ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

**DOKTORI (PHD) ÉRTEKEZÉSTERVEZET**

**KUN TAMÁS**

# A pszichológiai manipuláció jelentősége és geopolitikai hatásai

Témavezető: Dr. Babos Tibor címzetes egyetemi tanár

**BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA**

Budapest, 2024. május 30.

**TARTALOMJEGYZÉK**

# BEVEZETÉS

*„A képzelet mindent nagyobbra fest, mint a valóság lenni szokott.”*
Széchenyi

## A tudományos probléma megfogalmazása

***Problémafelvetés***

A pszichológiai manipuláció tömeges alkalmazása révén olyan biztonsági kockázatok láttak napvilágot, amelyek döntő mértékben képesek már befolyásolni egy-egy társadalom helyzetét. Ezek a kibertérben egymást nem kizárva politikai és pénzügyi haszonszerzés céljával kerülnek végrehajtásra. Az informatikai megoldások és alkalmazások térnyerésével a folyamatok sok esetben névtelenül, a háttérben meghúzódva zajlanak le úgy, hogy az elkövető kiléte rejtve marad. A manipulációs technikák az emberi tényezőt, mint a rendszer biztonsági szempontjából ***jellemzően legkönnyebben sebezhető pontját*** [1, p. 12] használják ki a befolyásolhatóság ismérveire támaszkodva.

***Helyzetértékelés***

Az egyéni szinttől ellépve jól látható, hogy az információs térben zajló kommunikáció penetrációs szintje nagyságrendeket lépett előre az elmúlt évtizedben. A közösségi média térnyerésével a tömegtájékoztatás formái új irányokat vettek, ebből kifolyólag a politikai folyamatok is felfejlődtek a kor adottságaihoz.

Az első világháború teljes mértékben átrajzolta a háborúkkal kapcsolatos elképzeléseket, a technológiai eszközök és a pusztítás mértéke pedig felülmúlta minden tekintetben az addigi történelmi tapasztalatokat. [2] A második világháború után kialakult világrend, ami meghatározta a hidegháború éveit az Egyesült Államok és a Szovjetunió alkotta egyensúlyra épült. [3, pp. 95-99] A hidegháború lezárását követő éveket illetően több vízió is napvilágot látott, melynek egy részében a liberális demokráciák diadalát dicsőítették, amik a „történelem végét” feltételezték, ezzel szemben állt a „civilizációk összecsapása” elmélet, amely pedig azt hangsúlyozta, hogy az újkori konfliktusok a civilizációk közötti kulturális és vallási ellentéteken fognak majd alapulni a jövőben. [4] A Magyar Köztársaság biztonság- és védelempolitikájának alapelveit 1998-ban a

kétpólusú világrendszer időszakához mérten úgy értékelték, hogy habár minimálisra is csökkent egy világméretű fegyveres konfliktus lehetősége, a sokrétűbb környezet viszont potenciálisan több veszéllyel fenyeget. [5] Európa biztonsága az euroatlanti régió gazdasági-társadalmi-politikai folyamatainak változásaitól függnek. Ezek megnyilvánulnak az európai hatalmi érdekérvényesítés történelmi jellemzőin, a globális és a regionális biztonsági kihívások tükrében, a védelmi képességek fejlődésében, a transzatlanti kapcsolatok dialektikájában, valamint a kontinens integrációs törekvéseiben. A Varsói Szerződés enyészetté válását követően az Észak-atlanti Szerződés Szervezete (NATO) 1994-ben útjára indította a Partnerség a Békéért programot, a Szövetség pedig 1999-ben három, Magyarország, Lengyelország és a Cseh Köztársaság; 2002-ben pedig hét új taggal, Észtország, Lettország, Litvánia, Szlovákia, Szlovénia, Románia és Bulgária szerepében bővült. [6, pp. 141-142] 2001. szeptember 11. egy fontos mérföldkőnek számít a világ biztonsági struktúrájában és a NATO történetében, mert ez volt az első alkalom, amikor a Szövetség 5. cikkelyének értelmében a New York-i terrortámadásokat a szervezet összes tagja elleni támadásnak ítélték meg. Ezen a napon kezdődött az ezt követő 20 évig tartó globális terror elleni háború. [7] A 2004-es narancsos forradalom képezte alapját a 2013 végén EuroMaidan néven folytatódó, tüntetéssorozatba torkolló elégedetlenségi hullámnak Ukrajnában, ami végül 2014. március 18.-án a Krím-félsziget az Oroszországi Föderáció általi elcsatolásában csúcsosodott ki. [8]

***A kutatás célrendszerét az alábbi kérdések mentén határoztam meg:***

1. Milyen összefüggés áll fent a manipuláció és a geopolitika között?
2. Milyen tényezőket kell vizsgálni ebben az összefüggésben?
3. Hogyan jelenik meg mindez a gyakorlati alkalmazásban?

