideológiák terjesztését, valamint nagyon magas arányú válasz volt a társadalmi feszültségek generálása is. Mindez arra utal, hogy a válaszadók többsége tisztában van azzal, hogy az információs hadviselés révén gyakran a társadalom megosztása, polarizálása a cél, illetve bizonyos politikai üzenetek sulykolása a közönség felé. Bányász Péter részletesen beszélt arról, hogy az információs műveletek tipikus megnyilvánulásai közé tartoznak a dezinformációs kampányok és a propaganda, narratívaépítés, amelyek hosszú távon formálják a közvéleményt. Emellett utalt arra is, hogy autoriter rezsimek a közösségi médiát saját geopolitikai céljaik elérésére használják, ami arra utal, hogy a narratívaépítés és propaganda mögött állami szándékok húzódhatnak. A közvéleményben is megjelenik az a felismerés, hogy az információs műveleteknek geopolitikai vagy hatalmi céljai is lehetnek. A válaszadók 81% gondolta, hogy a választások befolyásolása konkrét cél lehet.

Valamivel kevesebben, de még mindig a válaszadók több mint fele említette a gazdasági haszonszerzést mint lehetséges célt. Ez utóbbi érdekesen tágítja a kört, ugyanis nem csupán politikai vagy katonai indíttatású befolyásolásra gondolnak a kitöltők, hanem felismerik, hogy adott esetben anyagi érdekből, profitszerzés miatt is futhatnak manipulációs kampányok. Tovább árnyalja a képet, hogy a válaszadók jelentős része (43%) szerint diplomáciai érdekérvényesítés is állhat információs műveletek mögött, valamint hasonló arányban (44%) jelölték a katonai megtévesztést is a célok között. Ez azt mutatja, hogy a társadalom egy része tudatában van, hogy az információs hadviselés nem csak a polgári lakosság ellen irányulhat, hanem a katonai műveletek támogatására, kiegészítésére is szolgálhat.

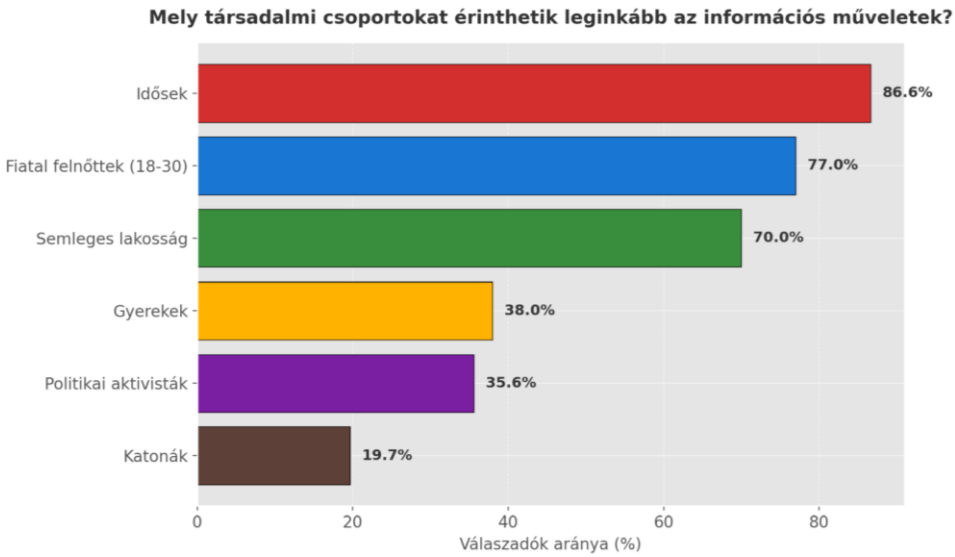
Dr. Haig Zsolt értelmezése kifejezetten felhívta a figyelmet arra, hogy az információs műveleteknek létezik egy kognitív és egy technikai/technológiai vetülete. A

NATO jelenlegi doktrínája túlnyomórészt a kognitív befolyásolásra koncentrál, vagyis arra, hogyan lehet megnyerni vagy manipulálni a közvéleményt. Ezzel önmagában nincs probléma, hiszen ez valóban az információs műveletek egyik valid célja. Ugyanakkor Haig kiemeli, hogy a 2023-ban kiéleződött orosz–ukrán háború rámutatott a technikai információs műveletek fontosságára is.

A harctéri körülmények között olyan tevékenységek zajlanak, mint ellenséges kommunikáció zavarása, hekkertámadások, sőt akár információs célpontok megsemmisítése. Ezek mind valódi információs műveleti tevékenységek, csak épp a technikai képességek körébe tartoznak. Haig Zsolt úgy látja, hogy a békés időszakban kidolgozott doktrínák hajlamosak elfeledkezni a technikai komponensről, pedig az háborús helyzetben kulcsfontosságú.

Érdekes módon a kérdőív válaszai között is megjelent a technikai aspektus fontossága. Bár nem kifejezetten kérdeztem rá, a katonai megtévesztés céljának sok válaszadó általi felismerése azt sugallja, hogy a lakosság egy része érti, a hadviselés részeként is alkalmaznak információs trükköket. Ugyanakkor valószínű, hogy a nyilvánosság elsősorban mégis a politikai és társadalmi vetületre fókuszál, hiszen a legmagasabb arányban említett célok ezekhez kötődtek.

Bányász Péter kiemelte, hogy az információs műveletek eszköztárát egyaránt használják állami és nem állami szereplők stratégiai céljaik elérése érdekében, legyen szó lélektani műveletekről, social engineering alapú kibertámadásokról vagy a társadalmi kohézió megbontásáról. A társadalmi kohézió megbontása jellemzően azt implikálja, hogy a műveletek célcsoportja a széles lakosság vagy annak bizonyos szegmensei, akiket egymás ellen lehet hangolni, vagy akiknek a bizalmát egymás iránt alá lehet ásni.



9. ábra: Mely társadalmi csoportokat érintik leginkább az információs műveletek?

A kérdőív egy külön kérdésben vizsgálta is a percepciót arról, hogy kik a célpontjai a közösségi médiában zajló információs műveleteknek (8. ábra). A válaszadók itt is több lehetőséget megjelölhettek, és az eredmények azt mutatják, hogy a közvélemény érzékeli, hogy bizonyos csoportok sebezhetőbbek vagy célzottabbak lehetnek. A legtöbben (86,6%) az időseket jelölték meg, mint célcsoportot. Ez egybevág az általános narratívával, miszerint az idősebb generáció könnyebben válnak álhírek és manipulációk áldozatává. Ugyanakkor szorosan mögötte van a fiatal felnőttek kategória (77%), ami arra utal, hogy a válaszadók szerint a 18-30 éves korosztály is kiemelt célpont lehet. Ennek több oka is lehet. Egyrészt a fiatalok töltik a legtöbb időt a közösségi médián, másrészt a fiatal felnőttek politikai szocializációja folyamatban van, nézeteik formálhatók, harmadrészt ők szavazóképes fiatalok vagy új szavazók, akiket például választások előtt érdemes befolyásolni.

A harmadik leggyakrabban említett célcsoport a „semleges lakosság” (70%). Ezt a kategória az olyan széles tömegeket takarja, akik nincsenek egyik politikai tábor vagy ideológia mellett elköteleződve, tehát befolyásolhatók. Dr. Haig Zsolt szavai visszaköszönnek itt, ugyanis a jelenlegi háborús felek egyike sem nagyon tudja meggyőzni a másikat, ezért elsősorban a semleges érintettekre van kihegyezve a befolyásolás, ahol a támogatás megnyerése a fő cél. Vagyis a semleges lakosság, a bizonytalanok meggyőzése tipikus célpontja az információs kampányoknak, legyen az belföldi vagy nemzetközi.

Illetve a válaszadók egy része más csoportokat is megjelölt. Meglepően sokan gondolták úgy, hogy a gyerekek is célpontok (38%). Ez azért érdekes, mert a gyerekek (14-18 év alattiak) többsége még nincs kitéve politikai célú manipulációnak, ugyanakkor a közösségi médiát már ők is használják. Az eredmény mutathatja azt a szülői aggodalmat vagy köztudatban levő félelmet, hogy a fiatalok védtelenek a közösségi médiában rájuk leselkedő manipulációkkal szemben. Ugyan a szakértői interjúk nem tértek ki külön a kiskorúakra mint célcsoportra, a médiaértés oktatásának fontosságát többen hangsúlyozták (lásd később), ami közvetve utal arra, hogy már fiatal korban fel kell vértezni a gyerekeket a kritikus gondolkodás képességével.

A politikai aktivistákat a válaszadók 35,6%-a említette célpontként. Ez arra utal, hogy a közvélemény egy része tisztában van vele, hogy a dezinformációs kampányok célja olykor a politikailag aktív rétegek befolyásolása, mozgósítása vagy megtévesztése. Példaként említhető egy ellenzéki mozgalom lejáratása hamis információkkal, vagy éppen fordítva, egy radikális csoport szándékos félretájékoztatása, hogy provokálják őket valamilyen lépésre.

Végül, viszonylag kevesen (19,7%) jelölték meg, hogy a katonák is célpontok lennének. Ez utóbbi érték külön figyelmet érdemel, mert itt tetten érhető egy perspektívabeli különbség a lakosság és a szakértők között. Míg a válaszadók zöme nyilvánvalóan civil szemszögből közelít és a polgári lakosságot látja veszélyeztetve, addig a szakértők között (különösen Kovács László személyében) megjelenik a tudatosság, hogy a katonai szervezetek és személyek is ki vannak téve információs fenyegetéseknek. Kovács László szerint a közösségi média katonai célú használata komoly kibervédelmi kockázatokat rejt. Például a katonák által megosztott érzékeny információkat fedhetnek fel, vagy lehetőséget adhatnak az ellenségnek a kapcsolati hálójuk feltérképezésére. Ugyanebben az interjúban rámutatott, hogy a katonai szervezetek esetében a műveleti biztonságot ki kell terjeszteni a közösségi média használatára is, mivel a figyelmetlen posztolás felderítési és kémkedési támadásokhoz vezethet. Ez a nézőpont a civil lakosság körében talán kevésbé ismert vagy tudatos, ahogy a fenti számok is mutatják. A kutatás egyik tanulsága, hogy az információs műveletek elleni védekezés nem csak a civilekre, hanem a fegyveres erők tagjaira is külön stratégiákat kíván.

Összességében a célok és célcsoportok percepciójáról elmondható, hogy a kérdőíves eredmények és a szakértői meglátások jelentős átfedést mutatnak a politikai-társadalmi dimenzióban. Mindkét forrás megerősíti, hogy az információs műveletek célja a közvélemény manipulálása, a társadalom befolyásolása, gyakran megosztó, destabilizáló szándékkal. A lakosság is érzékeli a jelenség komplexitását, de a hangsúly az észlelés szintjén a társadalmi befolyásra esik.

A szakértők pedig hozzáteszik, hogy a technikai eszközök ugyancsak részét képezik a modern információs hadviselésnek, még ha ezt a közvélemény kevésbé is látja. Bányász Péter szavaival élve, a közösségi média infrastruktúráját és algoritmusait egyes állami vagy nem állami aktorok saját geopolitikai céljaik elérésére használják, ami pontosan tükrözi a válaszadók által is sejtett célt (pl. választások befolyásolása, ideológiai terjesztés). Dr. Haig Zsolt ugyanakkor arra figyelmeztet, hogy ne feledkezzünk meg arról, hogy a hadviselésben a hardver és szoftver oldal, tehát a tényleges kiberhadviselés, informatikai támadások, elektronikai zavarás is ide tartozik, különösen nyílt konfliktus esetén. A lakossági válaszok alapján a polgári szférában még nem egyértelmű ennek a jelentősége, hiszen a legtöbben a dezinformációra asszociálnak információs művelet hallatán, nem pedig mondjuk egy hacker-támadásra.

A kérdőív feltárta, hogy az emberek mennyire érzik magukat felkészültnek a manipulált tartalmak felismerésére, és mit tesznek, ha ilyenekkel találkoznak. Ezek a kérdések a társadalom ellenálló képességét (rezilienciáját) hivatottak felmérni, ami kulcsfontosságú az információs műveletek sikeressége szempontjából. Az egyik kérdés megfogalmazása így hangzott: „Mennyire biztos abban, hogy képes azonosítani és megkülönböztetni a valódi és a manipulált tartalmat a közösségi médiában?” (1-től 5-ig skála, ahol az 5 jelentette azt, hogy teljes mértékben biztos a dolgában). Az eredmények szerint a válaszadók önbizalma közepes mértékű, enyhén pozitív irányba hajlik. A legtöbben a 4-es értéket választották (46,2%), ami azt jelzi, hogy majdnem a válaszadók fele inkább biztos a saját képességeiben, de nem teljesen. A második leggyakoribb válasz a 3-as volt (32,8%), ami a közepes magabiztosságot jelenti. Ötöst, tehát teljes magabiztosságot kevesen (10,7%) jelöltek, és hasonlóan kevesen voltak az önmagukban nem bízók: 1-est csak 4 fő (1,6%) adott, 2-est pedig 22 fő (8,7%).

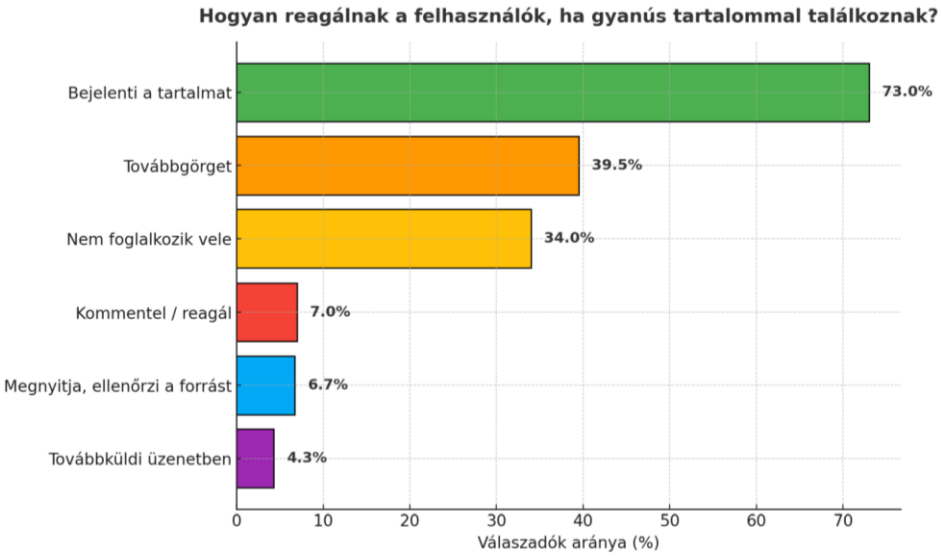
Ezek a számok arra utalnak, hogy a többség úgy érzi, van némi fogalma arról, hogyan lehet kiszűrni a manipulált tartalmakat, de csak egy kisebbség érzi magát

tévedhetetlennek ebben. Hasonló kérdés vonatkozott kifejezetten az álhírek (fake news) felismerésére: „Mennyire biztos abban, hogy képes azonosítani az álhíreket?” – itt az eredmények nagyon közel álltak az előző kérdéshez. Ismét a 4-es volt a leggyakoribb válasz (51,8%), 3-ast 63 fő (24,9%) adott, 5-öst 43 fő (17%). Az 1-es és 2-es együtt itt is alig haladta meg a 6-7%-ot. Látható tehát egy kis különbség: az álhírek kapcsán némileg többen jelöltek nagy magabiztosságot (5-öst), mint a manipulált tartalmak általában vett felismerésénél. Ennek oka lehet, hogy az álhír fogalma talán ismerősebb és konkrétabb az átlagember számára, míg a manipulált tartalom tágabb, így abban picit bizonytalanabbak.

Összességében azonban mindkét skálán az az eredmény látszik, hogy a közönség mérsékelten magabiztos, de nem elbizakodott a képességeit illetően. Felmerül a kérdés, hogy mennyire felel meg a valóságban a felhasználók valós képessége az önértékelésüknek? Ennek ellenőrzésére beépítettem a kérdőívbe egy apró „tesztkérdést”. Három állítást soroltam fel, és arra kértem a válaszadókat, jelöljék meg, melyik tűnik hamisnak vagy manipuláltnak. A három állítás a következő volt: (A) „A NATO 2024-ben bejelentette, hogy mesterséges intelligencia segítségével fogja közvetlenül manipulálni a tagállamok lakosságának politikai nézeteit a választások előtt.”; (B) „A mesterséges intelligenciával generált képek és videók (deepfake) már most megbízhatóan felismerhetők a legtöbb közösségi média algoritmusa által, így a felhasználóknak nem kell aggódniuk a manipulált tartalmak miatt.”; (C) „Az információs műveletek célja lehet a társadalmi megosztottság növelése, különösen választások vagy nemzetközi konfliktusok idején.”. A három közül két állítás nyilvánvalóan hamis vagy félrevezető (A és B), míg a harmadik (C) igaz. Ezzel a kérdéssel azt kívántam felmérni, hogy a válaszadók meg tudják-e különböztetni a valószerűtlen, hamis állításokat a hihető, igaz állítástól.

Az eredmények meglehetősen pozitív képet mutatnak. A válaszadók jelentős része sikeresen kiszűrte a hamis állításokat. Konkrétan 124 fő (49%) mindkét hamis állítást megjelölte és a valódit nem jelölte, vagyis teljesen helyesen válaszolt. További 94 fő (37%) legalább az egyik hamis állítást felismerte, így őket tekinthetjük részben sikeresnek. 35 fő (14%) jelölt meg olyan állítást is, ami valójában igaz (vagy nem jelölt meg hamisat), tehát ők tekinthetők tévesen válaszolónak. Fontos, hogy senki sem hagyta teljesen üresen ezt a kérdést, mindenki próbált választ adni. Összesítve elmondhatjuk, hogy a válaszadók 86%-a legalább részben tudta, mit kell hamisnak tartani, és majdnem

a fele teljes bizonyossággal azonosította mindkét hamis állítást. Ez azt sugallja, hogy a minta tagjai között viszonylag magas az általános média-műveltség vagy tudatosság ezen a téren.



10. ábra: Hogyan reagálnak a felhasználók, ha gyanús tartalommal találkoznak?

Annak vizsgálatára is kitértem, hogy a felhasználók milyen konkrét lépéseket tesznek, ha gyanús tartalommal találkoznak (9. ábra). Több lehetőség közül választhattak, akár többet is egyszerre, hiszen valós helyzetben is többféle reakció keveredhet. A leggyakoribb reakció a válaszok alapján 73%-a a válaszadóknak mondta, hogy bejelenti a gyanús tartalmat. Ez biztató jel abból a szempontból, hogy a felhasználók többsége aktívan fellép az észlelt dezinformáció ellen, legalább a platform felé jelzi. Ugyanakkor azt is látni kell, hogy a jelentés önmagában csak akkor ér valamit, ha a platform üzemeltetői lépnek.

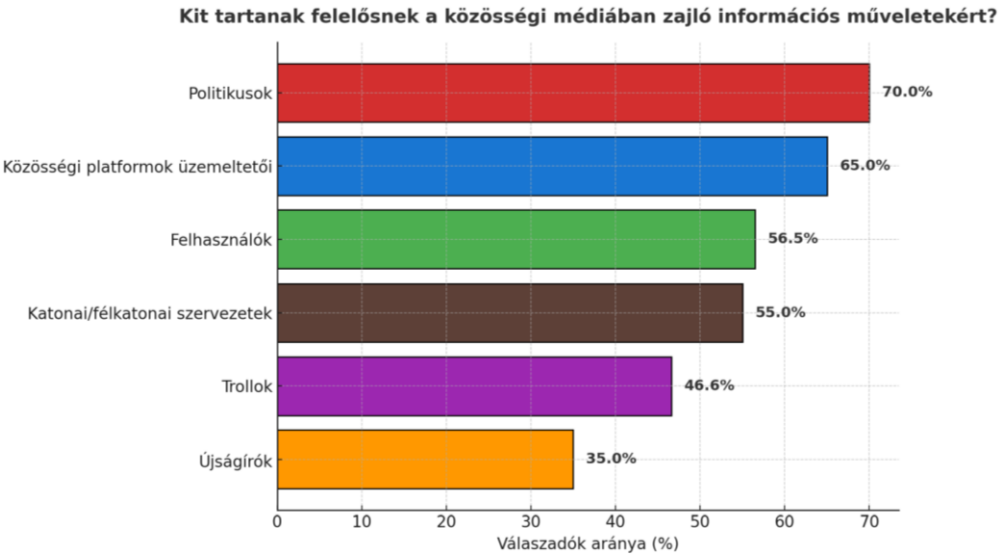
A második leggyakoribb reakció a „továbbgörgetés” volt. 39,5% válaszolta, hogy egyszerűen tovább görget és nem foglalkozik a tartalommal. Ehhez szorosan kapcsolódik egy másik opció, a „nem foglalkozik vele”, amit a válaszadók 34%-a jelölt be. Látható tehát, hogy jelentős arányban vannak, akik passzívan kerülik a problémás tartalmakat. Bár nem hisznek nekik, de nem is tesznek ellenük semmit, csak ignorálják. Ez emberileg érthető reakció, azonban társadalmi szinten aggasztó is lehet, mert ha a felhasználók nagy része csak elsiklik a dezinformáció felett anélkül, hogy azt jelezné vagy korrigálná, akkor a fals információ zavartalanul terjedhet tovább olyanokhoz, akik viszont elhiszik azokat. Mindössze kevesen mernek konfrontálódni, ugyanis kommentben reagálni a gyanús tartalomra csupán 7% szokott, ami arra utal, hogy kevesen állnak le nyilvánosan

vitatkozni egy esetleges trollal vagy propaganda-poszttal. Ez nem meglepő, hiszen egyre köztudottabb, hogy az online viták gyakran meddők, sőt kontraproduktívak lehetnek, és sokan tartanak attól, hogy saját magukat támadás érheti, ha megpróbálnak ellentmondani egy álhír terjesztőjének.