**Az értekezés tézise, hogy a pszichológiai manipuláció jelentőségének és geopolitikai eseményekre gyakorolt hatásainak megértéséhez szükséges legalább négy tényezőt számításba venni, amelyek:**

- A pszichológiai manipuláció megjelenésének és kialakulásának **fejlődéstörténete**;
- A kommunikációs **trendek változása**, fókuszban a **közösségi média** térnyerésével;
- Az emberi kapcsolatok természete és a **bizalomépítés** lehetséges módszerei;
- **A geopolitikai folyamatok formálásának képessége**

## Célkitűzések

A kiemelt társadalmi figyelmet élvező gazdasági- és társadalompolitikai kérdések elemzésén keresztül foglalkozom a **biztonság**, a **pszichológiai manipuláció** és a **kiberbiztonságot** érintő témákkal, valamint azok **geopolitikai eseményekre gyakorolt hatásainak** vizsgálatával. Annak érdekében, hogy ezeket a tényezőket vizsgálni tudjam, elkülönítem a tézisben megfogalmazott szempontok mentén a kutatási irányokat. Szükséges meghatározni egy keretet, amelyben a fent említett fogalmak elhelyezhetők; meg kell vizsgálni a közvetítő eszközök használatában jelen lévő változást; rá kell világítani az alapvető emberi interakciók sajátosságaira; majd ezeket ki kell vetíteni társadalmi szintű elemzésre.

***Az értekezés felépítése***

A fentiek tükrében **az értekezés az alábbi négy fejezetre épül:**

1. A biztonság, a pszichológiai manipuláció, a kibertér és a kritikus infrastruktúrák;
2. A közösségi média szerepe és hatása a társadalmi folyamatokra;
3. Az emberi kapcsolatok természete, a bizalom szerkezeti felépítése;
4. A pszichológiai manipuláció geopolitikai eseményekre gyakorolt hatásainak vizsgálata 2019-2023.

Az értekezés *első fejezetében* meghatározom a **keretrendszert**, amelyben a kutatási probléma elhelyezkedik. A három alfejezetben a pszichológiai manipuláció történeti hátterét, a kibertér és a kritikus infrastruktúrák kapcsolatát és a korszerű támadási típusokat mutatom be, mely utóbbi esetben az informatikai megoldások alkalmazásával a támadók a pszichológiai manipulációra építve hajtanak végre támadásokat.

A *második fejezetben* az **eszközhasználatban** bekövetkezett változásokat ismertetem. A három alfejezetben kitérek a tömegkommunikációban (hírközlésben) bekövetkezett változásokra, végig veszem a közösségi média történeti áttekintését, amely számottevően rajzolta át az elmúlt évtized kommunikációs trendjét, valamint az álhírek és a médiamanipuláció korszakos jelenségét vázolom fel, ami fontos eleme napjaink politikai kommunikációjának.

A *harmadik fejezetben* egy továbbfejlesztett **modellen** keresztül mutatom be a bizalom felépülésének szerkezetét. Az emberi kapcsolatokban a bizalom kulcsszerepet játszik,

ami a manipuláció hatásainak vizsgálata során jól alkalmazható, valamint alkalmas eszköz lehet a védekezési metódusokban is.

A *negyedik fejezetben* **esettanulmányokon** keresztül a pszichológiai manipuláció gyakorlatban történő megjelenését elemezem. A három alfejezetben a SARS-CoV-2 (Covid-19) koronavírus világjárvány, az afganisztáni kivonulás és az orosz-ukrán háború eseményeit mutatom be, valamint példákat hozok a modern tömegkommunikációs csatornákon megjelent tartalmakról, amik közlésének módja egyértelműen meghatározó szerepet tölt be a közvélemény befolyásolásában.