Kevéssé gyakori reakció (6,7%) a forrás megnyitása, ellenőrzése. Pedig a médiaértés klasszikus tanácsa lenne, hogy ellenőrizzük a gyanús hír forrását. A relatíve alacsony arány azt mutatja, hogy a felhasználók többsége vagy nem ér rá, nem veszi a fáradságot erre, vagy eleve annyira nyilvánvaló butaságnak ítéli a tartalmat, hogy nem tartja szükségesnek a részleteket megnézni. Végül 4,3% válaszolta azt, hogy üzenetben továbbküldi barátainak a gyanús tartalmat. Ez utóbbit értelmezhetjük úgy, hogy privát csatornán megosztja, valószínűleg hozzáfűzve a saját véleményét. Ez azért érdekes, mert mutatja, hogy akár jó szándékkal is hozzájárulhatunk a manipulált információ terjedéséhez, ha privát körben továbbítjuk, még ha kritikus megjegyzéssel is.

A felmérés rámutatott, hogy viszonylag kevés felhasználó néz utána a dolgoknak, ami alátámasztja azt az igényt, hogy oktatással, tudatosságnöveléssel javítani kellene ezen a téren. Bányász Péter interjúnk során kiemelte, hogy minél tudatosabbak a polgárok, annál kevésbé válnak áldozattá, és ezt már iskolai szinten el kellene kezdeni.

Később részletesen kifejtette, hogy a médiaműveltségnek, kritikai gondolkodásnak alapvető készségekké kell válniuk minden digitális térben mozgónak. Ezek a szakértői javaslatok teljes összhangban vannak a kérdőív következő eredményrészével, melyben azt vizsgáltuk, hogy a válaszadók hogyan viszonyulnak az oktatáshoz és tudatosságnöveléshez mint lehetséges megoldáshoz.



11. ábra: Kit tartanak felelősnek a közösségi médiában zajló információs műveletekért?

A kérdőív utolsó szakaszában rákérdeztem néhány lehetséges intézkedésre és felelősségi körre az információs műveletek ellenében (10. ábra). Először is arra voltam kíváncsi, hogy a válaszadók kit vagy kiket tartanak felelősnek a közösségi médiában terjedő információs műveletekért. Mivel ezek összetett jelenségek, több opciót is felajánlottam és a résztvevők több választ is megjelölhettek. Az eredmények rávilágítanak arra, hogy a közvélemény szerint a felelősség megoszlik különböző szereplők között, de nem azonos mértékben. A legtöbben, a válaszadók 70%-a úgy vélte, hogy a politikusok felelősek az ilyen manipulációkért. Ez nem feltétlenül meglepő, hiszen a politikai dezinformáció mögött gyakran konkrét hatalmi érdekek húzódnak és a választók is hajlamosak a politikát okolni a társadalmi feszültségekért vagy megtévesztésekért.

Ezt követi a közösségi platformok üzemeltetőinek felelőssége a válaszadók 65% szerint. Az utóbbi években világszerte előtérbe került a Facebook, X és más techóriások felelősségének kérdése, miszerint mennyire asszisztálnak vagy éppen lépnek fel az álhírek terjedése ellen. A felhasználók jelentős része tehát a platformokat is felelősnek tartja, hiszen ők biztosítják a terepet és algoritmusokat, amelyek a tartalmakat terítik. Dr. Bányász Péter utalt is arra, hogy a platformok algoritmusainak átláthatatlansága gond, és a szabályozóknak, platformoknak szorosabban együtt kellene működniük a hatékonyabb tartalomszűrés és az algoritmusok transzparenciája érdekében.

A harmadik helyen a felhasználókat magukat jelölték meg, mintegy 56,5%. Ez jelentheti azt, hogy a válaszadók szerint az emberek saját maguk is hibásak, amikor

kritikátlanul továbbosztanak manipulatív tartalmakat, vagy épp ők maguk generálják azokat. Valóban, az információs műveletek terjedéséhez sokszor felelőtlen felhasználók kellenek, akik megosztják a szenzációsnak tűnő híreket. Így a felelősség részben a társadalmon is van, amit a válaszadók többsége érez, bár érdekes módon kevesebben hibáztatják a felhasználókat, mint a politikusokat vagy platformokat.

Ez arra utal, hogy némileg külsőbb szereplőket látnak fő bűnösnek, de saját szerepüket is belátják. A „trollok" a megkérdezettek 46,6%-a szerint felelősek. Ez a kategória némiképp átfedhet a politikusokkal vagy állami aktorokkal, de lényegében a dezinformációs ökoszisztéma tagjait jelenti, akiket sokan hibáztatnak. Szintén jelentős azok aránya, akik a katonai vagy félkatonai szervezeteket (55%) tartják felelősnek. Ide sorolhatjuk például az idegen hatalmak hírszerzését, kiberháborús egységeit. Az utóbbi években a NATO és EU is többször vádolt meg orosz katonai hírszerzési csoportokat kibertámadásokkal és dezinformációs műveletekkel, így a köztudatba bekerült, hogy bizony a hadseregeknek is vannak ilyen kapacitásaik. Dr. Bányász is utalt rá, hogy állami szereplők is használják a közösségi médiát stratégiai, akár offenzív célokra.

Ami a legalacsonyabb arányt illeti, az újságírók kerültek ide, akiket 35% jelölt meg. Ez is egy fontos üzenet, mert bár az újságírók elvben a hiteles tájékoztatás letéteményesei, a gyakorlatban a média szereplői is keveredhetnek dezinformációs botrányokba, illetve egy részük a dezinformáció gyártásában is részt vesz. A válaszadók egyharmada tehát az újságírói felelősséget is felveti, bár ezt kevesebben tartják fő problémának, mint a politikai vagy online tényezőket.

Ez egybecseng azzal a narratívával, hogy a média megosztott. Vannak hiteles, tényalapú orgánumok és vannak szenzációhajhász vagy politikailag motiváltak, és a közönség nagy része talán bízik abban, hogy az újságírói etika szabályai szerint a többség nem szándékosan félrevezető. Ugyanakkor a harmaduk látja, hogy a médiának is lehet szerepe a torzításban. A felelősség megítélését követően rákérdeztünk arra is, hogy a válaszadók szerint a közösségi média cégeknek vállalniuk kellene-e nagyobb felelősséget az információs műveletek megelőzésében és kezelésében. Itt nagyon egyértelmű eredmény született, ugyanis a válaszadók 90,1% igennel válaszolt. Ez a majdnem egyhangú eredmény erős társadalmi elvárást jelez a platformok felé. A közösség úgy érzi, a Facebook, YouTube, X stb. többet kellene tegyen az álhírek, propagandák ellen. Bányász Péter kifejtette, hogy a közösségi média vállalatoknak felelősséget kell

vállalniuk a tartalommoderációs eljárások fejlesztéséért, transzparens jelentési rendszereket kell kidolgozniuk, és együtt kell működniük független kutatókkal, szabályozókkal. Ugyanakkor figyelmeztetett, hogy nagy kihívás megtalálni az egyensúlyt a platformok szabályozása és az információs szabadság fenntartása között. Tehát miközben a társadalom nyomást helyez a platformokra, fontos, hogy a megoldások ne csorbítsák a szólásszabadságot. Ez egy nehéz, de szükséges kompromisszumkeresés.

A kérdőív eredménye mindenesetre azt mutatja, hogy a felhasználók nagy része a jelenleginél erélyesebb platform-beavatkozást tart szükségesnek. Ezt a vélekedést a szakértői interjúkban Bányász mellett Haig Zsolt is alátámasztja egy konkrét példán keresztül. Haig említette, hogy a mesterséges intelligenciának már volnának olyan lehetőségei, melyek segíthetnék a manipulatív tartalmak szűrését, csakhogy a közösségi média platformok számára ez jelenleg kontraproduktív lenne, mivel ütközik az üzleti érdekeikkel. Vagyis a platformok eddig azért nem léptek fel kellőképpen, mert a virális tartalmak növelik az aktivitást és profitot. Ez alátámasztja a közönség érzését, miszerint a techcégek nem viselik a felelősségüket és változtatniuk kellene ezen a gyakorlaton.

Hasonló kérdés merült fel a kormányok szerepével kapcsolatban: vajon a kormányoknak szerepet kell-e vállalniuk a közösségi média platformokon folyó információs műveletek szabályozásában? Itt a közvélemény megosztottabb. A többség (58,1%) igennel felelt, de jóval kisebb arányban, mint a cégek felelősségénél. 56 fő (22,1%) azt mondta, hogy „talán”, míg 50 fő (19,8%) szerint nem kellene kormányzati szerepvállalás. Ez azt tükrözi, hogy bár sokan elvárnák a kormányok fellépését, mégsem olyan elsöprő a támogatottsága, mint a vállalati felelősségnek. Ennek oka lehet a bizalmatlanság vagy óvatosság. A polgárok bizonyára érzik, hogy ha a kormány túlzottan beleszól a tartalmak szabályozásába, az könnyen cenzúrához vezethet vagy politikai célú visszaélésekhez.

Bányász Péter ugyanakkor hangsúlyozta, hogy a platformok szabályozása és szakpolitikai együttműködés is szükséges része az információs hadviselés elleni küzdelemnek. Ő utalt az Európai Unió új szabályozási keretére, a DSA, amely fokozott kötelezettségeket ró a nagy platformokra. Ugyanakkor Bányász is megjegyezte, hogy a szabályozás mindig le van maradva a technológiai fejlemények mögött, tehát önmagában a kormányzati fellépés sem csodaszer.

Fontos tehát az egyensúly és a többpilléres megoldás, tehát a technológiai eszközök fejlesztése, platformfelelősség, szabályozás és a társadalom edukációja együtt. A kérdőív eredményei alapján a társadalom is valami ilyesmit szeretne: nem utasítja el a kormányzati szerepvállalást, de számottevő a bizonytalanság és ellenérzés is, ami óvatosságra inti a döntéshozókat. Vélhetően sokan úgy gondolják, hogy a kormány segítsen, de ne korlátozza túlzottan a netes szólást, tehát egyensúlyt várnak.

A felhasználók javaslatai és igényei is megjelentek a kérdőívben, részben zárt kérdések, részben nyílt kérdések formájában. Külön rákérdeztem, hogy segíthetnek-e az oktatási és figyelemfelkeltő kampányok abban, hogy a felhasználók jobban azonosítsák és reagáljanak az információs műveletekre. Erre 73,1% válaszolt igennel, 21% talánnal, és 5,9% nemmel. Tehát egy nagyon erős többség hisz az edukáció és awareness erejében. Ez teljes összhangban áll mind a szakirodalommal, mind a szakértői interjúkkal, tehát a médiatudatosság növelése a védekezés egyik alappillére.

Ezen belül is konkrétan rákérdeztem arra a felvetésre, hogy az iskolai oktatás részévé kellene-e tenni a felelős internet használatot, beleértve az információs műveletekről szóló ismereteket. Itt a válaszadók szinte egyöntetűek: 91,3% igennel felelt, alig 3,6% mondott nemet, és 5,1% talán-t. Ez az eredmény azt sugallja, hogy a társadalom felismeri, hogy a fiatal generációkat már az iskolában fel kell készíteni az online tér kihívásaira. A magyar köznevelésben jelenleg is vannak törekvések digitális írástudás fejlesztésére, de a válaszadók nyilván ennél nagyobb hangsúlyt látnának indokoltnak. Néhány válaszadó a nyílt kérdésekben konkrétan megemlítette például, hogy a kerettantervet 21. századivá kellene átalakítani, már gyerekkortól tudatosítani az információs műveletek veszélyeit, sőt volt, aki példaként említette a jelenlegi „KiberPajzs” program kibővítését vagy hasonló kezdeményezést, ami kifejezetten az álhírekre és társaikra fókuszálna. Ez egybecseng Dr. Bányász javaslatával, aki szerint az oktatásnak nagyobb hangsúlyt kell fektetnie az információs műveletek felismerésére és kezelésére, és a médiaműveltségnek alapvető készségnek kell lennie.

A felnőtt lakosság is érdeklődik a téma iránt. Megkérdeztük a kitöltőktől, hogy szeretnének-e többet megtudni arról, hogyan ismerhetik fel a manipulált információkat a közösségi médiában? A válaszadók 45%-a határozott igennel felelt, további 38% szintén igennel, de azzal a kitétellel, hogy csak akkor, ha rövid és közérthető anyagról van szó. 7,5% mondta azt, hogy nem szeretne többet, mert „már jól felismerik”, 4,7% válaszolt

nemmel, és 4,3% talánnal. Tehát a passzív vagy érdektelen réteg itt nagyon kicsi, mindössze <10%. Ez megint csak arra utal, hogy az emberek többsége tisztában van vele, hogy még nem tud eleget, és hajlandó is tanulni, ha megfelelő formában kapja az információkat.

Haig Zsolt például elmondta, hogy a közösségi média előtti korban a katonák számára tiltott volt ellenséges röplapokat olvasni, nehogy azok demoralizálják őket. Ma ugyanígy tilalmakkal nem sokra mennénk, inkább a tudatosságot kell növelni (esetükben is). Bányász és Kovács is a képzés, oktatás fontosságát hangsúlyozta. Kovács a katonai szervezeteknél a folyamatos gyakorlati képzést említette, mint ami elengedhetetlen a kibertérből jövő fenyegetések ellen. A civilek esetében ugyanez a logika. Minél többet tud valaki arról, hogy milyen trükkökkel próbálhatják manipulálni, annál kevésbé lesz kiszolgáltatott. A kérdőív válaszai alapján a lakosság erre nyitott és igényli is. Ez jó alapot teremt bármilyen jövőbeli figyelemfelhívó kampányhoz vagy oktatási programhoz, hiszen nagy az érdeklődés.

A kérdőív végén két nyílt kérdés szerepelt, amelyek minőségi szempontból gazdagítják az eredményeket. Az egyik arra kérte a résztvevőket, hogy írjanak le egy példát, amikor manipulált információval találkoztak a közösségi médiában. Erre a 253 válaszadóból 118-an (46,6%) adtak valamilyen példát. A válaszok elemzése betekintést nyújt abba, hogy a felhasználók milyen konkrét eseteket tartanak említésre méltónak, mi ragadta meg őket leginkább. A példák sokszínűek, de néhány gyakori téma észrevehető.

Többen említettek a világjárvánnyal kapcsolatos manipulált információkat. Például hamis hírek a vakcinák veszélyességéről vagy chipet tartalmazásáról, összeesküvés-elméletek a vírus eredetéről, csodaszerek és áltudományos „gyógymódok” reklámozása. Ez egybecseng Bányász Péter említett példájával is, miszerint az álhírek csökkentették a közegészségügyi intézkedések elfogadottságát.

Számos válaszban felbukkant az „orosz” és „ukrán” szó, ami arra utal, hogy a háború kapcsán a közösségi médiában terjedő propagandát sokan megtapasztalták. Volt, aki orosz forrásból származó háborús álhíreket említett, más a nyugati vagy ukrán oldal propagandaelemeire utalt. Haig Zsolt felhívta a figyelmet arra, hogy 2023 februárja óta intenzív információs műveleti kampányok zajlanak az orosz-ukrán háborúban minden téren, és a válaszok tanúsága szerint a magyar közönség is találkozik ezek visszhangjával.

Több válasz érintette a magyar belpolitikai vonatkozású megtévesztéseket. Visszatérő elem volt például a „Megafon” szó, amely a kormánypárti média-influenszer központot jelöli. Sokan valószínűleg olvastak vagy láttak ezzel kapcsolatban tartalmat, és megemlítették, hogy a Megafonhoz köthető oldalak torzítják a valóságot, propagandaanyagot terjesztenek. Volt, aki azt hozta fel példaként, hogy egy ellenzéki politikusról vagy eseményről szóló hír erősen manipulált narratívával jelent meg a közösségi médiában.

Néhány válaszban általánosabb összeesküvés-elméletek tűntek fel, mint például a laposföld-elmélet posztok. Ezek is jelen vannak a magyar közösségi médiában, és noha a többség talán marginálisnak tartja őket, néhányan megjegyezték, hogy ilyenekkel is találkoztak. Az ilyen típusú dezinformáció fő veszélye a szélsőséges gondolkodás és paranoia terjesztése, ami végső soron a demokratikus intézményekkel szembeni bizalomromboláshoz járulhat hozzá.

Több válaszadó említette a technológiai megoldások fontosságát, például mesterséges intelligencia alapú szűrők beépítését a közösségi oldalakba, vagy automatikus, robotizált előszűrést a közzététel előtt. Ezek a javaslatok arra utalnak, hogy a felhasználók elvárják, hogy a modern technológia, ami részben a probléma, váljon a megoldás részévé is. Ezt erősíti meg Bányász Péter megjegyzése, miszerint a mesterséges intelligencián alapuló eszközök fejlesztése nélkülözhetetlen a jövőben. Ugyanakkor tudjuk, hogy teljes mértékben a technikára bízni a szűrést veszélyes is lehet, de a válaszadók sokasága mégis ezt tartaná hatékonynak, nyilván mert emberi erővel nem lehet mindent ellenőrizni.

A fenti összegzésből látszik, hogy a kérdőív és az interjúk eredményei egymást erősítik és a kvantitatív adatok alátámasztják a szakértők által elmondottakat, illetve a szakértői insightok segítenek értelmezni a kérdőívben kirajzolódó trendeket.

5.2 Jogszabályi és gyakorlati ajánlások

Az eredmények ismeretében világosan kirajzolódik, hogy a közösségi média és az információs műveletek metszéspontjában számos kockázat jelentkezik, amelyek kezelése összetett feladat. A kérdőíves felmérés rávilágított a felhasználói oldal tapasztalataira és elvárásaira, míg a szakértői interjúk a stratégiai és intézményi szempontokat emelték ki. Ezek alapján az alábbi konkrét ajánlásokat fogalmaztam meg, melyek jogszabályi változtatásokra és gyakorlati intézkedésekre egyaránt kiterjednek. Az ajánlások

címzettjei a katonai és kiberbiztonsági szervezetek, a döntéshozók, valamint maguk a közösségi média platformok is, hiszen a védelem és megelőzés több szereplő együttműködését követeli meg.

5.2.1. Integrált stratégia és doktrína kialakítása az információs műveletek kezelésére

A Magyar Honvédség és a nemzetbiztonsági szervek számára elengedhetetlen egy naprakész, integrált stratégia megléte, amely explicit módon foglalkozik a közösségi média terén folyó információs műveletekkel. Jelenleg készülőben van Haig Zsolt által említett egy MH Összhaderőnemi Információs Műveleti Doktrína, ami jó alap, de fontos, hogy ez a doktrína komplex módon kezelje a kérdést. Véleményem szerint fontos, hogy a doktrína és a belőle levezetett szabályzatok egyaránt tartalmazzanak kognitív és technikai elemeket.

Dr. Haig Zsolt kritikája alapján a NATO és a magyar irányelvek eddig túlzottan a közvélemény-befolyásolásra koncentráltak, elhanyagolva a technikai aspektusokat. Éppen ezért az új stratégiának ki kell küszöbölnie ezt a hiányosságot. Azaz a doktrínának rögzítenie kell, hogy a közösségi média a hadműveleti tér része, amelyen az ellenség dezinformációs és hackertámadásokat is indíthat, ezért védelmi és ellenintézkedéseket kell tervezni rá. Emellett javasolt a honvédségen belül egy dedikált információs műveleti egység, vagy munkacsoport megerősítése, amely folyamatosan figyeli a közösségi médiában megjelenő fenyegetéseket, elemzi az ellenséges információs kampányokat és koordinálja a reagálást. NATO-szinten több országban működnek már hasonló egységek (pl. stratcom központok), Magyarországnak is célszerű aktívan részt vennie a NATO és EU kereteken belüli információs hadviselés elleni programokban, és ezeket a tapasztalatokat a hazai doktrínába beépíteni.