***A kutatás lehatárolása***

Katonai műszaki tudományok
- Védelmi elektronika (informatika és kommunikáció)
  - informatika, kommunikáció, elektronikus hadviselés
    - **lélektani hadviselés**
  - mérnöki (műszaki) tevékenység
    - pszichológiai manipuláció
      - **politikai/jogi/katonai** megjelenése
      - **informatikai** megjelenése
  - közösségi média
    - katonai tevékenység a társadalmi kommunikációban
    - a manipuláció (hibrid hadviselés) **hatása a hírközlésben**

A vizsgálat **fókusza** az események közlésének módján van, valamint az alkalmazott eszközök vizsgálata a meghatározó, azonban nem hanyagolhatók el az események megértéséhez szükséges háttérismeretek sem. Itt érdemes még egyszer hangsúlyozni a földrajzi helyzetből fakadó lehetőségeket és adottságokat, ami a geopolitika alapkoncepciója. A kutatómunka **megalapozottságát** az irodalomjegyzékben szereplő 234 hivatkozás adja, melynek **hitelességét** a hazai és nemzetközi szakirodalom, kormányzati és nemzetközi szervezetek nyilatkozatai és ajánlásai, illetve nagy múlttal rendelkező hírszolgáltatók beszámolóinak feldolgozásán keresztül hivatott alátámasztani. Az értekezés **összességében** a geopolitikai eseményekre jellemző dinamikát a pszichológiai manipuláció társadalmi-gazdasági folyamatokra gyakorolt hatásain keresztül igyekszik megvilágítani, valamint annak jelentőségét hangsúlyozni. Rendezőelve kapaszkodót kíván nyújtani abban a komplex információs közegben, melyben a rejtett szándékok folyamatosan körbevesznek minket.

## A téma kutatásának hipotézisei

**H1: Feltételezem, hogy a kritikus infrastruktúrák védelme nélkül a társadalmi biztonság nem értelmezhető**

A mindennapos tevékenységek támogatásához elengedhetetlenek ezek a létesítmények a zavartalan működés szempontjából. A társadalom biztonságérzetére ezek működésében felmerülő fennakadások komoly aggodalmat ébreszthetnek a lakosságban.

**H2: Feltételezem, hogy a tömegkommunikációban szignifikáns változás történt az elmúlt évtizedben**

A technológiai fejlődés, illetve közösségi média térnyerése nem elhanyagolható mértékben változott meg a vizsgált időszakban, súlyuk a közgondolkodásban kiemelkedővé vált, a lakosság tájékoztatása során pedig felelősséggel kell eljárnia fontossági szerepéből kifolyólag.

**H3: Feltételezem, hogy az álhírek azonosítására és szűrésére szemlélet/modell alkotható**

Meggyőződésem, hogy a médiában megjelenő álhírek módszeres megfigyeléssel kiszűrhetők, a bennük megjelenő érdekek azonosíthatók.

**H4: Feltételezem, hogy a manipuláció szerepe meghatározó lehet a geopolitikai események alakulásában**

A hírszerzési- és kommunikációs (például a propaganda) tevékenység már a hidegháborúban lételeme volt nemzetállamok döntési mechanizmusainak, az internet alapú kommunikációs struktúrák alkalmazásával pedig robbanásszerű szintlépés történt.

## Kutatási módszerek

Az értekezésben szereplő **esettanulmányok**, mint *kvalitatív kutatási módszer* a 2019 és 2023 közötti évek eseményeit taglalják. Az események vizsgálatában a **megfigyelés**, mint *empirikus kutatási módszer*, a szakirodalmi feldolgozás és forráskutatás során az **analízis**, **szintézis**, **indukció** és **dedukció-**, a modellalkotás során az **absztrakció**, mint *logikai tudományos módszer* került alkalmazásra. [9] Az események volumenét illetően a folyamatokba való beavatkozás lehetőségét kizártnak tekintem. A bizalomépítés folyamatát a mérhetőség oldaláról vizsgálva saját logikát építettem fel, amelyben az érzelmi tényező jelentőségét emeltem ki. A jelenlegi információs környezet megértését elősegítendő, fogalomrendszerben gyűjtöttem össze azokat az elemeket, amelyek az információs térben történő tevékenységhez, valamint a bizalmi helyzetek leképezéséhez elengedhetetlenül járulnak hozzá.

# 1 A BIZTONSÁG, A PSZICHOLÓGIAI MANIPULÁCIÓ, A KIBERTÉR ÉS A KRITIKUS INFRASTRUKTÚRÁK

*„Tudatlanságból sohasem lesz biztonság.”*
Teller

### *Bevezetés*

A nemzetállamok legkézenfekvőbb társadalmi ellenőrzési szervezetei évszázadok óta kétséget kizáróan a katonaságok voltak. A társadalmak működésének szempontjából mindig is léteztek olyan infrastruktúrák, amelyek elérhetősége és használata kulcsfontosságú szereppel bírt, ilyen például a vízhálózat. A különbség napjainkban ezek rendelkezésre állásának biztosításában van, valamint az esetleges fennakadásokból fakadó társadalmi elégedetlenség megnyilvánulásaiban.