5.2.2. A katonai és kiberbiztonsági szervezetek belső protokolljainak fejlesztése

Úgy vélem, hogy a megfelelő felkészülés érdekében a honvédségnek és más fegyveres testületeknek naprakésszé kell tenniük a műveleti biztonságra vonatkozó előírásaikat, kiterjesztve azokat a közösségi média használatra.

Világos szabályokban kell rögzíteni, milyen tartalmat oszthat meg egy katona a szolgálattal összefüggésben a közösségi médiában. Például tilos legyen szolgálati helyszínekről, érzékeny infrastruktúráról, beosztásról, technikai eszközökről képet posztolni engedély nélkül. Már léteznek ilyen szabályok, de a digitális korszakban

érdemes újra kommunikálni és betartatásukat ellenőrizni. Minden olyan tartalom megosztása kockázat, ami a honvédelmi munkáról jellemzőt árul el.

Rendszeres továbbképzéseket ajánlott tartani a katonáknak és kiberbiztonsági szakembereknek az aktuális információs fenyegetésekről. Ezeken be kell mutatni a legújabb trükköket (pl. deepfake videók), felhívni a figyelmet az adathalász profilokra, az álhírek terjesztésének módjaira. A képzés ne csak elméleti legyen, hanem gyakorlati felkészítés is szükséges, akár szimulációkkal, hogy mit tegyen egy katona, ha a közösségi médiában keresztül kémkedés vagy manipuláció célpontjává válik. Dr. Kovács László az interjú során hangsúlyozta a folyamatos, gyakorlati képzés fontosságát, ami véleménye szerint részben segítene a katonai szervezetek érzékeny operatív adatainak effektív védelemben.

A kritikus beosztású személyeknél és műveleti területen lévő alakulatoknál érdemes lehet korlátozni a közösségi média használatát a szolgálat ideje alatt. Például egy misszióban részt vevő katona ne posztolhasson valós időben a helyzetéről, vagy egy kibervédelmi központ munkatársainak munkahelyi gépeiről teljesen blokkolni lehetne a közösségi média elérését. Ezen intézkedések célja megnehezíteni az ellenség számára az információszerzést és a célba juttatást. Természetesen ez ütközhet személyiségi jogi kérdésekkel, de a műveleti biztonság elsődlegessége esetén indokolt korlátozás lehet. Kovács László is utalt rá, hogy a hozzáférés-korlátozással és egyéb technikai védelemmel szükséges óvni a kritikus területeket ott, ahol ez a műveleti biztonság szempontjából kiemelten fontos.

Ahol a honvédség maga folytat információs műveletet (például toborzó kampányok, stratégiai kommunikáció), ott javasolt a tartalmak készítőinek anonimitását védeni. Ez azért fontos, hogy a szerzőket ne lehessen célba venni vagy visszakeresni. Ugyanígy, hírszerzési vagy elhárítási céllal a katonai szervezetek létrehozhatnak fedőprofilokat a közösségi médiában, amelyekkel megfigyelhetik a gyanús csoportokat anélkül, hogy felfednék kilétüket. Azonban elengedhetetlen, hogy ennek is legyen protokollja, tehát legyenek a szükséges etikai és jogi keretei lefektetve, hogy ne sérüljön pl. a polgári lakosság adatvédelme.

5.2.3. Közösségi média platformok szabályozása és együttműködése

Az eredmények tükrében a döntéshozóknak erőteljesebb szabályozói fellépést kell mérlegelniük a közösségi médiacégek irányában. Az Európai Unió már megtette az első

lépéseket, például hatályba helyezte a korábbiakban már említett Digitális Szolgáltatások Törvényét (DSA), ami kötelező kockázatértékelést, átláthatósági jelentéseket és tartalommoderációs eljárásokat ír elő a nagy platformoknak. Magyarországnak e jogszabály hazai érvényesítése során figyelnie kell arra, hogy a külön magyar nyelvű és geopolitikai sajátosságú dezinformációs trendeket is vegyék figyelembe a cégek.

Véleményem szerint biztonsági érdekek miatt kötelezni kell a nagy közösségi platformokat, hogy osszanak meg információt arról, miként működnek a hírfolyam-algoritmusaik, különös tekintettel arra, hogyan kezelik a téves információkat. A szabályozóknak biztosítaniuk kell, hogy a platformok fejlesszék algoritmusaikat a szélsőségesen manipulatív tartalmak terjedésének visszaszorítására. Emellett az olyan felhasználói eszközöket, mint a „jelentés" gomb, hatékonyabbá kell tenni, ez történhet úgy is, hogy a sokszor jelentett posztokat automatikusan időlegesen korlátozni, amíg egy moderátor megvizsgálja azokat.

Szükség van egyértelmű jogi keretre arról, milyen típusú tartalmakat kell a platformoknak eltávolítaniuk (pl. választási dezinformáció, közegészségügyi álhírek). Ugyanakkor biztosítani kell a tisztességes eljárást is, azaz, hogy a felhasználók tudhassák, miért távolították el a tartalmukat, és legyen lehetőségük fellebbezni. A platformoknak erős hazai jelenléttel rendelkező moderációs csapatot kell fenntartaniuk, akik értik a magyar nyelvet és kontextust. Enélkül a globális cég könnyen nézőpontokat téveszt és az alkalmazott algoritmus akár túlreagálthat bizonyos magyar szavakat, vagy épp nem érzékeli az iróniát.

A szabályozók megfontolhatják a közösségi médián a valódi személyazonosság igazolásának ösztönzését bizonyos esetekben. Nem arra gondolok, hogy tiltsák az anonimitást, hanem hogy például politikai hirdetéseket csak igazolt személy, ill. gazdasági szereplő adhasson fel. Ez ugyanis gátolhatja a trollfarmokat abban, hogy ezerszám hozzanak létre kamuprofilokat. A botok detektálására a platformoknak fontosnak tartanám, hogy fejlett mintázatfigyelést vezessenek be. Például, ha egy profil, napi több száz posztot produkál, valószínűleg nem ember. Ehhez a jogi felhatalmazást a DSA már megadja, de a nemzeti nyomon kell követniük a végrehajtást, mely szerepet Magyarországon akár az NMHH is betölthetné.

Fontos, hogy a szabályozás betartatása érdekében legyenek szankciók, akár jelentős bírságok a techcégekre, ha nem felelnek meg a kötelezettségeknek. Az EU DSA

is több százmilliós bírságokat helyezett kilátásba. Nemzeti szinten is elő lehetne írni, hogy ha egy platform nem távolít el bizonyos veszélyes tartalmakat meghatározott időn belül, akkor pénzbüntetéssel sújtható. A korábbi részben elemzett kérdőívben is mutatkozott igény a "valótlan hírt terjesztő platformok" pénzbüntetésére.

A platformoknak meg kell könnyíteniük a kutatók hozzáférését az adatokhoz, hogy függetlenül elemezhető legyen a dezinformáció terjedése. Továbbá, egy állami koordinációs szerv rendszeres kapcsolatot tarthatna a platformok regionális képviseleteivel, és gyors csatornát biztosít például választási kampányidőszakban a dezinformációk jelentésére. Ebben az együttműködésben a civil tényellenőrzők is helyet kaphatnának. Az együttműködés keretein belül a hatóság összeülhetne a Facebookkal és tényellenőrző szervezetekkel, hogy megvitassák az aktuális álhír-trendeket és lépéseket.

5.2.4. Oktatás, képzés és tudatosságnövelés a civil lakosság körében

Ahogy a kérdőív válaszadói szinte egyhangúlag támogatják, az iskolai tananyag részévé kell tenni a digitális média tudatos használatát. Amit véleményem szerint nem elszigetelt, hanem integrált módon érdemes megtenni. Például magyar nyelv és irodalom órán lehet elemezni sajtócikkeket, történelem órán beszélni a propaganda történelmi példáiról és mai párhuzamairól, etika órán a dezinformáció társadalmi hatásáról. Emellett lehet önálló projekteket indítani a középiskolákban, ahol a diákok maguk gyűjtenek példákat álhírekre, és bemutatják azokat társaiknak. A tanárokat is fel kell készíteni erre a szerepre, azaz a pedagógus-továbbképzésbe is vegyék fel ezt a témakört.

Szükség van országos szintű figyelemfelkeltő kampányokra, melyek felhívják a lakosság figyelmét az információs manipuláció veszélyeire és megmutatják, hogyan lehet védekezni. Ezeknek a kampányoknak érthetőnek és közérthetőnek kell lenniük. Lehetnek rövid kisvideók a televízióban, közösségi médiában terjesztett infografikák, vagy akár plakátok formájában, melyeken olyan rövid üzenetek állhatnának, hogy: „Ne dőlj be az álhíreknek!”, „Ellenőrizd a forrást, mielőtt megosztod!”, „Ismerd fel a manipulált képeket!” stb. Ilyen kampányt indíthatna például a Nemzeti Kibervédelmi Intézet együttműködve civil szervezetekkel. A kormányzat számára is ajánlott, hogy apolitikus, közérdekű üzenetként kezelje ezt a témát, és különítsen el forrásokat e kampányokra amint teszi például a közlekedésbiztonság vagy kábítószer-prevenció terén is.

Tekintve, hogy a felmérés szerint az idősek kiemelt célcsoportot jelentenek és vélhetően sebezhetőbbek, fontos őket külön is elérni. Ajánlott közösségi házakban,

nyugdíjasklubokban, akár egyházakon vagy nyugdíjas egyesületeken keresztül médiahasználati workshopokat tartani idősebbeknek. Ezek keretében fiatal trénerek megmutathatják, hogyan ismerjék fel a gyanús, hogyan használjanak egyszerű módszereket.

Mivel a manipulációs technikák fejlődnek, a tudatosításnak is lépést kell tartania. Ajánlott, hogy a kormányzat illetékes szerve időről időre adjon ki figyelmeztetést a lakosságnak, ha épp egy bizonyos típusú dezinformációs kampány erősödik. Például, ha a hírszerzés azt látja, hogy közeledik egy választás és nő az álhírek száma egy témában, legyen egy hivatalos közlemény vagy sajtótájékoztató, ami felhívja erre a figyelmet. Ezt Kovács László is alátámasztotta azzal, hogy a közösségi médián keresztül indított hibrid támadások fenyegetése egyre nő, ezért fontos a gyors reagálás és a proaktív védelem. Bányász Péter is megjegyezte, hogy a gyors válságkommunikáció, azaz a hivatalos szervek gyors és hiteles reakciója fontos eszköz lehet egy információs támadás semlegesítésében.

5.2.5. Nemzetközi és intézményi együttműködés erősítése

Nem elég csupán nemzeti erőfeszítéseket tenni, ezért csatlakozni kell az EU stratcom kezdeményezéseihez, például az East StratCom Task Force-hoz, amely az orosz dezinformáció ellen jött létre, vagy az Európai Demokratikus Akcióterv programjaihoz, melyek a választások védelmét célozzák. A NATO keretében a Stratégiai Kommunikációs Kiválósági Központ és a Kiber Védelmi Kiválósági Központ is foglalkozik ezekkel a kérdésekkel, ezért ajánlott, hogy a magyar szakértők aktívan vegyenek részt az ottani kutatásokban, gyakorlatokban. Bányász Péter szerint a platformok elleni fellépés akkor tud a leghatékonyabban működni, ha szabályozók nemzetközileg együttműködve lépnek fel. Ezt a gondolatot kiterjeszthetjük akár állami szintre is, ahol példának okáért a V4 országok közösen kezdeményezhetnének regionális konferenciát az információs műveletek kezeléséről.

Fontos a szomszédos és szövetséges országokkal való tapasztalatcsere is, hiszen több fronton is hasonló gondokkal küzdünk. Ajánlott évente nemzetközi szakmai fórumot tartani, ahova meghívjuk más országok tapasztalatait. Az ilyen együttműködés segít felderíteni a határokon átnyúló információs műveletek hálózatait is.

A kormányzati és katonai szerveknek együtt kell működniük a civil társadalommal és a technológiai szektorral. Ez magába foglalja a hazai egyetemek,

kutatóintézetek támogatását e téma kutatásába, valamint a nagy IT vállalatokkal való párbeszédet. Ide tartozhat pl. a Facebook magyarországi irodájával való rendszeres konzultáció, vagy a Google-lel a YouTube tartalomszűrés javítása ügyében való egyeztetés. A civil szervezetek bevonása növeli a beavatkozások legitimitását és hatékonyságát, hiszen sokszor ők látják első kézből a problémákat.

5.2.6. Jogi hiányosságok pótlása és keret kialakítása az információs hadviselés ellen

Fontosnak tartok egy jogi definíció megalkotását az információs művelet és a dezinformációs tevékenység fogalmára a magyar jogban. Ez segítene abban, hogy a hatóságok jogszerűen tudjanak eljárni ilyen ügyekben. Jelenleg csak közvetett tényállások vannak, de azok nem fedik le a jelenség minden aspektusát. Egy pontos definíció alapján be lehetne azonosítani, mi számít tiltott magatartásnak.

Fontolóra vehető, hogy bizonyos súlyos esetekben az ilyen cselekményeket nemzetbiztonsági fenyegetésnek minősítsék. Ez feljogosítaná a szolgálatokat az erőteljesebb fellépésre, például titkosszolgálati eszközök alkalmazására a hálózat felderítésére. Természetesen ez sarkalatos pont, ügyelni kell a visszaélések elkerülésére, de például egy átfogó, választást célzó külföldi dezinformációs kampány esetén indokolt lehet.

A választási eljárásról szóló törvényeket ajánlott kiegészíteni a digitális kampánytevékenység szabályozásával. Például tilos legyen anonim módon politikai hirdetéseket közzétenni, vagy elő lehessen írni, hogy a közösségi médiában terjedő súlyos rágalmakat a Választási Bizottság gyorsított eljárásban vizsgálhassa, és kötelező helyreigazítást rendeljen el a platformon is, ne csak egy nyomtatott sajtótermékben. Ez jogszabályi oldalról segít kezelni a kampányidőszakban elszabaduló álhír dömpinget.

Azonosíthatóak konkrét szervezetek vagy hálózatok, amelyek sorozatosan és bizonyíthatóan álhíreket gyártanak és terjesztenek a közösségi médiában, akkor jogi eszközökkel fel lehet lépni ellenük. Ez jelenthet működési engedély bevonást, büntetőeljárást kezdeményezést konkrét ügyek kapcsán, vagy polgári peres úton kártérítési igényeket, ha valaki károsultja volt a tevékenységüknek. Az ilyen jogi fellépésnek visszatartó ereje lehet, bár sokszor ezek a csoportok rejtve működnek, így a felderítésükhöz is erősítendő a nyomozati munka.

Összességében az ajánlások lényege egy többrétegű védelmi vonal kiépítése az egyén szintjén, a közösség szintjén, a nemzet szintjén és a nemzetközi színtéren együttesen. Csak így lehet hatékonyan kezelni a közösségi média által felerősített információs hadviselés kockázatait. Fontos hangsúlyozni a rugalmasságot is. Az ajánlásokat időről időre felül kell vizsgálni a technológiai és társadalmi változások fényében. Ami ma beválik, lehet, hogy holnap már kevés, ezért a szabályozónak és a hadvezetésnek is agilisnak kell lennie e téren.

6. ÖSSZEGZETT KÖVETKEZTETÉSEK

Kutatómunkám célja az volt, hogy **feltárjam a közösségi média szerepét a katonai és információs műveletekben, különös tekintettel a kibertérben zajló hadviselésre, az információs befolyásolás mechanizmusaira, valamint az ezekből fakadó nemzetbiztonsági kockázatokra és lehetőségekre**. A kutatás hipotézisei és célkitűzései alapján részletes elemzést végeztem a közösségi média alkalmazásáról a modern hadviselésben, amely mind a stratégiai kommunikáció, mind a befolyásolási műveletek és a kibertámadások szempontjából meghatározóvá vált.

A kutatás első számú hipotézise szerint **a közösségi média hatékony eszköz az információs műveletek során**. Az elemzett esettanulmányok és elméleti megközelítések egyaránt megerősítették ezt az állítást. A platformok gyorsasága, globális elérése és tömegbefolyásolási képessége révén a közösségi média mára alapvető hadviselési eszközzé vált. A 2014-es Krím-félsziget annexiója vagy **az ukrajnai háború tapasztalatai rávilágítottak arra, hogy a közösségi média képes valós idejű, célzott üzenetközvetítésre**, mellyel akár a hadszíntér percepciója is jelentősen befolyásolható.

A második hipotézis a szabályozatlanság kérdését vizsgálta. A platformok decentralizáltsága, jogi szürkezónája és a felhasználói aktivitás kvázi-kontrollálhatatlansága révén valóban olyan környezetet biztosítanak, amelyben a dezinformáció gyorsan és akadálytalanul terjedhet. Ez a tulajdonság különösen vonzó az információs háborúkban érdekelt állami és nem állami szereplők számára. A közösségi média tehát nem csupán információs eszköz, hanem stratégiai célpont is lett, amelynek kontrollálása vagy manipulálása önmagában is komoly erőforrásokat igényel.

A harmadik hipotézis a közösségi média stratégiai kommunikációs képességeit állította a vizsgálat középpontjába. Az elemzés alátámasztotta, hogy a platformok lehetőséget adnak a valós idejű, célzott kommunikációra, valamint az ellenség információs fölényének aláásására. A katonai szervezetek részéről azonban ez csak akkor lehet sikeres, ha megfelelő intézményi kapacitásokkal, szakmai protokollokkal és képzett személyzettel párosul a közösségi média alkalmazása. A közösségi kommunikációs stratégiák nem helyettesíthetik a klasszikus katonai döntéshozatalt, viszont képesek erősíteni annak hatását és legitimitását.

A negyedik hipotézis szintén alátámasztást nyert. A hamis profilok, adathalász kampányok, információgyűjtés és megfigyelés céljára használt algoritmusok mind hozzájárulnak a közösségi média platformok támadó potenciáljához. A vizsgálatok alapján kijelenthető, hogy a közösségi média nem csupán az információs hadviselés, hanem a kiberhadviselés egyik alapvető eszközévé is vált, amely komoly veszélyt jelent a katonai szervezetek operatív biztonságára, különösen ha az egyéni felhasználás nem kontrollált.

A kutatás során megfogalmazott célok eredményei azt mutatják, hogy **a közösségi média és az információs műveletek között rendkívül szoros és kölcsönös kapcsolat van, amely mindkét fél, a támadó és a védekező számára kritikus fontosságú**.

A közösségi média szerepének elemzése rámutatott, hogy a **közösségi platformok alkalmazása a hadműveletek minden szakaszában releváns lehet**. Ugyanakkor a platformok használata egyre inkább kihívások elé állítja a hagyományos katonai logikát, mivel az üzenetek percepcióját nem kizárólag a tartalom, hanem a közeg, az algoritmikus terjesztés és a célcsoport reakciókészsége is befolyásolja. Ez újfajta katonai és stratégiai gondolkodást tesz szükségessé, amely integrálja a társadalomtudományi, kommunikációs és technológiai szempontokat.

A dolgozatban elvégzett vizsgálatok, illetve az azokból levontkövetkeztetések egyik fontos eredménye, hogy a közösségi médiát érintő szabályozás hiánya súlyos biztonságpolitikai következményekkel járhat. Megállapítottam, hogy **a platformok üzleti logikája gyakran ellentétes a nemzetbiztonsági és katonai szempontokkal**. A megfelelő jogi, technológiai és etikai keretek kialakítása tehát alapvető fontosságú a jövőbeni konfliktusok megelőzése és kezelése érdekében. Emellett külön figyelmet kell fordítani a platformok átláthatóságára, az automatizált tartalomterjesztési rendszerek auditálására, valamint az állami és civil szféra közötti együttműködésre a biztonságos információs környezet fenntartása érdekében.

A katonai szervezetek számára a közösségi média alkalmazásához szükség van megfelelő szervezeti és infrastrukturális háttérre. A digitális műveltség, a kockázatfelismerés, a stratégiai kommunikációs képességek fejlesztése, valamint a kiberbiztonsági protokollok betartása elengedhetetlen ahhoz, hogy a közösségi média ne csak veszélyforrást, hanem valódi lehetőséget jelentsen. Ennek érdekében olyan komplex képzési programokat kell bevezetni, amelyek a katonai személyzet digitális

kompetenciáinak fejlesztését célozzák, különös tekintettel a platformhasználat biztonsági és etikai aspektusaira.

A technológiai fejlesztések új dimenziókat nyitnak az információs műveletekben. Ugyanakkor ezek az eszközök csak akkor lehetnek hatékonyak, ha a használatukat körülvevő stratégiai, etikai és szabályozási keretek is megfelelően kidolgozottak. A mesterséges intelligencia nem csupán új támadási lehetőségeket, hanem az ellenintézkedések kulcseleme is lehet, például valós idejű tartalomazonosítás vagy forrásellenőrzés formájában.

Összességében a dolgozat eredményei egyértelműen alátámasztják, hogy a közösségi média katonai alkalmazása nem választható el a digitális hadviselés tágabb kontextusától. A közösségi platformok nem pusztán kommunikációs eszközök, hanem a modern háborúk és geopolitikai küzdelmek szerves részei. Az információs fölény megszerzése ma már nemcsak az ellenséges erők legyőzését jelenti, hanem a közvélemény, a médiatér és az online narratívák feletti uralom biztosítását is.

A jövő kihívása abban áll, hogy a katonai és nemzetbiztonsági szervezetek képesek legyenek adaptálódni ehhez az új realitáshoz. Ez több szinten is változásokat igényel, méghozzá a hadászati gondolkodásban, az intézményi struktúrákban, a képzési rendszerekben, valamint a technológiai fejlesztésekben. Az információs műveletek sikere nemcsak a technológiai fölényen, hanem az etikai és társadalmi legitimitás fenntartásán is múlik. A katonai műveletek során a közösségi média hatékony és biztonságos alkalmazása csak akkor valósulhat meg, ha az átláthatóság, a felelősség és a jogállamiság elvei nem csorbulnak, és ha az információs hadviselés nem válik öncélú manipulációs gyakorlattá.

ÚJ TUDOMÁNYOS EREDMÉNYEK

1) **A közösségi média kettős természetének (StratCom-eszköz + kiberhadviselési felület) integrált tézise**

A kutatásaimmal igazoltam, hogy a közösségi média a modern konfliktusokban kettős funkciót tölt be: **egyszerre szolgál stratégiai kommunikációs (StratCom) eszközként és a kiberhadviselés egyik műveleti felületeként**. A dolgozat empirikus és elméleti elemzései alapján e két dimenzió nem választható szét, mivel az információs műveletek, a dezinformáció és az OPSEC-kockázatok ugyanazon platform-infrastruktúrára épülnek. Ez az eredmény alátámasztja a H3 és H4 hipotéziseket, valamint teljesíti a közösségi média stratégiai szerepének feltárására irányuló kutatási célokat.

2) **Empirikus mintázat: „észlelt kompetencia" vs. „minimális valós ellenőrzés" – a társadalmi reziliencia mérhetőségének operacionalizálása**

Bizonyítottam, hogy a társadalom önbizalma mögött mérhető, de nem teljes körű dezinformáció-felismerési képesség áll. A dolgozat módszertani újítása, hogy a vizuális és információs műveltséget nem kizárólag önbevallásos kérdésekkel méri, hanem ellenőrző tesztkérdések beépítésével elkülöníti az észlelt kompetenciát a tényleges felismerési képességtől. Az eredmények rámutatnak arra, hogy a válaszadók közepes szintű önbizalma mögött mérhető, de nem teljes körű dezinformáció-felismerési képesség áll. Ez az operacionalizálás hozzájárul a társadalmi reziliencia empirikus mérhetőségéhez, és alátámasztja a K2 kutatási célt.

3) **Felhasználói reakcióprofil: a „platform-jelentés" dominanciája mellett magas a passzív elhárítás aránya, ami korlátozza a védekezési láncot**

Meghatároztam a kibertéri, különösen a közösségi pltaformok esetében a védekezési lánc hatékonyságát befolyásoló tényezőket. Az empirikus adatok alapján azonosítható egy reakciós minta, amely szerint a felhasználók többsége gyanús tartalom esetén platformszintű jelentést tesz, ugyanakkor jelentős arányban jelen van a passzív elkerülő magatartás is. A dolgozat kimutatja, hogy ez a viselkedés korlátozza a védekezési lánc hatékonyságát, mivel a jelentések tényleges hatása nagymértékben függ a platformok feldolgozó- és moderációs kapacitásától. Ez az eredmény közvetlenül kapcsolódik a destabilizációs hatások vizsgálatához és a K2 kutatási célhoz.

4) **Szabályozási következtetés: a közösségi média „stratégiai célponttá” vált, a jogi szürkezóna pedig a műveletek hatékonyságának strukturális feltétele**

Javaslatot tettem arra, hogy az információs műveletek keretében a közösségi platformok milyen módon erősítsék annak hatékonyságát, és milyen védekező mechanizmusok szükségesek. Kutatásom megállapítja, hogy a közösségi média jogi és intézményi szürkezónája strukturális feltételként erősíti az információs műveletek hatékonyságát. A platformok decentralizált működése és eltérő szabályozása következtében a közösségi média nemcsak eszköze, hanem önálló stratégiai célpontja is a kiber- és információs hadviselésnek. Ez az eredmény alátámasztja a H2 hipotézist, valamint a szabályozási és nemzetbiztonsági összefüggések feltárására irányuló kutatási célokat.

AJÁNLÁSOK

1. A nemzeti és nemzetközi kiberbiztonsági és védelmi stratégiák kidolgozásakor a közösségi médiát integrált műveleti térként szükséges kezelni, amelyben az információs és kibertéri műveletek egymást erősítve jelennek meg. Ennek megfelelően indokolt olyan összehangolt StratCom–cyber–OPSEC keretrendszerek kialakítása, amelyek nem különálló szakpolitikai területekként, hanem egységes fenyegetési ökoszisztémaként kezelik a közösségi platformokat. Ehhez javaslom a dolgozatomban elvégzett vizsgálatokat és azok eredményeit felhasználni.

2. A társadalmi reziliencia és médiaműveltség fejlesztésére irányuló programokban az önbevallásos kompetenciamérést ki kell egészíteni gyakorlati, helyzetalapú teszteléssel, amely képes mérni a tényleges dezinformáció-felismerési és döntési képességeket. A kutatás eredményei alapján javaslom egy standardizált mérési keret kidolgozását, amely empirikus adatokat szolgáltat a képzési beavatkozások hatékonyságáról, és hosszabb távon összehasonlíthatóvá teszi a reziliencia-szinteket.

3. A közösségi média platformokkal való együttműködés során a válságkezelési és kiberbiztonsági tervezésnek figyelembe kell vennie a moderációs kapacitások korlátait. Ennek érdekében indokoltnak tartom olyan prioritásalapú jelentési és feldolgozási protokollok kialakítását, amelyek válsághelyzetekben kiemelten kezelik a nemzetbiztonsági és közbizalmat érintő tartalmakat, csökkentve a passzív felhasználói magatartásból fakadó kockázatokat.

4. A dolgozatom eredményei alapján javaslom a közösségi média szabályozásának nemzetközi szintű harmonizálását, különös tekintettel a hibrid fenyegetésekre és információs műveletekre. A jogi szürkezónák felszámolása érdekében javaslom továbbá olyan nemzetközi normák és együttműködési mechanizmusok kialakítása, amelyek világosan meghatározzák a platformok felelősségét válsághelyzetekben, miközben biztosítják az alapvető jogok és a demokratikus diskurzus védelmét.

ÁBRÁK ÉS KÉPEK JEGYZÉKE

RÖVIDÍTÉSEK JEGYZÉKE

AES — *Advanced Encryption Standard* — fejlett titkosítási szabvány

AI — *Artificial Intelligence* — mesterséges intelligencia

AJP — *Allied Joint Publication* — NATO szövetséges összhaderőnemi kiadvány

AR — *Augmented Reality* — kiterjesztett valóság

AR/VR — *Augmented Reality / Virtual Reality* — kiterjesztett / virtuális valóság

CCDCOE — *NATO Cooperative Cyber Defence Centre of Excellence* — NATO Kibervédelmi Kiválósági Központ (Tallinn)

CoE — *Centre of Excellence* — kiválósági központ (pl. NATO COE-k)

DCO — *Defensive Cyber Operations* — defenzív kibertér műveletek

DDoS — *Distributed Denial of Service* — elosztott szolgáltatásmegtagadásos támadás

DSA — *Digital Services Act* — Digitális Szolgáltatásokról szóló rendelet (EU)

EDMO — *European Digital Media Observatory* — Európai Digitális Média Megfigyelőközpont

EEAS — *European External Action Service* — Európai Külügyi Szolgálat

ENSZ — *United Nations (UN)* — Egyesült Nemzetek Szervezete

EU — *European Union* — Európai Unió

FedEx — *Federal Express*

GDPR — *General Data Protection Regulation* — Általános adatvédelmi rendelet

GPS — *Global Positioning System* — globális helymeghatározó rendszer

GRU — *(Russian military intelligence; többféle átírás)* — orosz katonai hírszerzés (a dolgozat nem bontja ki)

HUMINT — *Human Intelligence* — emberi hírszerzés

IAM — *Identity and Access Management* — identitás- és hozzáférés-kezelés

IDS — *Intrusion Detection System* — behatolásészlelő rendszer

IPS — *Intrusion Prevention System* — behatolásmegelőző rendszer

IRA — *Internet Research Agency* — (orosz) „trollgyárként” emlegetett szervezet (a dolgozat nem definiálja formálisan)

ISIS — *Islamic State of Iraq and Syria* — Iszlám Állam

ISR — *Intelligence, Surveillance and Reconnaissance* — felderítés, megfigyelés és felderítő információgyűjtés

IT — *Information Technology* — információtechnológia

IoT — *Internet of Things* — dolgok internete

MH — *Magyar Honvédség*

MI — mesterséges intelligencia

MIL — *Media and Information Literacy* — média- és információs műveltség

NAFO — *North Atlantic Fellas Organization* — online közösség/mém-hálózat

NATO — *North Atlantic Treaty Organization* — Észak-atlanti Szerződés Szervezete

NIS — *Network and Information Security (Directive)* — NIS irányelv (hálózat- és információbiztonság)

NIS2 — *NIS2 Directive* — NIS2 irányelv

NMHH — Nemzeti Média- és Hírközlési Hatóság

NetzDG — *Netzwerkdurchsetzungsgesetz* — német „hálózatérvényesítési”/platformszabályozási törvény

OCO — *Offensive Cyber Operations* — offenzív kibertér műveletek

OPSEC — *Operational Security* — műveleti biztonság

OSINT — *Open Source Intelligence* — nyílt forrású hírszerzés

PET — *Privacy-Enhancing Technologie*

PSYOPS — *Psychological Operations* — pszichológiai műveletek (pszichológiai hadviselés)

PSYWAR — *Psychological Warfare* — pszichológiai hadviselés

RBAC — *Role-Based Access Control* — szerepkör-alapú hozzáférés-vezérlés

RSA — *Rivest–Shamir–Adleman* – aszimmetrikus titkosítási algoritmus

RSS — *Really Simple Syndication* — hírcsatorna-formátum

RT — *RT (Russia Today)* — orosz nemzetközi médiaszolgáltató márkaneve

SCADA — *Supervisory Control and Data Acquisition* — ipari felügyeleti irányítórendszer

SIGINT — *Signals Intelligence* — jelhírszerzés

StratCom — *Strategic Communications* — stratégiai kommunikáció

UNESCO — *United Nations Educational, Scientific and Cultural Organization* — ENSZ Nevelésügyi, Tudományos és Kulturális Szervezete

USA — *United States of America* — Amerikai Egyesült Államok

VK — *(közösségi platform rövid neve)* — VK (VKontakte)

VR — *Virtual Reality* — virtuális valóság

genAI — *generative AI* — generatív mesterséges intelligencia

Publikációs lista

Bihaly, Barbara. (2021). *Az elektronikai hadviselés eszközei az információs és kibertérműveletek támogatásában az ukrán konfliktus példáján keresztül.* HADMÉRNÖK, 16(4), 101–112.

Bihaly, Barbara. (2022). *A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában.*HADTUDOMÁNYI SZEMLE, 14(3), 45–55

Bihaly, Barbara. (2022). *Kibervédelem a NATO-ban és az EU-ban.* HADTUDOMÁNYI SZEMLE, 15(4), 37–49.

Bihaly, Barbara**.** (2022). *A felhőalapú szolgáltatások alkalmazása az amerikai haderőben, különös tekintettel az U.S. Army stratégiájára.* HADMÉRNÖK, 17(4), 113–129.

Bihaly, Barbara. (2022). *A mesterséges intelligencia felhasználása az információs és kibertérműveletekben – az orosz minta.* HADMÉRNÖK, 17(3), 97–107.

Fábri, Barbara. (2025). *The War That Went Viral: The Russian–Ukrainian War on Social Media.* HADTUDOMÁNYI SZEMLE, 18(2), 91–106.

Fábri Barbara. (2025) A kiber- és az űrbiztonság metszéspontjai 1., Az űr és a kibertér kapcsolata. *Felderítő Szemle.* 24(2). 136-150.

FELHASZNÁLT IRODALOM

[1] Kiss, Á. P. (2009). Generációk a hadviselésben - Negyedik generáció. *2*(2), 10-18.

[2] Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

[3] Lehto, M., & Hutchinson, B. (2021). Mini-drones swarms and their potential in conflict situation. *CCWS 2020 15th International Conference on Cyber Warfare and Security*, 326-333.

[4] Dunlap, C. J. (2014). The hyper-personalization of war: cyber, big data, and the changing face of conflict. *Georgetown Journal of International Affairs*, 108-118.

[5] Svetoka, S. (2016). *Social media as a tool of hybrid warfare*. NATO Strategic Communication Centre of Excellence.

[6] Kovács, L. (2023). Nyomásgyakorlás a kritikus információs infrastruktúrák támadásán keresztül. In *Taktikák és stratégiák a kiberhadviselésben* (pp. 151-168). Ludovika Egyetemi Kiadó.

[7] Rybak, Ł., & Dudczky, J. (2019). Increasing the information superiority on the modern battlefield through the use of virtual reality systems. *Security and Defence Quarterly*, *25*(3), 86-98.

[8] Négyesi, I. (2023). A vitruális valóság technológia alkalmazásának lehetőségei a katonai készségfejlesztésben. *Hadtudományi Szemle*, *2*, 3-16.

[9] Haig, Z., Kovács, L., Ványa, L. (2011). Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata. *Felderítő Szemle*, *10*(1-2), 183-209.

[10] Garamone, J. (2018. február 13.). *Cyber tops list of threats to U.S., director of national intelligence says*. Elérhető: https://www.war.gov/News/News-Stories/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/

[11] Bihaly, B. (2021). Az elektronikai hadviselés eszközei az információs és kibertérműveletek támogatásában az ukrán konfliktus példáján keresztül. *Hadmérnök*, *16*(4), 101-112. Elérhető: https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/5581/4829 utoljára letöltve: 2026.04.09.

[12] Haig, Zs. (2022) Kibertéri kognitív befolyásolás az információs műveletekben. *Hadtudományi Szemle, (15)*2. 115-130. Elérhető: https://folyoirat.ludovika.hu/index.php/hsz/article/view/6139/5078 utoljára letöltve: 2026.04.09.

[13] Geneva Academy. (2024. március). *Artificial Intelligence and Related Technologies in Military Decision-Making (Expert Consultation Report)*. Elérhető: https://archives.geneva-academy.ch/joomlatools-files/docman-files/Artificial%20Intelligence%20in%20Military%20Decision%20Making.pdf utoljára letöltve: 2026.04.09.

[14] Bihaly, B. (2022). A mesterséges intelligencia felhasználása az információs és kibertérműveletekben– az orosz minta. *Hadmérnök*, *17*(3), 97-107. Elérhető: https://real.mtak.hu/154327/1/07_bihaly_97-107_HM2022_3.pdf utoljára letöltve: 2026.04.09.

[15] Atkinson, R. (2024). Artificial Intelligence in Modern Warfare: Strategic Innovation and Emerging Risks. *Military Review*, 103-107.

[16] Frater, M., & Ryan, M. (2001). *Communications Electronic Warfare and the Digitised Battlefield*. Elérhető: https://researchcentre.army.gov.au/sites/default/files/wp116-comms_ew_and_digitised_battlefield_michael_frater_michael_ryan.pdf utoljára letöltve: 2024.04.09.

[17] NATO. (2015). *Allied Joint Publication AJP-3.10 – Allied Joint Doctrine for Information Operations*. NATO Standardization Office.

[18] Haig, Zs. (2011). Az információs hadviselés kialakulása, katonai értelmezése. *Hadtudomány*, *21*(1-2), 12-28.

[19] Haig, Zs. (2018). *Információs műveletek a kibertérben*. Dialóg Campus Kiadó.

[20] Kovács, L. (2018). *Kiberbiztonság és -stratégia*. Dialóg Campus Kiadó.

[21] Rácz, A. (2010). Az Orosz Föderáció új katonai doktrínája. *Nemzet és Biztonság*, *3*(2), 92-94.

[22] Ajir, M., & Vailliant, B. (2018). Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, *Fall*, 70-89.

[23] Haig, Zs., & Várhegyi, I. (2005). *Információs műveletek a hadszintéren*. Zrínyi, p. 198.

[24] Springer, P. J. (2015). *Cyber Warfare: A Reference Handbook*. ABC-CLIO.

[25] NATO. (2020). *AJP-3.20 ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS*. Elérhető: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf utoljára letöltve: 2024.04.09.

[26] Magyarország Kormánya. (2020). *1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról*.

[27] Magyarország Országgyűlése. (2012). *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről*.

[28] Csiki Varga, T., & Tálas, P. (2020). Magyarország új nemzeti biztonsági stratégiájáról. *Nemzet és Biztonság*, *3*, 89–112.

[29] Róbert, H. (2025. április 1.). *Mesterséges intelligencia használata a kibervédelemben és kibertámadások során*. biztonsagpolitika.hu. Elérhető: https://biztonsagpolitika.hu/kiemelt/mesterseges-intelligencia-hasznalata-a-kibervedelemben-es-kibertamadasok-soran utoljára letöltve: 2024.04.09.

[30] Kovács, L. (2021). Offenzív kiberműveletek II.: Kibererők és képességeik. *Hadmérnök*, *16*(3), 119-137.

[31] Bányász, P., & Orbók, Á. (2013). A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. *Hadmérnök*, 188-209.

[32] Bányász, P. (2015). A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle*, 21-36.

[33] Dévai, D. (2019). A kiberfegyver koncepció evolúciója. *Hadmérnök*, 272-280.

[34] ESET. (n.d.). *Mi is az a NIS2? Milyen új módosítások léptek életbe 2025. január 1-jével?* Elérhető: https://www.eset.com/hu/mi-is-az-a-nis2-milyen-uj-modositasok-leptek-eletbe/ utoljára letöltve: 2024.04.09.

[35] Stoddart, K. (2022). Non and sub-state actors: Cybercrime, terrorism, and hackers. In *Cyberwarfare: threats to critical infrastructure* (pp. 351-399). Springer International Publishing.

[36] Al-Bayati, A. S. (2023). *Enhancing Performance of Hybrid AES, RSA and Quantum Encryption Algorithm*. Anglia Ruskin Research Online (ARRO).

[37] Knapp, E. D. (2024). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Elsevier.

[38] Sultana, S., et al. (2022). AI-powered threat detection in modern cybersecurity systems: Enhancing real-time response in enterprise environments. *World Journal of Advanced Engineering Technology and Sciences*, 136-146.

[39] Kuehn, P., et al. (2020). Sharing of Cyber Threat Intelligence between States. *T H E M E N S C H W E R P U N K T*, 22-28.

[40] Investopedia. (2023). *Social Media: Definition, Importance, Top Websites & Apps*. Elérhető: https://www.investopedia.com/terms/s/social-media.asp utoljára letöltve: 2024.04.09.

[41] Hanna, K. T. L. B. (2025. január 23.). *What is social media?* Elérhető: https://www.techtarget.com/whatis/definition/social-media utoljára letöltve: 2024.04.09.

[42] Kaplan, A. M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59-68.

[43] Nagy, T. (2012). *Vélemény 2.0 – Közösségi média könyv*.

[44] Klausz, M. (2016). *A közösségi média nagykönyve*. Atheneum Kiadó.

[45] Xing, L. D. K. W. H. X. P., & G. J. (2019). Behavioral habits-based user identification across social networks. *Symmetry*, *11*(9), 1134.

[46] Hutsul, T. K. M. T. V. K. O. M. O. I. V., & S. A. (2024). Review of approaches to the use of unmanned aerial vehicles, remote sensing and geographic information systems in humanitarian demining: Ukrainian case. *Heliyon*, *10*(7).

[47] Borelli, M. (2023). Social media corporations as actors of counter-terrorism. *New Media & Society*, *25*(11), 2877-2897.

[48] Hajli, N. S. U. T. M., & S. F. (2022). Social bots and the spread of disinformation in social media: the challenges of artificial intelligence. *British Journal of Management*, *33*(3), 1238-1253.

[49] Saxena, P. S. V. P. A. F. U., & S. K. (2023). *Multiple aspects of artificial intelligence*. Book Saga Publications.

[50] Okoli, U. I. O. O. C. A. A. O., & A. T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, *21*(1), 2286-2295.

[51] Putter, D., & H. S. (2022). Social media intelligence: The national security–privacy nexus. *Scientia Militaria: South African Journal of Military Studies*, *50*(1), 19-44.

[52] Goldfield, C. C. (2020). "The Right to Be Forgotten" and Its Unintended Consequences to Intelligence Gathering. *Fla. J. Int'l L.*, *32*, 183.

[53] Ináncsi, M. F. T. (2022). Álhírek ellenőrzése a közösségi média felületeken a COVID-19 járvány alatt. *Hadtudományi Szemle*, *32*, 42–53.