**Biztonság:** *„az eszközök, rendszerek és hálózatok olyan megkívánt állapota, amelyben a veszélyek megfelelő szintű kezelése megtörténik.”* [10, p. 10]

### *A biztonság, mint állapot*

A biztonság szó, mint jelző a latin *securus* szóból ered, ami alatt legfőképpen a szorongástól mentes állapotot értették a 16. században. [11] más formában szintén latinul *sine cura* azaz „gond nélkül” alakban is használatos. [12] A biztonsággal szoros kapcsolatban álló fogalmak a *védelem* és a *rendszer* mely előbbi esetében egy számunkra kedvezőtlen kimenettel rendelkező esemény ellenében foganatosítunk intézkedéseket, amelyet egy logikusan felépített struktúra követ. Ahhoz, hogy **rendszernek** hívjuk, ahhoz szükség van a **szabályok szervezett hálózatára**, hiszen ez alapján működik. [13, pp. 70-72] A biztonság állapotként történő definiálása során olyan megközelítéssel is találkozhatunk, hogy a biztonság „*egy olyan kedvező állapot, melynek megváltozása nem valószínű.”* [14] A katonai műszaki tudományok területéhez hozzátartozik minden olyan haditechnikai eszköz fejlesztése, technológiának kutatása, amelyek később a védelmi szektorban alkalmazhatók. [15] Az információbiztonság és informatikai biztonság közötti eltérés a rendszerben kezelt és tárolt dolog védelme és maga a rendszer védelmében keresendő. Ezeknek az informatikai rendszereknek védelmének érdekében lett megalkotva a 2013. évi L. az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény. [16]

A komplex kockázati modell megközelítésben [17] jellemzően négy kockázati tényezőt szükséges figyelembe venni:

- **az emberi tevékenységből fakadó kockázatot;**
- a technika alkalmazásából származó kockázat (ilyen például a rendellenes működés vagy a meghibásodás);
- a környezet közrehatásából származó kockázati hatások (például elemi csapások);
- a gazdasági kockázatot.

Az emberi tevékenység során mindig is fellelhető volt az egymás közötti tudatos információs tevékenység, amely során a szemben álló felek hírszerzést (kémkedést), félrevezetést, propaganda- és nyilatkozatháborút, valamint ezek rokontevékenységeit alkalmazták kölcsönösen egymás ellen. Azonban ezek sosem voltak annyira tudatosan tervezettek, mint amit napjainkban információs hadviselésnek, NATO terminológiában **információs műveleteknek** nevezünk. [18] [19]

Az információs műveleteket alkotó elemek közé sorolandók: [20]

– a műveleti biztonság (Operation Security – OPSEC);
– a katonai megtévesztés (Military Deception – MILDEC);
– **a pszichológiai műveletek (Psychological Operations – PSYOPS);**
– a fizikai pusztítás (Physical Destruction – PD);
– az elektronikai hadviselés (Electronic Warfare – EW);
– a számítógép-hálózati műveletek (Computer Network Operations – CNO).

**Lélektani hadviselés:** *„szűkebb értelemben a titkos, manipulatív befolyásolás módszerei, tágabb értelemben minden olyan, közvetlenül halált nem okozó eszköz és módszer, amellyel háborúban és békében az emberek erkölcsileg, politikailag, eszmeileg, érzelmileg célzatosan és tudatukon kívül befolyásolhatók. Mindkét értelmezés szerint fő módszerei a félrevezetés, a lejáratás, a rágalmazás és a pánikkeltés. Fő eszközei a befolyásoló ügynökök és a tömegtájékoztatási apparátusok."* [21]

**Manipuláció:** Olyan viselkedés, amelynek célja mások kihasználása, ellenőrzése vagy más módon történő befolyásolása előnyszerzés érdekében. [22]