[54] Goswami, M. (2024). AI-based anomaly detection for real-time cybersecurity. *International journal of research and review techniques*, *3*(1), 45-53.

[55] Mozumder, M. A. I. S. R. I. U. S. M. I. A. A., & K. H. C. (2023). The metaverse for intelligent healthcare using XAI, blockchain, and immersive technology. *IEEE International Conference on Metaverse Computing, Networking and Applications*, 612-616.

[56] Werth, J. B. M. H. B. H. R. E. I. N., & P. C. (2023). A Review of Blockchain Platforms Based on the Scalability, Security and Decentralization Trilemma. *ICEIS*, *1*, 146-155.

[57] Yamuna, S. M., & M. C. P. (2025). ETHICAL DATA PRACTICES IN THE DIGITAL AGE: ENSURING PRIVACY, TRANSPARENCY, AND ACCOUNTABILITY. *PSG College of Arts & Science*, 59-63.

[58] Fábri, B. (2025). The War That Went Viral: The Russian–Ukrainian War on Social Media. *Hadtudományi Szemle*, *18*(2), 91-106.

[59] Cohen, R. S., et al. (2021). *Combating foreign disinformation on social media: Study overview and conclusions*. RAND.

[60] Marathe, A. R., et al. (n.d.). *Simulation for Future Command and Control: A Multifaceted Challenge*. NATO.

[61] Hayes, M. D. M. B. H. R. E., & M. M. (2013). Social Media Influencing C2 in Underdeveloped and Degraded Operational Environments. *18th ICCRTS: "C2 in Underdeveloped, Degraded and Denied Operational Environments"*.

[62] Rushing, B. (2024). Analysis of Media Influence on Military Decision-Making. *International Conference on Cyber Warfare and Security*, 308-316.

[63] Rettore, P. H. Z. P. A. M. Z. C., & S. P. (2023). Military data space: Challenges, opportunities, and use cases. *IEEE Communications Magazine*, *62*(1), 70-76.

[64] Yin, J. L. A. C. M. R. B., & P. R. (2012). Using social media to enhance emergency situation awareness. *IEEE intelligent systems*, *27*(6), 52-59.

[65] Granåsen, M. (2019). *Exploring C2 Capability and Effectiveness in Challenging Situations: Interorganizational Crisis Management, Military Operations and Cyber Defence*. Linköping University Electronic Press.

[66] Henderson, S. (2024). Deception in cyberwarfare. In *Research Handbook on Cyberwarfare* (pp. 223-246). Edward Elgar Publishing.

[67] Voke, M. R. (2019). *Artificial Intelligence for Command and Control of Air Power*. Air University Press.

[68] Beatrix, T. (2023). *Az orosz információs hadviselés elmélete és nyelvi-retorikai eszköztára (disszertáció)*. Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola.

[69] Aro, J. (2022). *Putyin trolljai - Igaz történetek az orosz infoháború frontvonalából*. Corvina Kiadó Kft.

[70] Khaldarova, I., & P. M. (2020). Fake news: The narrative battle over the Ukrainian conflict. In *The future of journalism: Risks, threats and opportunities* (pp. 228-238). Routledge.

[71] Everstine, B. (2015. június 4.). Carlisle: Air Force Intel Uses ISIS 'Moron's' Social Media Posts to Target Airstrikes. *AirForce Times*, *4*. Elérhető https://www.airforcetimes.com/news/your-air-force/2015/06/04/carlisle-air-force-intel-uses-isis-moron-s-social-media-posts-to-target-airstrikes/ utoljára letöltve: 2024.04.09.

[72] Comunello, F., & A. G. (2012). Will the revolution be tweeted? A conceptual framework for understanding the social media and the Arab Spring. *Islam and Christian–Muslim Relations*, *23*(4), 453-470.

[73] Llewellyn, C. C. L. F. H. A. R. L. (2018). For Whom the Bell Trolls: Troll Behaviour in the Twitter Brexit Debate. *Journal of Common Market Studies*.

[74] Hetrick, C. (2023. március 3.). *How to spot AI fake content—and what policymakers can do to help stop it*. Elérhető: https://phys.org/news/2024-07-ai-fake-content-policymakers.html utoljára letöltve: 2024.04.09.

[75] Nadal, L. d. J. P. (2024). Beyond the deepfake hype: AI, democracy, and "the Slovak case". *Harvard Kennedy School Misinformation Review*, *5*(4).

[76] Pennycook, G. (2022). Fighting misinformation on social media using crowdsourced judgments of news source quality. *Proceedings of the National Academy of Sciences*, *116*(7).

[77] Diósi, S. (2024). *Mesterséges intelligencia, szintetikus valóság. Az MI és GenMI rendszerekkel kapcsolatos globális kihívások és európai szabályozási stratégiák (disszertáció)*. Pécsi Tudományegyetem.

[78] Rasak, M. J. (2021). Event Barraging and the Death of Tactical Level Open-Source Intelligence. *Military Review*, 48-57.

[79] Hewson, J. (2023. március 2.). *A Private Company Is Using Social Media to Track Down Russian Soldiers*. Foreignpolicy.com. Elérhető: https://foreignpolicy.com/2023/03/02/ukraine-russia-war-military-social-media-osint-open-source-intelligence/ utoljára letöltve: 2024.04.09.

[80] Penninger, R. (2019. január 14.). Operationalizing OSINT Full-Spectrum Military Operations. *Small Wars Journal*. Elérhető: https://archive.smallwarsjournal.com/jrnl/art/operationalizing-osint-full-spectrum-military-operations utoljára letöltve: 2024.04.09.

[81] Somogyi, Z. M. (2021). A második hegyi-karabahi háború katonai szemszögből 1. *Honvédségi Szemle*, *149*(5), 35-47.

[82] Field, M. (2019. február 19.). NATO researchers used social media to learn details of a military exercise and manipulate troops. It wasn't very hard to do. *Bulletin of the Atomic Scientists*. Elérhető: https://thebulletin.org/2019/02/nato-researchers-used-social-media-to-learn-details-of-a-military-exercise-and-manipulate-troops-it-wasnt-very-hard-to-do/ utoljára letöltve: 2024.04.09.

[83] Al-Rawi, A. K. (2014). Cyber warriors in the middle east: The case of the syrian electronic army. *Public Relations Review*, *40*(3), 420-428.

[84] Cluley, G. (2015. április 9.). *French TV network taken off air after attack by pro-ISIS hackers*. Elérhető: https://www.tripwire.com/state-of-security/french-tv-channel-hacked-off-air utoljára letöltve: 2024.04.09.

[85] Alexander, D. E. (2014). Social media in disaster risk reduction and crisis management. *Science and engineering ethics*, *20*(3), 717-733.

[86] Bratu, S. (2016). The critical role of social media in crisis communication. *ResearchGate*, 232-238.

[87] Nakashima, E. (2019. február 26.). U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms. *Small Wars Journal*. Elérhető: https://smallwarsjournal.com/2019/02/26/us-cyber-command-operation-disrupted-internet-access-russian-troll-factory-day-2018-midterms/ utoljára letöltve: 2024.04.09.

[88] Varga, F. (2024). A KÖZÖSSÉGI MÉDIA KÖZIGAZGATÁSI ALKALMAZÁSÁNAK LEHETŐSÉGEI ÉS AZOK MÉRHETŐSÉGE. *KözigazgatásTudomány*, (2), 140–161.

[89] Mayfield III, T. D. (2011). A Commander's Strategy for Social Media. *Joint Force Quarterly*, *60*(7).

[90] Chouhan, P. K. a. G. S. A. (2024). Deception Technology for Active Defence: Background and Opportunities. *IEEE International Conference on Communications Workshops (ICC Workshops)*.

[91] Canham, M., & T. J. (2022). Planting a poison SEAD: Using social engineering active defense (SEAD) to counter cybercriminals. In *International Conference on Human-Computer Interaction* (pp. 48-57). Springer International Publishing.

[92] Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In *Proceedings of the 7th European Conference on Information Warfare* (p. 163). Academic Publishing Limited.

[93] spacewar.com. (2008. május 14.). *CYBER WARS NATO launches cyber defence centre in Estonia*. Elérhető: https://www.spacewar.com/reports/NATO_launches_cyber_defence_centre_in_Estonia_999.html utoljára letöltve: 2024.04.09.

[94] Maisaia, V., Guchua, A., & Zedelashvili, T. (2020). The cybersecurity of Georgia and threats from Russia. *Eastern Review*, *9*(1), 105-119.

[95] Lange-Ionatamishvili, E., Svetoka, S., & Geers, K. (2015). *Strategic communications and social media in the Russia Ukraine conflict*. NATO Strategic Communications Centre of Excellence.

[96] Whitehead, D. E., et al. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In *2017 70th Annual conference for protective relay engineers* (pp. 1-8). IEEE.

[97] Greenberg, A. (2020). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Random House USA.

[98] Lee, R. M. A. M. J. C. T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity ISAC – SANS Report*. EISAC.

[99] Ziegler, C. E. (2018). International dimensions of electoral processes: Russia, the USA, and the 2016 election. *International Politics*, *55*(5), 557-574.

[100] Nance, M. (2016). *The plot to hack America: How Putin's cyberspies and WikiLeaks tried to steal the 2016 election*. Simon and Schuster.

[101] Christian, J. D. (2020). *Russian Cyber Operations to Destabilize NATO (disszertáció)*. Naval Postgraduate School.

[102] Krasznay, C. (2020). Case study: The notpetya campaign. *Információ és kiberbiztonság*, 485-499.

[103] Rácz, A. (2015). *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*. The Finnish Institute of International Affairs.

[104] Jaitner, M. (2015). *Russian Information warfare of 2014*. NATO CCD COE Publications.

[105] Doroshenko, L., & Lukito, J. (2021). Trollfare: Russia's disinformation campaign during military conflict in Ukraine. *International Journal of Communication*, *15*(8).

[106] Holloway, M. (2017. május 10.). *How Russia Weaponized Social Media in Crimea*. Elérhető: https://thestrategybridge.org/the-bridge/2017/5/10/how-russia-weaponized-social-media-in-crimea utoljára letöltve: 2024.04.09.

[107] York, J. (2023. február 24.). *'World's first TikTok war': Ukraine's social media campaign 'a question of survival'*. Elérhető: https://www.france24.com/en/europe/20230224-world-s-first-tiktok-war-ukraine-s-social-media-campaign-a-question-of-survival utoljára letöltve: 2024.04.09.

[108] Tiffany, K. (2022. március 10.). *The Myth of the 'First TikTok War'*. Elérhető: https://www.theatlantic.com/technology/archive/2022/03/tiktok-war-ukraine-russia/627017/ utoljára letöltve: 2024.04.09.

[109] Johansson-Nogués, E. Ş. E. (2023). Fabricating a war? Russian (dis)information on Ukraine. *International Affairs*, *99*(5), 2015–2036.

[110] De Guzman, C. (2024. szeptember 17.). *Meta Is Globally Banning Russian State Media on Its Apps, Citing 'Foreign Interference*. Elérhető: https://time.com/7021897/meta-facebook-instagram-whatsapp-rt-russian-state-media-global-ban/ utoljára letöltve: 2024.04.09.

[111] Xu, W., et al. (2025). Social media warfare: investigating human-bot engagement in English, Japanese and German during the Russo-Ukrainian war on Twitter and Reddi. *EPJ Data Science*, *14*(10).

[112] Shahi, G. K., & Mejova, Y. (2025). Too Little, Too Late: Moderation of Misinformation around the Russo-Ukrainian Conflict. In *Proceedings of the 17th ACM Web Science Conference 2025*.

[113] West, D. M. (2023. október 12.). *Posting murder on social media platforms*. Elérhető: https://www.brookings.edu/articles/posting-murder-on-social-media-platforms/ utoljára letöltve: 2024.04.09.

[114] Gilbert, D. (2024. október 22.). *The Shitposting Cartoon Dogs Sending Trucks, Drones, and Weapons to Ukraine's Front Lines*. Elérhető: https://www.wired.com/story/nafo-ukraine-russia-war/ utoljára letöltve: 2024.04.09.

[115] Ciuriak, D. (2022). *The Role of Social Media in Russia's War on Ukraine*.

[116] Weatherbed, J. (2023. október 20.). *Blue checkmarks on X are 'superspreaders of misinformation' about Israel-Hamas war*. Elérhető: https://web.archive.org/web/20231020203856/https://www.theverge.com/2023/10/20/23925086/x-verified-blue-checkmarks-superspreader-misinformation-israel-hamas-war utoljára letöltve: 2024.04.09.

[117] Karagiorgos, G. K. C. C. P. I. (2023). *Gaza Through Whose Lens? Breaking Apart U.S. Coverage of the Israel-Hamas War*. Elérhető: https://features.csis.org/gaza-through-whose-lens/index.html utoljára letöltve: 2024.04.09.

[118] Európai Unió. (2022). *(EU) 2022/2065 rendelet a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (a digitális szolgáltatásokról szóló rendelet)*.

[119] Gerasimov, V. (2016). The Value of Science Is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. *Military Review*, 23-29.

[120] European Commission. (2025). *A dezinformáció visszaszorítását célzó magatartási kódex*. Elérhető: https://digital-strategy.ec.europa.eu/hu/library/code-conduct-disinformation utoljára letöltve: 2024.04.09.

[121] OECD. (2024). *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*. OECD Publishing.

[122] UNESCO. (2023). *Guidelines for regulating digital platforms: A multistakeholder approach to safeguarding freedom of expression and access to information*.

[123] OHCHR. (2021). *Disinformation and Freedom of Opinion and Expression. Report of the UN Special Rapporteur on Freedom of Expression (Irene Khan), A/HRC/47/25*. United Nations OHCHR.

[124] Douek, E. (2021). Governing Online Speech: From 'Posts-as-Trumps' to Proportionality and Probability. *Columbia Law Review*, *121*(3), 759–832.

[125] OECD. (2022). *Building Trust and Reinforcing Democracy: Preparing the Ground for Government Action*. OECD Public Governance Reviews. OECD Publishing.

[126] MacCarthy, M. (2022. december 21.). *COMMENTARY U.K. government purges "legal but harmful" provisions from its revised Online Safety Bill*. Elérhető: https://www.brookings.edu/articles/u-k-government-purges-legal-but-harmful-provisions-from-its-revised-online-safety-bill/ utoljára letöltve: 2024.04.09.

[127] Pamment, J. (2020). *The EU's role in fighting disinformation: taking back the initiative*. Carnegie Endowment for International Peace.

[128] NATO. (2025. február 3.). *NATO's approach to counter information threats*. Elérhető: https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats utoljára letöltve: 2024.04.09.

[129] HM Government. (2023). *Online Safety Act 2023*. HM Government (legislation.gov.uk).

[130] Európai Bizottság. (n.d.). *A demokrácia védelme*. Elérhető: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy_hu utoljára letöltve: 2024.04.09.

[131] Lewandowsky, S. v. d. L. S. (2021). Countering Misinformation and Fake News through Inoculation and Prebunking. *European Review of Social Psychology*, *32*(1), 348–384.

[132] Roozenbeek, J. v. d. L. S. (2019). The fake news game: actively inoculating against the risk of misinformation. *Journal of Risk Research*, *22*(5), 570–580.

[133] Roozenbeek, J. S. C. R. D. S. K. J. F. A. L. J. R. G. v. d. B. A. M. v. d. L. S. (2020). Susceptibility to misinformation about COVID-19 around the world. *Royal Society Open Science*, *7*(10).

[134] Bateman, J. J. D. (2024). *Countering Disinformation Effectively: An Evidence-Based Policy Guide*. Carnegie Endowment for International Peace.

[135] Guess, A. N. J. T. J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*, *5*(1).

[136] Calvo, D., et al. (2021). Countering disinformation: improving the Alliance's digital resilience. *NATO Review*, (8).

[137] Chesney, R. C. D. (2019). Deepfakes and the New Disinformation War. *Foreign Affairs*, *98*(1), 147-155.

[138] Verdoliva, L. (2020). Media Forensics and Deepfakes: An Overview. *IEEE Journal of Selected Topics in Signal Processing*, *14*(5), 910-932.

[139] Fehér, A. T. N. I. (2021). Mesterségesintelligencia-alapú kibertértámadási modellek. *Műszaki Katonai Közlöny*, *31*(3), 73-87.

[140] Pomerlau, M. (2023. május 26.). *DOD sends new cyber strategy to Congress, releases unclassified fact sheet*. Elérhető: https://defensescoop.com/2023/05/26/dod-sends-new-cyber-strategy-to-congress-releases-unclassified-fact-sheet/ utoljára letöltve: 2024.04.09.

[141] Nakashima, E. (2019. február 26.). *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterm*. Elérhető: https://smallwarsjournal.com/2019/02/26/us-cyber-command-operation-disrupted-internet-access-russian-troll-factory-day-2018-midterms/ utoljára letöltve: 2024.04.09.

[142] HM Government. (2021). *Global Britain in a competitive age*. UK Government.

[143] European Council. (2019. május 19.). *A Europe that protects: good progress on tackling hybrid threats*. Elérhető: https://ec.europa.eu/commission/presscorner/detail/en/ip_19_2788 utoljára letöltve: 2024.04.09.

[144] Lasconjarias, G. L. J. A. (2019). *NATO's Response to Hybrid Threats*. NATO Public Diplomacy Division.

[145] Hadnagy, C. J. (2011). *Social Engineering: The Science of Human Hacking*. Wiley.

[146] Eset. (n.d.) Malware – Rosszindulatú alkalmazások. itt: https://www.eset.com/hu/malware/#:~:text=A%20malware%20kifejezés%20a%20„malicious”%20(rosszindulatú)%20és,áldozatokra%2C%20hogyan%20viselkedik%20vagy%20milyen%20kárt%20okoz. utoljára letöltve: 2026.04.06.

[147] Lexiq.hu. (n.d.) RSS. itt: https://lexiq.hu/rss utoljára letöltve: 2026.04.06.

MELLÉKLETEK

I. A kérdőív kérdései és adható válaszok

Demográfiai adatok

1. Neme (csak egy válasz lehetséges)

◯ Nő

◯ Férfi

◯ Nem szeretnék válaszolni

2. Kora (csak egy válasz lehetséges)

◯ 18–24

◯ 25–29

◯ 30–35

◯ 36–40

◯ 41–45

◯ 46–50

◯ 50 év felett

3. Ön hol él? (csak egy válasz lehetséges)

◯ Főváros

◯ Nagyváros

◯ Kisváros

◯ Község

◯ Falu

Platformhasználati szokások

7. Milyen gyakran használja a közösségi média platformokat?

◯ Naponta több órát

◯ Naponta egy órát

◯ Hetente néhány órát

◯ Ritkábban

8. Milyen célokra használja a közösségi médiát? (több válasz is lehetséges)

◯ Kommunikáció családdal, barátokkal

◯ Hírolvasásra

◯ Érdeklődési körbe tartozó oldalak követésére

◯ Egyéb szórakozásra

9. Mely platformokat használja? (több válasz is lehetséges)

◯ Facebook

◯ Instagram

◯ Snapchat

◯ Twitter (X)

◯ TikTok

◯ VK

◯ YouTube

◯ Reddit

10. Melyiken találkozott a legtöbb gyanús tartalommal? (több válasz is lehetséges)

◯ Facebook

◯ Instagram

◯ Snapchat

◯ Twitter (X)

◯ TikTok

◯ VK

◯ YouTube

◯ Reddit

Tudatosság – Hallott-e már róla?

Az információs műveletek olyan **tudatosan megtervezett és összehangolt tevékenységek összessége**, amelyek célja az egyének vagy közösségek **gondolkodásának, döntéshozatalának, érzelmeinek és viselkedésének befolyásolása**. Ezek az akciók **a kognitív, technikai és fizikai térben** egyaránt zajlanak, és jellemzően **stratégiai vagy politikai célokat** szolgálnak – például a közvélemény manipulálását, a társadalmi stabilitás megingatását, vagy katonai műveletek támogatását.

Az információs műveletek során gyakran használnak **digitális platformokat**, különösen a **közösségi médiát**, ahol a dezinformáció, propaganda, pszichológiai hadviselés (PSYOPS), trollhálózatok, botok, és a deepfake technológiák **kulcsszerepet játszanak**. Ezek lehetnek állami vagy nem állami szereplők által végrehajtott kampányok, amelyek célja gyakran a **semleges célcsoportok meggyőzése vagy manipulálása**.

11. Hallotta már az „információs műveletek” kifejezést a közösségi médiában?

◯ Igen

◯ Nem

◯ Talán

12. Találkozott valaha a közösségi média platformjain végzett információs műveletekkel?

◯ Igen

◯ Nem vagyok benne biztos

◯ Nem

13. Mennyire aggódik az információs műveletek közösségi médiára gyakorolt hatása miatt?

1–5 skála:

1 = Egyáltalán nem aggódom

5 = Nagyon aggódom

14. Ön szerint mi lehet egy információs művelet célja? (több válasz is lehetséges)

◯ Közvélemény manipulálása

◯ Választások befolyásolása

◯ Gazdasági haszonszerzés

◯ Diplomáciai érdekérvényesítés

◯ Társadalmi feszültség keltése

◯ Politikai narratívák terjesztése

◯ Katonai megtévesztés

Felismerési képesség – Kognitív észlelés

15. Mennyire biztos abban, hogy képes azonosítani és megkülönböztetni a valódi és a manipulált tartalmat a közösségimédiában?

1–5 skála

16. Mennyire biztos abban, hogy képes azonosítani az álhíreket?

1–5 skála

17. Jelentett vagy jelölt már gyanús tartalmat?

◯ Igen

◯ Nem

◯ Talán

18. Mit tesz, ha gyanús tartalmat lát? (több válasz is lehetséges)

◯ Továbbosztja

◯ Kommentel

◯ Jelenti

◯ Üzenetben továbbküldi

◯ Elgörget

◯ Megnyitja a forrást

◯ Nem foglalkozik vele

19. Melyik állítás tűnik hamisnak vagy manipuláltnak? (kritikai gondolkodás teszt)

◯ NATO MI-vel manipulálja a lakosságot

◯ Deepfake-eket már minden platform felismeri

◯ Társadalmi megosztottság fokozása választások előtt

Hozzáállás és attitűd

20. Ön szerint kik a felelősek az információs műveletekért? (több válasz is lehetséges)

◯ Felhasználók

◯ Platformüzemeltetők

◯ Politikusok

◯ Katonai/félkatonai szervezetek

◯ Újságírók

◯ Trollok

21. Ön szerint a közösségi média cégeknek nagyobb felelősséget kellene vállalniuk az információs műveletek megelőzésében és kezelésében?

◯ Igen

◯ Nem

◯ Nem tudom

22. A kormányoknak szerepet kell-e vállalniuk a közösségi média platformokon folyó információs műveletek szabályozásában?

◯ Igen

◯ Nem

◯ Talán

23. Ön szerint az információs műveletek célzottan mely csoportokat próbálnak befolyásolni? (több válasz is lehetséges)

◯ Gyerekek

◯ Fiatal felnőttek

◯ Idősek

◯ Politikai aktivisták

◯ Semleges lakosság

◯ Katonák

Oktatás és edukáció

24. Ön szerint az oktatási és figyelemfelkeltő kampányok segíthetnek a felhasználóknak jobban azonosítani és reagálni aközösségi médiában végzett információs műveletekre?

◯ Igen

◯ Nem

◯ Talán

25. Ön szerint az iskolai oktatás részévé kéne tenni a felelős internet használatot, benne az információs műveletekről szólókampányokat?

◯ Igen

◯ Nem

◯ Talán

26. Szeretne többet megtudni a manipulált tartalmak felismeréséről?

◯ Igen, mindenképp

◯ Igen, ha rövid és közérthető anyag

◯ Talán

◯ Nem

◯ Már jól felismerem

Nyitott kérdések (opcionális)

Írja le:

27. Írjon le egy példát, amikor manipulált információval találkozott közösségi médiában!
28. Mit tartana leghatékonyabb eszköznek az információs műveletek elleni fellépéshez?

I. Interjú Dr. Haig Zsolttal

1. Hogyan definiálná az „információs műveleteket” a modern hadviselés kontextusában?

Nekem vannak a mainstreamtől, akár még a doktrínális megfogalmazásoktól eltérő nézeteim az információs műveletekről. Úgyhogy, az a fajta megközelítés, ami jelen pillanatban a NATO-ban van, és ami felé megy a Magyar Honvédség is, hiszen készül épp egy MH Összhaderőnemi Információs Műveleti Doktrína, és én úgy látom, hogy az a fajta koncepció, ami megszületett 2023-ban a legújabb NATO doktrínával, aminek a lényege, hogy a STRATCOM irányít, és alapvetően az információs műveletek arra szolgál, hogy hogyan lehet a közvéleményt befolyásolni és alakítani, amivel nincs is probléma, hiszen ez egy ténylegesen valid koncepció és meghatározás, de egy dolgot felejtettek el: 2023 február óta zajlik egy orosz-ukrán háború, ahol a mélyben látszik, hogy nagyon komoly információs műveleti kampányok/tevékenységek is zajlanak minden téren. A NATO és a készülő magyar doktrína abba a hibába esett, hogy megmaradt abban a nyugodt légkörben, ami a megelőző 20 évet jellemezte. Ez a béketámogató, békefenntartó, béketeremtő műveletek végrehajtása és azok információs műveleti támogatása, amikor az ellenség legfeljebb látens, vagy hibrid esetben „semleges érintettek” vannak, tehát ezen műveletek fő hangsúlya azon van, hogy hogyan lehet megnyerni vagy befolyásolni, manipulálni a közvéleményt. Viszont a háborús körülmények között, ahol valós ellenségek állnak szemben, ott, bár létezik a befolyásolás, de a sikeressége (pl orosz és ukrán felek között) alacsony lesz, nem fogják tudni egymás meggyőzni arról, hogy ez egy legális háború, vagy épp arról, hogy nem, és ez a régóta folyó ideológiai befolyásolásnak köszönhető. Ebben az esetben a befolyásolás a semleges érintettekre lesz kihegyezve, ahol a támogatás megnyerése a fő cél.

Azt felejtik el, hogy a harctéren vannak további információs műveleti tevékenységek, amik nyilván kevésbé látványosak. Az információs műveleteknek van egy kognitív vonzata és egy technikai/technológiai vonzata. A kognitívra helyezik most a fő hangsúlyt a doktrínális koncepciók és a technikai részről elfeledkeznek. Ennek a fő oka az, hogy a technikai vonzata a semleges érintettekre nem vonatkozik. Nem akarnak senkit (semleges felet) megzavarni, lehallgatni, nem akarnak senkinek a számítógépes rendszerébe behatolni és tönkretenni, vagy adatbázisokat törölni, vagy információs célpontokat megsemmisíteni, amik valós információs műveleti tevékenységek, de ezek mind-mind a

technikai képességek körébe sorolhatók, és ezek háborús műveletekben egyértelműen létező és alkalmazott tevékenységek, jelenleg is csinálják. Most is vezetési pontokat, információs célpontokat, olyan infrastruktúrákat, amelyek nagy mértékben befolyásolják az információs társadalom működését, sorra pusztítanak el. Amellett, hogy vasúti csomópontokat és minden egyéb más célpontot is támadnak a fizikai térben.

Működik a kibertámadási rész. Már a háború megindítása előtt is, és azóta is folynak ezek a kampányok. Működik az elektronikai támadás. Igen komoly eszköz parkkal rendelkezik mindkét fél és jelentős ilyen jellegű támadó tevékenységek zajlanak éppen.

Summa summárum, az én véleményem és definícióm eltér attól a doktrinális meghatározástól, ami egyértelműen besorolja a stratcom alá, bár nyilvánvaló kapcsolódások vannak a stratcommal, mert a politikai és stratégiai narratívának a közlése és terjesztésére jó eszköz az infoops (lasd: psyops, PR, cimic, mis- és desinformation). De mindeközben a doktrínákban az ellentevékenység vagy védelem legfeljebb 1-2x szerepelnek, vagy a kibertámadások és elektronikai támadások is egy-egy bekezdésnyi szerepet kaptak. Tehát el van tolódva az egész történet, holott mire találták ki az információs műveleteket a 90-es évek elején és jelent meg az első doktrína 96-ban? Hogy ezeket a különböző területeken és szinteken lévő információs műveleti tevékenységeket összehangolja és koordinálja és ezáltal egy olyan erősokszorozó képességet alakítson ki a szingergiák következtében, ami a célok eléréséhez sokkal könnyebben elvezet. De, hogyha az egyik oldalt negligáljuk, mert nem veszünk róla tudomást, vagy csak megemlítjük, az elveszi a lényegét az információs műveleteknek, ami az, hogy az információs tevékenységeket hogyan fogjuk tudni összehangolni a műveletekben.

Tehát amikor én ezekről (tehát az információs műveletekről) gondolkodom, azt mondom, hogy az információs környezetben, tehát az információs, fizikai és kognitív térben zajló olyan információs tevékenységek összessége, ami alapvetően a műveleteket támogatja, mégpedig olyan módon, hogy kognitív technikákkal és módszerekkel közvetlenül hat az emberi gondolkodásra, vélekedésre, viselkedésre; a technikai módszerekkel meg közvetetten, azért, mert elveszi tőle az eszközt, mert nem tud rádiózni, nem tudja használni a számítógépét, nem működik a harcálláspont, amitől a parancsnok ideges lesz és kognitív hatások jönnek létre, ezáltal kedvezőtlenül hat a döntési folyamatokra is. Tehát ezzel a két területtel gyakorol hatásokat a célközönségre, ami egyszerre az ellenség, a saját erő és a semleges érintett; ezáltal támogatva a katonai műveleteket.

2. Milyen szerepet játszik a pszichológiai hadviselés az információs műveletekben?

A válasz az, hogy jelentős. A pszichológiai műveletek, a PSYOPS, jelentősek. Régen egyébként az amerikaiak is hadviselésként, PSYWAR-ként hivatkoztak rá, de ennek volt egy olyan negatív oldalága, amit manapság úgy emlegetünk, hogy fekete PSYOPS. Ez annyit tesz, hogy nem valós tényeken alapuló álhírekkel próbálunk meg propagálni és befolyásolni. A NATO megfogalmazása szerint a PSYOPS az valós tényeken alapuló befolyásolást jelent és azt kell megnézni, hogy ez milyen módon tudom felépíteni abból a célból, hogy a közvéleményt a leghatékonyabban el lehessen érni és magammellé állítani. A manipuláció, az álhír terjesztés pedig nem ez a kategória, hanem a megtévesztésé.

A lélektani műveletek, vagy pszichológiai műveletek legalább annyira fontos részét képezik az információs műveleteknek, mint a civil-katonai műveletek, a műveleti biztonság, az elektronikai hadviselés, vagy a kibertámadások. Pont az a lényege, hogy nem teszünk különbséget, de lehetnek olyan fázisai vagy időszakai a háborúnak, vagy az adott műveletnek, amikor egyik képesség jobban előtérbe kerül.

Keresztkérdés: Tehát akkor az csak egyfajta percepció, hogy a pszichológiai műveletek vannak előtérben, mert azt jobban látjuk, többször halljuk a médiában és kevésbé látjuk a többi információs műveletet?

Válasz: igen és van is ennek egy negatív leképződése a Magyar Honvédségben, mert például a területek szét vannak szórva a Honvédségen belül, és gyakran külön említik a PSYOPS-ot az információs műveletektől. Ennek az a hátránya, hogy az információs műveletek nicnsenek egyben kezelve, így soha nem működnek a szinergiák és nem lesz igazi együttműködés.

Tehát a psyops igenis fontos. Afganisztánban például a psyops és cimic feladatokon volt a hangsúly. Ott nem volt lehetőség és szükség se elektronikai- vagy kibertér műveletekre, mert a tálibok füstjelekkel kommunikáltak. Mindig a művelet célja és a műveleti környezet dönti el, hogy mi a fontos. A lényeg, hogy hogyan tudjuk ezeket egymással összehangolni és koordinálni egy végcél érdekében.

3. Hogyan tudják az államok összehangolni a támadó információs műveleteket az etikai megfontolásokkal?

Mindig az a kérdés, hogy miylen célok érdekében hajtjuk végre az információs műveleteket, és milyen környezetben hajtjuk végre azokat. Az orosz-ukrán háborúban az etikai megfontolások egy x-ed rangú kérdés, ha megnézzük, akkor szóba sem kerül. A cél szentesíti az eszközt: mi az, amit meg tudok tenni, mivel tudom a másikat hatékonyan befeketíteni, manipulálni, milyen támadó és védekező képességet tudok alkalmazni. Akkor, amikor mondjuk békeidőben alkalmaznak infoopsot, pl politikai beavatkozások, ott próbálják elrejteni ezt a dolgot, letagadni, nincsenek morális megfontolásaik azoknak, akik ezt végrehajtják. Gerasimov egyértelműen ki is jelentette, hogy békétől békéig mindent kell használni. Ott van benne, hogy a kezdet kezdetétől információs műveleti kampányokat kell végrehajtani, és ezekben minden eszköz használható a cél elérésére. Persze vannak nemzetközi egyezmények, amelyeket figyelembe kell(ene) venni, de pont az információs műveletek egy olyan tevékenység, ami nem megfogható és a nemzeti vagy nemzetközi jog alapján nem lehet szankcionálni vagy szabályozni. Etikai és morális megfontolások pedig nincsenek. Például nézzük meg Trumpot, aki egy tönk szélén álló, félig lerombolt országot most lerabolna nemesfémekkel a további segítségért cserébe.

Keresztkérdés: Van vagy látható közeléségben van-e bármilyen információs műveleti nemzetközi jogi érvényű egyezmény? Van-e a genfi egyezményhez hasonlóan valami, ami meghatározza a vörösvonalakat az információs műveletekben?

Válasz: Én nem láttam ilyet és a kinetikus műveletek esetében a fegyverek megfoghatóak, míg az információs műveletek nem az. De itt is különbséget lehetne tenni technikai és kognitív megoldásokban. Az elektronikai támadások, az információs célpontok megsemmisítése például beletartozhat a már meglévő szabályok alá, pl. milyen esetben lehet fegyvert használni, és ebben az esetben teljesen mindegy, hogy valaki élő erőt pusztít, vagy radarokat. A drasztikus, fizikai hatások szabályozva vannak. A kognitív része viszont abszolút nincs és nem is látok arra példát, vagy törekvéseket, hogy ezt valamilyen módon megpróbálják szabályozni. Az EU-nak vannak ajánlásai az álhír terjesztésre, illetve az álhírekre való felkészítésre és szűrésre.

Én: De a közösségi média platformok ezt pont most szabotálják el

HZs: Igen, pedig a mesterséges intelligenciának vannak olyan lehetőségei, amik ezt segítsék, de a közösségi média platformok számára ez kontraproduktív lenne, mert akkor

rengeteg információ nem jelenne meg, pedig az ő céljük az, hogy minél több poszt kerüljön ki.

Én: Pedig eddig az volt a cél, hogy mindenkit a saját kis vélemény buborékjába zárjanak és ezt marketing szempontból kimaxolják a hírdető márkák számára. Eddig mindenki a saját híreit látta, a saját politikai véleményének megfelelő politikusok fizetett hirdetéseit, a kedvenc márkáját, illetve olyan termékeket, amiket feltételezhetően szeretne megvenni az eddigi aktivitása alapján. Ehhez képest megborultak a feedek és olyan dolgokat dobál be, amik nem relevánsak.

HZs: És mindeközben, ami nem tetszik, azt letiltják.

Az a lényege a közösségi médiának, hogy bárki bármit leírhat.

4. Melyek a legnagyobb kihívások az álhírek és dezinformáció elleni küzdelemben katonai konfliktusok során? Ha civilt fel kell készíteni, akkor a katonát mégjobban.

A katonának van bőven más dolga és az, hogy honnan érkezik neki az információ (parancsnoki lánc), az egy szűrőt jelent. Nem feltétlenül jó, ha a műveletekben résztvevő katona kezében ott a mobiltelefon és az internet és minden információhoz hozzáfér, mert a katona számára az egyik alapvető elv az, hogy a parancs határozza emg a tevékenységét, minden más másodlagos. Nem jó, ha a kapott parancs konfliktusos a világból érkező információkkal, és lehet, hogy amit olvas nem is valós tény. Én azt tartanám jó megoldásnak, ha ez szabályozva lenne, hogy ez hogyan érhető el, az egy másik kérdés. Mondhatnánk azt is, hogy kap mindenki egy egyszerű mobiltelefont, amivel csak telefonálni lehet és nem alkalmas internetezni vagy közösségi médiát használni. A másik oldala viszont az, hogy a katonák által készített felvételek, bejelentkezések, posztok közelebb hozzák a háborút az emberekhez. Manapság már, hogy a normál média már fasorban sincs már időben és real-timeban ahhoz képest, amit a harctérről rögtön feltöltenek. Meg kell nézni hány olyan OSINT oldal van, ahonnan a nagy újságok hivatkozzák a veszteségeket. A katonáknál, akik ténylegesen harcolnak be kellene korlátozni az eszköz használatot. A közösségi média előtt röplapokon terjesztették a dezinformációt, és a katonáknak tiltott volt ezeket elolvasni, hogy ne rombolják a morált. Nem változott semmi, csak a technológia.

5. Hogyan változott a közösségi média szerepe az információs műveletekben az elmúlt években?

96 az első doktrína megjelenése, közösségi médiát még hírből sem ismertünk, internet már volt, de nem tulajdonítottunk neki ekkora jelentőséget. A közösségi média megjelenése alapjaiban forgatta fel a közvélemény manipulációjára és alakítására irányuló törekvéseket. Azok a technikák, amik korábban léteztek mára abszolút háttérbe szorultak. A közösségi médián mindent szabad, konzekvenciák nélkül, és ezt ki is használják. Soha nem látott mértékben nőtt meg az információ terjesztés sebessége és soha nem látott mértékű tömegeket lehet elérni. Kontroll nélküli az üzenet továbbítás. Ezek korábban nem léteztek és a következmények beláthatatlanok.

Kommenteléshez: Mindenki mindent írhat, mindenki mindenről véleményt nyilváníthat és tényellenőrzés nélkül továbbközölhet vagy terjeszthet. Az sem mindegy, hogy kihez hogyan szólok hozzá és azt Ő hogyan tudja értelmezni. Itt teljesen elválik az, hogy az adott személynek milyen az iskolázottsági szintje, viszont ettől teljesen függetlenül ugyanúgy tudja egy alacsonyabban iskolázott alakítani a közvéleményt és nem érdekli, hogy más tényszerűen, hivatkozásokkal alátámasztva bizonyít valamit, mert megvan győződve a saját igazáról, mert más azt mondta, hogy ez így van, és ha ő mondta, akkor az biztos igaz. És a világ alakulása is ezt támasztja alá. Trump előretörése is annak köszönhető, hogy ezeket az embereket és segítségükkel a közvéleményt hogyan lehetett tovább manipulálni.

6. Milyen intézkedéseket kell hozni a katonai kommunikáció kibertámadásokkal szembeni védelme érdekében?

Attól függ, hogy mit értünk katonai kommunikáció alatt. Ha a távközlési hálózatokat nézzük, akkor: maguk a kiberképességek sokkal szélesebb kört ölelnek fel, mint szimpla szoftveres támadások. Ugynais azt kell megnézni mi a kibertér és abban hogyan jelennek meg az eszközök és megoldások. Egyre több a hálózatos technológia, amiben a kommunikációs platform az információt továbbítja akár gép-gép, gép-ember vagy ember-ember között. Ezek a rendszerek, főleg, ha vezetéknélküli rendszerekről van szó, érintik az elektromágneses teret, tehát ezek támadási lehetőségei rendkívüli mértékben kiszélesednek. A lehallgatáson és zavaráson túl, a hálózatos technológiákból fakadóan, különböző kiberképességekkel és szoftveres támadásokkal is le lehet ültetni egy rendszert. Pl a wifi elérhetetlenné ttétel megodlható szoftveres DDoS támadásokkal is.

Sok megoldás, akár szoftveres vagy hardveres megodlások is léteznek, mint vírusvédelem, biztonsági szoftverek, lehet az elektronikai védelmi megoldások és feltörekvő technológiák alkalmazásával (pl zaj-alatti sugárzás), de ide tartozik a titkosítás és rejtjelzés is, amit szintén szoftveresen meg lehet oldani, akár valós időben törhetetlen alaklmazásával.

A másik a felhasználó felkészítése és a tudatosság növelése. Pl Krím-annexiója: elromlottak az ukrán rádiók és elkezdtek mobiltelefont használni, amivel a bázis állomásokon keresztül bemérhetőek lettek.

Én: igen, erre szerettem volna kitérni, hogy ha az állomány egymásközötti kommunikációjáról vagy mégrosszabb: feladatszabásról van szó, azt hogyan mentsük meg a manipulációtól (értsd szervek viberen terveznek-szerveznek-feladatotszabnak, de egyre elterjedtebb a Signal, mert kiváló a titkosítása, de az orosz hackerek újonnan szeretik törni a Signal fiókokat). Tehát kiküszöbölhető-e az, hogy egy ponton mondjuk a Honvédség rádiói elromlanak vagy kiiktatják őket, és megkezdődik a pl Signalon történő feladatszabás, de ez mondjuk ne növelje a kitettséget?

HZs: De ez mindig így működik. Kitalálnak egy védelmet és hamarosan megszületik rá a támadási forma. Az oroszoknak is van egy rendszere, a Leer, ami egy drón, ami arra jó, hogy átveszi a bázisállomás szerepét és a földi kapcsolatok erre futnak be és innentől lehallgatható lesz a kommunikáció. Ha ezeket az eszközöket katonai célokra kezdik használni, az bizony komoly problémákat okozhat a híradónak. A katonai kommunikáció egyik legfontosabb niztonsági rendszabálya, hogy titkos információt tilos nyílt csatornán közvetíteni, ha ezt abban a hiszemben csinálja, hogy ezt mobiltelefonon teszi, ami egy viszonylag jól védett eszköz, mert nehezebben lehallgatható pl a közeghozzáférési technikák miatt, de hogyha átveszik az irányítást, akkor innentől kezdve lehallgathatóvá válik. Mindent meg lehet fogni, úgyhogy nagyon óvatosan kell bánni azzal, hogy a civil kommunikációs eszközöket és platformokat milyen módon használjuk információ továbbítására. Amíg ez teljesen jól működött a dél-szláv válságban, mert mikor a NATO ellehetetlenítette a szerb katonai rádiók működését zavarással, a szerbek elkezdtek mobiltelefonnal kommunikálni, ennek a zavarására nem volt képessége a NATO-nak akkor.

7. Hogyan mérhető az információs műveletek hatékonysága a közvélemény befolyásolása szempontjából?

Ez egy jó kérdés. Nem egy egzakt dolog. A technológiai oldala mérhető. Meg tudom mondani, hogy hány eszközöm van és hány eszközt zavartam meg, hány hálózat esett szét, hol nem működik a vezetésirányítási rendszer. Az, hogy a kognitív hatások hogyan jelentkeznek és milyen módon tudtuk elérni a tervezett eredményt gyakran nem ilyen egyértelmű. A technológiai hatás azonnal jelentkezik: vagy kommunikál vagy nem. Egy PSYOPS művelet hatása lehet,hogy csak napok vagy hetek múlva jelentkezik. A kognitiív térben való hatások eléréséhez idő kell. Nem várom el, hogy azonnali elfogadásra találjon az üzenet, de ha jól van megkomponálva, akkor idővel lesz látszatja, sokkal hosszabb érési ideje van, de ez nagyon nehezen mérhető.

8. Hogyan befolyásolja a mesterséges intelligencia elterjedése az információs műveleteket?

Rendkívüli mértékben. A hangsúly a felismerésen van, hogy hogyan lehet az egyszerű embert, akinek ezek szólnak, felkészíteni a felismerésre, hogy ne vegye készpénznek, hogy ezt a Putyin mondta, akkor megtörtént.

De nem csak a psyopsban, de más információs műveletekben is képes hatékonyságot növelni.

A legnagyobb lehetőséget a nagy-nyelvi-modellekben látom, amikoris üzeneteket kell megkomponálni. Ha megfelelően promptoljuk, akkor meg lehet komponálni vele az üzeneteket. Megmondnom neki ki a célcsoport, mi az üzenet, mi a módja az üzenet átadásának, mit akarok elérni, mi a célcsoport befogadó készsége, korcsoporti és nemi megoszlása, iskolázottsága, ha ezeket megadom, akkor az AI nagyszerű technológia arra, hogy segítsen a kognitív üzenetek átadására. Azt is meg tudom mondani, hogy most tényleges PSYOPS üzenetet gyártsál, ami valós tényekre alapul, vagy pedig mehet a fake news és egyéb manipulációs technikák. Ugyanúgy fel lehet használni arra is, hogy az álhíreket felismertessük vele, pl a közösségi média felületeken a megfelelő adatbázissal és tanítással.

II. Interjú Dr. Bányász Péterrel

1. Hogyan látja a közösségi média platformok és az információs hadviselés kapcsolatát?

   Magam részéről én nem tartom szerencsésnek az információs hadviselés terminológiát, mert azt inkább az orosz és kínai gondolkodásban alkalmazzák, míg a NATO oldaláról ezek inkább információs műveletekként használatosak. De az eredeti kérdésre válaszolva, a közösségi média platformok véleményem szerint az információs műveletek egyik legmeghatározóbb eszközévé váltak, tekintettel arra, hogy decentralizált, gyors és hatékony kommunikációs csatornákat biztosítanak különböző aktorok számára. Ezek az aktorok – beleértve állami és nem állami szereplőket egyaránt – a közösségi médiát stratégiai céljaik elérése érdekében használják fel, legyen szó social engineering útján megvalósított kibertámadásról, lélektani műveletekről vagy akár társadalmi kohézió és politikai stabilitás aláásásáról. Mindben a generatív mesterséges intelligencia közösségi oldalakon való elterjedése még hangsúlyosabban jeenik meg. Az információs műveletek tehát nem pusztán az ellenfél félretájékoztatására vagy véleményének manipulálására irányul, hanem hosszú távon akár a demokratikus intézmények működését is destabilizálhatja.

   A közösségi média platformok algoritmusvezérelt tartalomterjesztési mechanizmusai különösen alkalmassá teszik ezeket az eszközöket az információs műveletek hatékony végrehajtására. Az ilyen jellegű műveletek a PSYOPS oldaláról, ami engem leginkább foglalkoztat, jellemzően az alábbi területeken jelenik meg: dezinformációs kampányok, propaganda és narratívaépítés. A dezinformációs kampányok célzott, manipulált információk terjesztésével képesek a közvélemény alakulását befolyásolni, például politikai választásokba történő beavatkozás vagy társadalmi polarizáció elősegítése révén. A propaganda és narratívaépítés során egyes állami vagy nem állami aktorok olyan információs környezetet alakítanak ki, amely hosszú távon formálja a közvéleményt, s ez különösen jellemző az autoriter rezsimekre, amelyek a közösségi média infrastruktúráját és algoritmusait saját geopolitikai céljaik elérésére használják. A PSYOPS szempontjából a közösségi média kiváló eszköz a társadalmi feszültségek generálására, pánik- vagy félelemkeltésre, amelynek egyik

legszembetűnőbb példája a COVID-19 világjárvány alatt terjedő álhírek és összeesküvés-elméletek szerepe volt a közegészségügyi intézkedések elfogadottságának csökkentésében.

A közösségi média algoritmusai jelentősen torzítják az információs környezetet, mivel elsődleges céljuk a felhasználói figyelem fenntartása. Ennek következményeként olyan jelenségek figyelhetők meg, mint a visszhangkamrák és szűrőbuborékok kialakulása, amelyek révén a felhasználók csupán a saját világnézetükkel egyező tartalmakkal találkoznak, ezáltal csökken a kritikai gondolkodás érvényesülésének lehetősége. Emellett a virális terjedés mechanizmusai elősegítik a dezinformáció széleskörű elérhetőségét, míg a botok és trollhadseregek automatizált fiókokon keresztül mesterségesen felerősítik bizonyos narratívák láthatóságát és hatékonyságát.

Az online egyre növekvő nyomás alá kerülnek a kormányzatok és a civil társadalom részéről, hogy felelősséget vállaljanak az információs hadviselésben betöltött szerepükért. Az Európai Unió Digitális Szolgáltatásokról szóló törvénye (DSA) például olyan szabályozási keretet kíván biztosítani, amely növeli az algoritmusok átláthatóságát és az online platformok elszámoltathatóságát. Ugyanakkor a szabályozási intézkedések gyakran nem képesek megfelelő ütemben követni az új manipulációs technikák megjelenését, így az információs hadviseléssel szembeni védekezés multidiszciplináris megközelítést kíván meg. Ráadásul a 2024-es amerikai elnökválasztás teljesen újraírta ezeknek a platformoknak a működését, a korábbi tényellenőrzéssel, moderációs elvekkel kapcsolatos policyjukat törlik, miközben a nemrég lezajlott müncheni Biztonsági Konferencián JD Vance alelnök kifejezetten megfenyegette az EU-t, hogy nem kell itt a szigorú szabályozás az amerikai tech cégekkel szemben. Úgyhogy ez biztosan sok változást fog hozni a közeljövőben.

Ami a tématerületen a jelenlegi kiberbiztonsági kutatások legizgalmasabb megközelítése, az információs műveletek elleni védekezésre vonatkoznak: (1) mesterséges intelligencia és gépi tanulás alkalmazása a dezinformáció felismerésére és szűrésére; (2) hálózatelemzési módszerek fejlesztése az összehangolt információs műveletek feltérképezésére; (3) a digitális

médiaműveltség fejlesztése, amely hozzájárulhat a lakosság információs rezilienciájának növeléséhez.

Azt gondolom, a közösségi média egyszerre jelent lehetőséget és veszélyt az információs hadviselés kontextusában. Egyrészt elősegíti az információ szabad áramlását és a demokratikus részvételt, másrészt lehetőséget teremt az állami és nem állami szereplők számára manipulációs céljaik megvalósítására. Az algoritmusvezérelt tartalomterjesztés, a virális mechanizmusok és az automatizált befolyásolási eszközök együttesen arra világítanak rá, hogy a dezinformáció elleni küzdelem nem csupán technológiai, hanem társadalmi és szabályozási kihívás is egyben.

2. Milyen kihívásokkal szembesülnek a katonai szervezetek a közösségi média használata során konfliktusok idején?

A katonai szervezetek (de a védelmi szféra egyéb szereplői aspektusára is értve) számára a közösségi média konfliktusok idején egyszerre jelent stratégiai lehetőséget és jelentős biztonsági kihívást. A digitális platformok gyors és decentralizált információáramlást biztosítanak, amely lehetővé teszi az információs műveletek támogatását, ugyanakkor növeli a katonai műveletek sérülékenységét az ellenséges befolyásolási kampányokkal, dezinformációval és információ-, műveleti biztonsági fenyegetésekkel szemben. Az egyik legnagyobb kihívás a szenzitív információk védelme, mivel a közösségi médián keresztül könnyen kiszivároghatnak olyan adatok, amelyek az ellenség számára értékes hírszerzési forrásként szolgálhatnak, ahogy erre korábban számos példa volt (pl. izraeli katona posztolta, hova mennek éppen bevetésre és mikor). Az online térben megosztott képek, videók és geolokációs adatok lehetőséget adhatnak az ellenséges aktorok számára, hogy nyomon kövessék a katonai egységek mozgását, eszközállományát és logisztikai folyamatait, ami jelentős taktikai hátrányt eredményezhet. Itt nem csak a 2014-es orosz csapatok mozgására érdemes gondolni, hanem pl. a kiszivárgott fitness app adataira is, amikből ki lehetett rajzolni a különböző külföldi amerikai katonai bázisok helyét.

Ezzel párhuzamosan a katonai szervezetek számára komoly problémát jelent az ellenséges felek által kezdeményezett PSYOPS, amelynek célja a közvélemény befolyásolása, a katonai morál aláásása és a nemzetközi támogatás megingatása.

A közösségi média gyors és ellenőrizhetetlen információterjedése lehetővé teszi, hogy a hamis narratívák széles körben elérhetővé váljanak, és olyan automatizált bot-hálózatok vagy szervezett propagandaaktivitások erősítsék meg őket, amelyek jelentős társadalmi és politikai hatást gyakorolhatnak. A hamis információk és kiszivárgott tartalmak különösen akkor okozhatnak problémát, ha azok olyan vizuális bizonyítékokat tartalmaznak, amelyek delegitimálhatják a katonai beavatkozásokat, vagy negatív nemzetközi reakciókat válthatnak ki.

A közösségi média nemcsak az ellenséges aktorok manipulációs eszközeként jelenik meg, hanem hatással van a katonai szervezetek belső moráljára és a társadalmi percepcióra is. A katonák és hozzátartozóik online aktivitása befolyásolhatja az alakulat kohézióját, valamint pszichológiai ellenállóképességét, miközben a konfliktuszónából származó képek, videók vagy civil áldozatokról készült felvételek gyors terjedése társadalmi tiltakozásokat, politikai nyomást vagy éppen az adott katonai művelet támogatottságának csökkenését eredményezheti. Mindezek fényében a közösségi média használata kettős kihívást jelent a katonai szervezetek számára: egyrészt lehetőséget teremt a stratégiai kommunikációs műveletek támogatására, másrészt azonban fokozza a biztonsági kockázatokat. Bár a katonai szervezetek képesek lehetnek ellen-narratívák kialakítására, a szövetségesi támogatás erősítésére és a lakossági tájékoztatás biztosítására, a platformok algoritmusvezérelt tartalomterjesztési mechanizmusai torzíthatják az információs környezetet, és kiszolgáltathatják a katonai kommunikációt az ellenséges aktorok befolyásolási technikáinak.

A közösségi média szabályozása, az adatvédelmi mechanizmusok megerősítése és a digitális kockázatok kezelése véleményem szerint komoly kihívást jelent a katonai szervezetek számára, különösen az új technológiák – például a mesterséges intelligencia által generált deepfake tartalmak, az automatizált bot-hálózatok és a fejlett OSINT-eszközök – megjelenésével

3. Hogyan befolyásolhatja a közösségi médiában terjedő dezinformáció a katonai műveletekről kialakított közvélekedést?

   A közösségi médiában terjedő dezinformáció komoly hatást gyakorolhat a katonai műveletekről kialakított közvélekedésre, mivel a digitális platformok gyors információáramlást és széles körű elérést biztosítanak, ugyanakkor gyakran

nélkülözik a megfelelő ellenőrzési mechanizmusokat. Véleményem szerint a dezinformáció egyik legnagyobb veszélye, hogy torzíthatja a konfliktusokról szóló narratívákat, és olyan hamis vagy manipulált tartalmakat terjeszthet, amelyek befolyásolják a társadalmi percepciót, politikai döntéshozatalt és a katonai műveletek legitimitását. Az álhírek, félrevezető vizuális tartalmak és kontextusból kiragadott információk célzott alkalmazása jelentős mértékben képes formálni a lakosság attitűdjét, különösen akkor, ha érzelmileg töltött vagy polarizáló témákat érintenek.

Úgy gondolom, hogy a közösségi média algoritmusai, amelyek a felhasználók érdeklődése és interakciói alapján erősítik meg a preferált tartalmakat, tovább fokozzák a dezinformáció hatását, mivel elősegítik a visszhangkamrák és szűrőbuborékok kialakulását. Ez azt eredményezheti, hogy egyes társadalmi csoportok kizárólag olyan információkat fogyasztanak, amelyek megerősítik előzetes véleményüket, ezáltal csökkentve a kritikai gondolkodás és a kiegyensúlyozott tájékozódás lehetőségét. Az ellenséges aktorok – legyenek azok állami vagy nem állami szereplők – kihasználhatják ezt a jelenséget célzott dezinformációs kampányok indítására, amelyek a katonai műveletek ellen hangolhatják a közvéleményt, megoszthatják a szövetséges országokat, és gyengíthetik a hadműveletek társadalmi támogatottságát. Ezt az orosz-ukrán háború esetén tökéletesen látjuk. Mindez egyébként a kiberönkéntesek bevonásában is komoly szerepet játszhat, amelyek aztán kibertámadások elkövetésében is lecsapódik.

A katonai műveletek során különösen veszélyesnek tartom a valós idejű információmanipulációt, amely során ellenérdekelt felek torzított vagy hamis adatokat terjesztenek a katonai beavatkozásokról, harci cselekményekről vagy azok következményeiről. Az ilyen tartalmak – például mesterséges intelligenciával generált hamis videók, átalakított műholdfelvételek vagy manipulált beszámolók – képesek aláásni a katonai szervezetek hitelességét, és akár politikai nyomás alá helyezhetik azokat az államokat, amelyek a műveleteket végrehajtják.

Meggyőződésem, hogy a közösségi médiában terjedő dezinformáció elleni fellépés egyik kulcsa a transzparens és hiteles kommunikáció, amely időben

reagál a hamis információkra, és lehetővé teszi a közvélemény számára, hogy megbízható forrásokból tájékozódjon. A katonai szervezetek számára ezért elengedhetetlen, hogy hatékony ellen-narratívákat alakítsanak ki, és megfelelő kapacitással rendelkezzenek az információs térben zajló manipulációk felismerésére és semlegesítésére. Véleményem szerint a jövőben a közösségi média által előidézett információs kihívások egyre nagyobb szerepet kapnak a hadviselésben, így az ehhez való alkalmazkodás nemcsak technológiai fejlesztéseket, hanem kommunikációs stratégiák újragondolását is igényli.

4. Milyen technológiai eszközök segíthetnek az álhírek azonosításában és terjedésük megakadályozásában?

   Úgy gondolom, hogy az álhírek azonosítása és terjedésük megakadályozása összetett kihívás, amely multidiszciplináris megközelítést és fejlett technológiai eszközök alkalmazását igényli. Az egyik legfontosabb ilyen eszköz a mesterséges intelligencia és a gépi tanulás, amelyek lehetővé teszik a dezinformációs mintázatok felismerését és az automatizált tartalomelemzést. Az algoritmusok képesek azonosítani a szövegekben előforduló gyakori nyelvi torzításokat, érzelmileg túlfűtött megfogalmazásokat vagy strukturálisan gyanús tartalmakat, amelyek jellemzően az álhírek sajátosságai közé tartoznak. Az ilyen modellek természetesnyelv-feldolgozási technológiákat alkalmazva felismerhetik az elfogult megfogalmazásokat, a szándékosan félrevezető narratívákat és a korábban azonosított hamis hírekkel való hasonlóságokat.

   Emellett a hálózatelemzési és OSINT technológiák is kulcsfontosságú szerepet játszanak az álhírek terjedésének feltérképezésében. A közösségi médián belüli interakciós hálózatok vizsgálata lehetőséget nyújt arra, hogy azonosítsam azokat a fiókokat, amelyek egy adott narratíva terjesztésében kiemelkedő szerepet játszanak. Az úgynevezett „botdetekciós” algoritmusok képesek felismerni azokat az automatizált fiókokat és koordinált kampányokat, amelyek célja az álhírek mesterséges felerősítése. Úgy látom, hogy a hálózatkutatás és a gráfelméleti megközelítések segítségével az álhírterjesztés mögött álló mintázatok ismeretében célzottabb beavatkozások hajthatók végre, például az ilyen fiókok eltávolítása vagy az algoritmikus elérésük csökkentése révén.

Fontosnak tartom továbbá a deepfake-detektáló algoritmusok és a vizuális manipuláció felismerésére szolgáló technológiák fejlesztését, mivel az álhírek egyre gyakrabban jelennek meg manipulált képek és videók formájában. Az arcfelismerő és képanalízis-alapú mesterséges intelligencia képes kiszűrni azokat a vizuális eltéréseket, amelyeket emberi szemmel nehéz észrevenni, például az arcok elmosódását, az árnyékok inkonzisztenciáját vagy az anomáliákat a szemmozgásban. Ezek az eszközök lehetővé teszik, hogy a közösségi média platformjai automatikusan figyelmeztetéseket jelenítsenek meg a gyanús tartalmak mellett, vagy akár blokkolják is azokat.

A technológiai eszközök mellett meggyőződésem, hogy az álhírek elleni küzdelem nem lehet kizárólag algoritmusokra bízott folyamat. A humán ellenőrzés és a tényellenőrző mechanizmusok továbbra is elengedhetetlenek, különösen az összetett vagy politikailag érzékeny témák esetében. Az olyan szervezetek, mint a Snopes, a PolitiFact vagy az Európai Unió által támogatott tényellenőrző kezdeményezések, szakértői elemzésekkel és bizonyítékokon alapuló értékelésekkel segítik a dezinformáció elleni védekezést. Kérdés, hogy ezeknek mi lesz a sorsa, ahogy erre az első kérdésnél már utaltam. Az AI-alapú megoldások és a humán szakértelem kombinációja biztosíthatja, hogy az álhírek felismerése és semlegesítése a lehető legpontosabb és leggyorsabb legyen.

Véleményem szerint a jövőben a közösségi média platformoknak és a kormányzati szabályozóknak szorosabban kell együttműködniük annak érdekében, hogy hatékonyabb tartalomszűrési mechanizmusokat vezessenek be, és transzparensebbé tegyék az algoritmusok működését. A mesterséges intelligencián alapuló eszközök, a hálózatelemzés, a vizuális manipulációt felismerő algoritmusok és a humán tényellenőrzés együttes alkalmazásával az álhírek terjedése jelentős mértékben csökkenthető, ugyanakkor fontos, hogy ezek az intézkedések ne sértsék a szólásszabadság alapelveit. Ezért úgy látom, hogy az álhírek elleni küzdelem egyik legnagyobb kihívása az egyensúly megtalálása a platformok szabályozása és az információs szabadság fenntartása között.

5. Hogyan lehet a közösségi médiát úgy használni a közvélemény formálására konfliktusok idején, hogy az megfeleljen az etikai normáknak?

Úgy gondolom, hogy a közösségi média konfliktusok idején hatékony eszközként szolgálhat a közvélemény formálására, ugyanakkor elengedhetetlen, hogy annak használata megfeleljen az etikai normáknak és ne sértse az információs integritást. A legfontosabb alapelv számomra a transzparencia és hitelesség, amely biztosítja, hogy a megosztott információk megbízható forrásokon alapuljanak, és ne manipulálják a közvéleményt félrevezető vagy torzított narratívákkal. Úgy vélem, hogy a közösségi média felelős alkalmazása érdekében minden kommunikációs stratégiának arra kell törekednie, hogy objektív, tényszerű és ellenőrizhető információkat osszon meg, elkerülve az érzelmileg túlfűtött vagy polarizáló tartalmakat, amelyek felerősíthetik a társadalmi feszültségeket.

A közvélemény formálása során kiemelten fontosnak tartom az etikai irányelvek betartását, különös tekintettel az emberi jogok védelmére, a háborús dezinformáció terjedésének megakadályozására és a társadalmi stabilitás fenntartására. A közösségi médiát úgy kell alkalmazni, hogy az elősegítse a konfliktusokról való pontos és kiegyensúlyozott tájékoztatást, ugyanakkor ne váljon eszközzé az ellenséges propaganda, a manipuláció vagy a pszichológiai hadviselés számára. Az etikus kommunikáció egyik kulcseleme szerintem az, hogy a közösségi médiában megjelenő információk ne keltsenek indokolatlan pánikot vagy feszültséget, hanem a lehetőségekhez mérten a konfliktusok békés rendezésének előmozdítását szolgálják.

A platformok felelős használatának egyik hatékony módja a tényellenőrzés és a megbízható források előtérbe helyezése, amely biztosítja, hogy a közösségi médiában megjelenő információk ne legyenek manipuláció tárgyai. Véleményem szerint az álhírek és a dezinformáció elleni küzdelemben elengedhetetlen a szakmai és független tényellenőrző szervezetek szerepvállalása, valamint olyan algoritmikus megoldások alkalmazása, amelyek csökkentik a hamis információk terjedését anélkül, hogy ez a szólásszabadság aránytalan korlátozásához vezetne.

Ezen túlmenően úgy látom, hogy a közösségi média használata során figyelembe kell venni a célközönség információs környezetét és annak sajátosságait, mivel a különböző kulturális, politikai és társadalmi háttérrel rendelkező emberek eltérően értelmezhetik ugyanazt az információt. Éppen ezért elengedhetetlen, hogy a közösségi médiában megosztott tartalmak megfelelő kontextusba helyezve

jelenjenek meg, elkerülve azokat a kommunikációs stratégiákat, amelyek félreértésekhez vagy a helyzet további eszkalálódásához vezethetnek.

Meggyőződésem, hogy a közösségi média konfliktusok idején nem csupán a gyors információátadás eszköze, hanem felelősséggel is jár annak biztosítása, hogy az információs tér ne váljon manipulációs kísérletek terepévé. Ennek érdekében a közösségi média tudatos és etikus használatát elősegítő stratégiáknak össze kell hangolniuk a transzparens kommunikációt, a tényeken alapuló tájékoztatást és a dezinformáció elleni fellépést, miközben tiszteletben tartják az információs szabadság elvét és a közvélemény tisztességes tájékoztatásának követelményeit. Bár folyamatosan a „kell" kifejezést használtam, de az emberképem miatt ez tudom, inkább a „sollen-sein" kategóriájába tartozik, vagyis ezeket kellene követni, de a világ, amiben élünk, és ahogy fejlődünk, ezeket meg is tartja a „kellene" kategóriájában, de nem fognak megvalósulni.

6. Mi a közösségi média platformok felelőssége abban, hogy megakadályozzák eszközeik visszaélésszerű használatát információs hadviselés során?

   Úgy vélem, hogy a közösségi média platformok komoly felelősséget tartoznak abban, hogy megakadályozzák eszközeik visszaélésszerű használatát az információs műveletek során, mivel ezek a digitális terek nem csupán az információáramlás közvetítői, hanem egyben alakítói is. A platformok működésükből fakadóan hatalmas mennyiségű adatot kezelnek, és algoritmusaik aktívan befolyásolják, hogy milyen tartalmak jutnak el a felhasználókhoz. Éppen ezért elengedhetetlennek tartom, hogy a vállalatok olyan etikus és átlátható moderációs mechanizmusokat alkalmazzanak, amelyek képesek kiszűrni a manipulációra, félrevezetésre és társadalmi destabilizációra irányuló kampányokat, miközben nem sértik az információszabadság alapelveit.

   A közösségi média platformok felelőssége szerintem több szinten is érvényesül. Egyrészt biztosítaniuk kell, hogy fejlett technológiai megoldásokkal – például mesterséges intelligencia és hálózatelemzés alkalmazásával – hatékonyan detektálják és semlegesítsék a koordinált dezinformációs műveleteket. Az automatizált bot-hálózatok, trollcsoportok és hamis fiókok felismerése és eltávolítása alapvető feladatuk kell, hogy legyen, hiszen ezek az eszközök gyakran szolgálnak információs hadviselési stratégiák végrehajtására. Úgy látom, hogy az

átlátható és felelősségteljes algoritmusok kialakítása, valamint azok rendszeres auditálása kulcsfontosságú annak érdekében, hogy minimalizálják az információs műveletek által okozott társadalmi károkat.

Másrészt fontosnak tartom, hogy a platformok ne csupán technológiai szinten, hanem szabályozási és szakpolitikai együttműködés révén is aktívan részt vegyenek az információs hadviselés elleni küzdelemben. Ez azt jelenti, hogy felelősséget kell vállalniuk a tartalommoderációs eljárások fejlesztéséért, a transzparens jelentési rendszerek kidolgozásáért, valamint a független kutatók és tényellenőrző szervezetek számára való hozzáférés biztosításáért. Az átláthatóság különösen fontos tényező, hiszen a felhasználóknak joguk van tudni, hogy milyen mechanizmusok alapján szűrik vagy korlátozzák az egyes információkat.

Úgy vélem, hogy a közösségi média vállalatoknak kiemelt figyelmet kell fordítaniuk arra is, hogy megakadályozzák az állami vagy nem állami szereplők által végrehajtott információs műveleteket, amelyek a demokratikus folyamatokat, a társadalmi kohéziót vagy a nemzetbiztonságot veszélyeztetik. A politikai reklámok, a célzott manipulációs kampányok és az algoritmusok torzító hatásai mind olyan területek, ahol fokozott felelősségvállalásra van szükség, hiszen az információs hadviselés nemcsak egy adott platformot érint, hanem szélesebb értelemben a társadalom stabilitását és a globális biztonságot is befolyásolhatja.

Meggyőződésem, hogy a közösségi média platformok szerepe az információs tér fenntartható és etikus működtetésében az elkövetkező években egyre nagyobb jelentőséggel bír majd. A technológiai megoldások, a szabályozási keretek és a társadalmi felelősségvállalás hármas pillérére épülő stratégia nélkülözhetetlen ahhoz, hogy ezek a platformok ne váljanak az információs hadviselés eszközeivé. Ugyanakkor az egyensúly megtalálása a dezinformáció elleni hatékony fellépés és a szólásszabadság tiszteletben tartása között továbbra is az egyik legnagyobb kihívás marad, amelyre a közösségi média vállalatoknak és a szabályozó hatóságoknak egyaránt reflektálniuk kell. De ahogy már többször utaltam rá, a Trump-adminisztráció kapcsán bekövetkező átalakulásnak csak az elején vagyunk a platformszabályozásban, így nehéz bármit mondani azzal kapcsolatban, hogyan fog alakulni ez a terület globálisan nézve.

7. Hogyan járul hozzá a közösségi média a globális propaganda és dezinformáció terjedéséhez?

   Erről több aspektusból tettem már említést, így nem ismételném. Viszont azt gondolom, fontos lenne a fogalmak tisztázása és egymás kapcsolatainak meghatározása. Hogyan kapcsolódik a dezinformáció és a propaganda, meg egyáltalán, a rendszeresen használt kifejezések, mint álhírek, disinfo, misinfo, malinfo, propaganda stb. között mi a viszony. Az interjú alanyok ezeket lehetséges, hogy eltérő módon értelmezik, és a válaszaikból nem feltétlen fog kiderülni ez.

8. Hogyan tudják a kormányok és szervezetek leküzdeni a közösségi médián terjedő hamis információk jelentette kihívásokat válsághelyzetekben?

   Úgy gondolom, vitán felüli, hogy a kormányok és szervezetek számára a közösségi médián terjedő hamis információk kezelése válsághelyzetekben az egyik legnagyobb kihívást jelenti, mivel ezek a platformok rendkívül gyors és széles körű információáramlást tesznek lehetővé, ugyanakkor gyakran nélkülözik a megfelelő ellenőrzési mechanizmusokat. Véleményem szerint az álhírek elleni hatékony fellépés elsődleges eszköze a gyors és hiteles kommunikáció, amely biztosítja, hogy a lakosság megbízható forrásokból értesüljön a kialakult helyzetről. A hivatalos kormányzati szerveknek és nemzetközi szervezeteknek proaktív módon kell jelen lenniük a közösségi médiában, és olyan kommunikációs stratégiát kell alkalmazniuk, amely minimalizálja a dezinformáció térnyerésének esélyét.

   Meggyőződésem, hogy válsághelyzetekben a közösségi médián terjedő hamis információk elleni küzdelem egyik leghatékonyabb módja az intézményesített tényellenőrzési mechanizmusok kialakítása és megerősítése. Az állami intézményeknek, független tényellenőrző szervezeteknek és médiaplatformoknak szorosan együtt kell működniük annak érdekében, hogy az álhíreket gyorsan azonosítsák és cáfolják, még mielőtt azok széles körben elterjednének. Ezt a célt szolgálhatják a mesterséges intelligencia és hálózatelemzési technológiák, amelyek képesek valós időben detektálni a dezinformációs kampányokat és az automatizált tartalomterjesztési stratégiákat.

Úgy látom, hogy a kormányoknak és szervezeteknek nem csupán az álhírek cáfolására kell koncentrálniuk, hanem arra is, hogy erősítsék a társadalom információs rezilienciáját, vagyis a lakosság képességét a hiteles információk felismerésére és a manipulációs kísérletekkel szembeni ellenállásra. Ennek érdekében szükségesnek tartom az átfogó médiaműveltségi és digitális oktatási programok bevezetését, amelyek segítenek a polgároknak kritikus szemmel értékelni az online térben megjelenő tartalmakat. Minél tudatosabb a társadalom a dezinformáció működési mechanizmusairól, annál nehezebb az álhírek tömeges elterjedése és társadalmi károkozása. De megint csak, „sollen-sein”

9. Hogyan látja a közösségi média szerepének jövőjét a hibrid hadviselés kontextusában?

   Úgy vélem, hogy a jövőben tovább erősödik, mivel ezek a platformok egyre inkább az információs műveletek elsődleges terepévé válnak. Úgy látom, hogy a közösségi média a hibrid hadviselésben elsősorban a PSYOPS és társadalmi destabilizáció céljából lesz kihasználva, különösen olyan konfliktusokban, ahol az információs fölény megszerzése döntő jelentőséggel bír.

   A közösségi média jövőbeli szerepének egyik legfontosabb aspektusát abban látom, hogy a technológiai fejlődés és az algoritmikus tartalomterjesztés egyre kifinomultabb manipulációs lehetőségeket kínál az állami és nem állami szereplők számára. A mesterséges intelligencia által generált deepfake videók, a hamis profilokat üzemeltető bot-hálózatok és az automatizált dezinformációs kampányok lehetővé teszik, hogy a konfliktusok során egyes szereplők célzott módon befolyásolják a közvéleményt és a politikai döntéshozatalt. Egyre inkább azt tapasztalom, hogy a közösségi médiában zajló információs műveletek nemcsak a harctéri eseményekről szóló narratívákat torzítják, hanem a demokratikus intézmények legitimitását és a nemzetközi kapcsolatok stabilitását is alááshatják.

   A hibrid hadviselés jövőjében kulcsfontosságúnak tartom, hogy a közösségi média hogyan reagál az új típusú információs fenyegetésekre. A platformoknak egyre nagyobb felelősséget kell vállalniuk azzal kapcsolatban, hogy ne váljanak az információs hadviselés eszközévé, ugyanakkor úgy látom, hogy a jelenlegi

szabályozási és moderációs mechanizmusok még nem elég fejlettek ahhoz, hogy hatékonyan kezeljék a hibrid fenyegetések komplexitását. A jövőben várhatóan szorosabb együttműködésre lesz szükség a kormányok, a közösségi médiavállalatok és a biztonsági szakértők között, hogy olyan technológiai és szabályozási keretrendszert alakítsanak ki, amely csökkenti az információs hadviselés hatékonyságát.

Úgy gondolom, hogy a közösségi média a hibrid hadviselésben nem csupán a fenyegetések színtere, hanem potenciálisan védelmi eszköz is lehet. A dezinformáció elleni küzdelemben nagy szerepet játszhatnak az olyan fejlett technológiák, mint a hálózatelemzés, a mesterséges intelligencia-alapú tartalomellenőrzés és a forrásmegbízhatósági algoritmusok, amelyek segíthetnek az álhírek terjedésének csökkentésében. Ugyanakkor az információs reziliencia növelése – vagyis a társadalmak tudatosabbá tétele az információs manipulációval szemben – ugyanolyan fontos szerepet játszik majd a jövő konfliktusainak kezelésében.

A PSYOPS mellett azért azt sem szabad elfelejteni, hogy a közösségi médiában zajló adathalász kampányok támogathatnak különböző kibertér műveleteket.

Összességében úgy látom, hogy a közösségi média a hibrid hadviselés egyik legmeghatározóbb eszközévé válik, amelyet egyszerre lehet kihasználni információs manipuláció céljából és felhasználni a dezinformáció elleni védekezésben. A jövő kulcskérdése az lesz, hogy a technológiai fejlődés és a szabályozási környezet képes lesz-e lépést tartani az egyre összetettebb információs hadviselési stratégiákkal, és hogy milyen mértékben sikerül a közösségi médiát a demokratikus értékek és az információs biztonság fenntartásának szolgálatába állítani.

10. Mennyire fontos a közösségi média tudatosság a civil és katonai szereplők számára a manipulációk elkerülése érdekében?

    Úgy vélem, hogy a közösségi média kulcsfontosságú a manipulációk elkerülése érdekében, teljesen mindegy, hogy civil vagy katona (de érvényes rendőrre, nemzetbiztonságira) az ember, mivel a digitális platformok egyre nagyobb

szerepet játszanak az információs műveletekben és a dezinformáció terjesztésében. A közösségi média működésének és a manipulációs technikáknak az ismerete nélkül a felhasználók – legyenek azok állampolgárok, döntéshozók vagy katonai szakemberek – könnyen áldozatául eshetnek olyan információs stratégiáknak, amelyek célja a félrevezetés, a közvélemény befolyásolása vagy éppen a társadalmi destabilizáció.

A civil társadalom számára a közösségi média tudatosságot elengedhetetlennek tartom az információs reziliencia növelése szempontjából, hiszen az álhírek, összeesküvés-elméletek és célzott dezinformációs kampányok egyre kifinomultabb módszerekkel terjednek, és sokszor nehezen megkülönböztethetők a valós hírektől. A kritikus gondolkodás fejlesztése, az információforrások ellenőrzése és az algoritmusok működésének megértése mind hozzájárulnak ahhoz, hogy a polgárok ellenállóbbá váljanak az online manipulációval szemben. Minél tudatosabb egy társadalom az információs tér veszélyeivel kapcsolatban, annál kevésbé lesz sérülékeny a propaganda, a pszichológiai hadviselés és a polarizáló narratívák hatásaival szemben.

A katonai szereplők esetében a közösségi média tudatosság még nagyobb jelentőséggel bír, mivel az információs műveletek közvetlen hatással lehetnek a hadműveletek biztonságára, a stratégiai döntéshozatalra és a harctéri helyzetértékelés pontosságára. A katonai személyzet közösségi médiahasználata – akár szándékosan, akár véletlenül – olyan kritikus információkat szivárogtathat ki, amelyek az ellenség számára felderítési előnyt biztosíthatnak, például a csapatmozgásokról, fegyverzetről vagy műveleti tervekről. Emellett az ellenséges információs hadviselés egyik célja éppen az, hogy a katonai szereplők morálját aláássa, a szövetségesi viszonyokat megingassa, és a közvélemény támogatását csökkentse a katonai műveletekkel kapcsolatban.

Úgy látom, hogy a közösségi média tudatosság mind a civil, mind a katonai szférában egyre inkább stratégiai jelentőségűvé válik, és ennek megfelelően az oktatási és képzési programoknak is nagyobb hangsúlyt kell fektetniük az információs műveletek felismerésére és kezelésére. A médiaműveltség, a kritikai gondolkodás és az információs biztonsági protokollok ismerete alapvető

készségekké kell, hogy váljanak mindazok számára, akik a digitális térben aktívan részt vesznek a diskurzusban vagy döntéshozatali szerepet töltenek be.

Bár manipuláció a kérdés, és mindez sokszor az INFOOPS oldaláról jelenik meg, de azért egy phishing vagy más social engineering technikák is manipuláció körébe sorolható. Ezeknek a platformoknak a használata újabb és újabb kockázatokat rejt, pláne a genAI elterjedésével, és ezeknél a tudatosság erősítése egyre fontosabb lesz. A három lábú kisgyerek, aki üres PET-palackokból készített motort, sok mindenben elő fog jönni. Ha ezt valósnak hisszük, csak egy lépés, hogy a kommentél, ahol felköszönjtük, gratulálunk neki, megkapjuk a phishing linket, kedvezményes hitelajánlatot stb. Ez már létező támadás.

11. Hogyan befolyásolja a közösségi média és az információs műveletek kapcsolatát a mesterséges intelligencia?

    Erre korábbi kérdéseknél már reflektáltam, nem ismételném.

12. Milyen etikai kérdések vetődnek fel ezzel kapcsolatban?

    Erre is.

III. Interjú Prof. Dr. Kovács Lászlóval

1. Véleménye szerint melyek a legnagyobb kibervédelmi kockázatok a közösségi média katonai célú használatával kapcsolatban?

   Minden olyan tartalom megosztása, amely az adott honvédelmi célú munkára bármilyen jellemzővel bír. Technikai adatok megadása, fényképek és videók megosztása érzékeny beosztásban lévő személyekről. A másik, de ezzel összefüggő kockázat a kapcsolati hálózat(ok) feltérképezése.

2. Véleménye szerint hogyan védhetők meg a katonai szervezetek érzékeny operatív adatai a közösségi média platformokon keresztül történő kibertámadások ellen?

   Nagyon komoly szakmailag kontrollált információmegjelenésekkel, illetve folyamatos, gyakorlati képzést is magában foglaló felkészítésekkel.

3. Milyen lépéseket kell tenni a közösségi médián keresztül történő kémkedés megakadályozására katonai műveletek során?

   A fentiekben leírt eljárásrend betartása, a műveleti biztonság kiterjesztésével erre e területre is.

4. Hogyan értékeli a közösségi médián keresztül végrehajtott kibertámadások fenyegetését?

   Egyre növekvő kockázatot jelentenek az ilyen támadások. A kérdés az, hogy már az információszerzést is támadásnak minősítjük-e? (Véleményem szerint igen abban az esetben, ha az adott információszerzés támadás előkészületéhez, vagy rosszindulatú tevékenység tervezéséhez és majdani végrehajtásához szükséges).

5. Milyen szerepet játszik a titkosítás a katonai kommunikáció védelmében a közösségi médián?

   Ez nem érthető kérdés, mert minősített adatoka nem kerülhet közösségi média oldalakra. Amennyiben end-to-end titkosításról beszélünk, akkor az abszolút alap eljárás ma már, de nem a közösségi média, hanem inkább az instant messages szolgáltatások esetében.

6. Hogyan lehet javítani a kibervédelmi intézkedéseket a hibrid támadásokkal szemben, amelyek információs és kiber műveleteket kombinálnak?

Tudatosítás és folyamatos oktatás. Technikai védelemmel pedig ott (alapvetően hozzáférés korlátozással), ahol ez a műveleti biztonság szempontjából kiemelten fontos.

7. Milyen protokollokat kell követni a közösségi média csatornáinak biztonságos használatához az információs műveletek során?

   Felhasználó (tartalom készítője) anonimitásának biztosítása, célközönség jó kiválasztása, visszaható hatás elemzése.

8. Hogyan értékeli a kiberinfiltráció kockázatát, amelyet a közösségi médián keresztül történő szociális manipuláció jelent?

   Ez a hibrid műveletek egyik alapja. Így komoly kockázatot jelent.

9. Melyek a legjobb gyakorlatok a kritikus infrastruktúrák védelmére a közösségi médián keresztül indított kibertámadások ellen?

   Need to know elv alkalmazása. Körültekintő gyártói és rendszerinformációk publikálása. Felhasználók oktatása, és folyamatos technikai upgrade a sérülékeny és kiemelt rendszerekben.

10. Véleménye szerint hogyan befolyásolja a mesterséges intelligencia és a gépi tanulás a kibervédelmet a közösségi médiában zajló hadviselés kontextusában?

    Növekvő kockázatot jelent, mert az MI és az öntanulás, valamint a nagy mennyiségű adatfeldolgozás sokkal hatékonyabbá teszi a közösségi médiában történő befolyásolást.

11. Milyen etikai kérdéseket vet fel a mesterséges intelligencia a kibervédelem / katonai védelem /kritikus infrastruktúra védelem szempontjából?

    Már régen nincsenek etikai kérdések, hatékonyság és célok elérése van csak.