### *A manipuláció helye a lélektani hadviselésben*

A NATO terminológiában a **pszichológiai műveletek** (PSYOPS) célja a pszichológiai tényezőkre alapuló **lélektani hadviselés** (PSYWAR) folytatása. A PSYOPS alapelvei között szerepel az érzékelés, az attitűd és a hozzáállás befolyásolása célzott személyek és csoportok irányába, valamint a szövetséges küldetési célokkal kapcsolatban megfogalmazott magatartás megerősítése és serkentése. A PSYOPS tervezésnek összhangban kell lennie az **információs célokkal** (IO) amelyek az **operációs tervben** (OPLAN) vannak kifejtve és meghatározva. A **közügyekkel** (PA) ellentétben kizárólagos kontrollal rendelkezik a tartalmak és a célközönség kiválasztásában. A hatékony PSYOPS számára fontos a megfelelő intellektuális apparátus megléte, olyan erőforrások is, mint például a nyelvi támogatás, a grafikai tervezés és sokszorosítási kapacitások, médiasugárzási és egyéb szállítási megoldások. Az üzenetküldési módok között szerepelnek a személyes találkozások, hangosbemondók, a nyomtatott sajtó, telefon és fax, a rádió, a televízió és az internet. Saját eszközök alkalmazásán felül a helyi médiaszolgáltatók is érintettek lehetnek. A befolyás, mint különleges támogató eszköz pedig növelheti a tervezési spektrumot és a tevékenység volumenét. [23] A **katonai megtévesztés** (MILDEC) olyan tevékenység folytatását jelenti, ami ellenséges katonai, félkatonai vagy szélsőséges szervezet döntéshozóit olyan cselekedetre (vagy passzivitásra) sarkallja, ami a szövetséges küldetés sikerét elősegíti. Továbbá jellemzi az is, hogy az ellenséges fél rossz következtetéseket vonjon le az elemzések során, az OPSEC tevékenység emellett arra törekszik, hogy minden valós információt tagadjon, védve a helyes dedukcióját a szövetséges terveknek. [24] A tudományos kutatások katonai ügynökségek általi finanszírozása jól mutatja, hogy a jövőben a pszichológiatudomány a technikai összetevőkön felül is képes eszközöket biztosítani a társadalmi kontrolltechnikák támogatására, viszont nem jelenti azt, hogy ez a pszichológia és a kapcsolódó tudományágak fő alkalmazási területének bizonyulna. Ha azonban az igény továbbra is fennáll, akkor valószínűnek tűnik, hogy a jövőben pszichológiatudomány területén jelentős társadalmi kontrollalkalmazások rejlenek. Elsősorban a tudástermelés a tudományban az egyéni kézműves folyamatból egyfajta iparággá változott, és ezt az ipart, ha közvetve is, de az azt finanszírozó ügynökségek irányítják. Másodszor, ha a jelenlegi politikai és gazdasági légkörben a nyilvánvaló tendenciák fennmaradnak, akkor valószínű, hogy a fejlett államok társadalmi ellenőrzési alkalmazásaival szemben támasztott követelmények növekedni fognak. [25, p. 35]

## 1.1 A pszichológiai manipuláció történeti háttere

A manipulatív tevékenységek alkalmazása az emberi interakciókban egyidős lehet a magántulajdon megjelenésével. Már az ókorban is fellelhető a manipuláció katonai alkalmazása, példaként említve a pelusiumi csatát (i.e. 525), ahol a perzsák kihasználva az egyiptomiak a macskák iránti vallásos tiszteletét, állatokat dobtak eléjük, akik visszarettentek azok megsértésétől. [26] A történelem során számtalan alkalommal a civil lakosság ellen elkövetett tömeges brutalitás sem volt jellemzően megalapozatlan cselekedet, hanem kifejezetten katonai célokat szolgáltak. Azt kívánták elérni a leplezetlen pusztítással, hogy az elfoglalni kívánt terület lakosságának tudatába és mindennapjaiba betérjen a rettegés, ez által csökkentve az ellenállóképességet, ami a támadó csapatok veszteségeit is képes volt redukálni.

### *A hírszerzés és a dezinformáció alkalmazásának kezdeti elvei*

Szun-Ce ókori hadvezér számos fordításban és címmel megjelent (a legismertebb változat „A háború művészete") írásában a XIII. részben értekezik a kémek alkalmazásáról, ahol leírja, hogy fel kell ismerni az ellenség által küldött kémeket és saját szolgálatunkba kell állítanunk azokat, méghozzá olyan eszközök alkalmazásával, mint a számukra előnyös helyzetek megteremtése, amely révén saját érdekeink mentén leszünk képesek alakítani az általuk végzett cselekményeket. Különbséget tesz az „élet" és a „halál" kémjei között, mely utalása tevékenységük irányát szabja meg, amely lehet szövetséges érdekeket képviselő, valamint ellenséges erőket célzó. Említést tesz az időbeliség és az információ birtokában lévő döntéshozatal fontosságáról is. [27]

### *A múlt század hajnalán*

A 20. század elején Roscoe Pound amerikai jogtudós szerint a jog egy eszköz, ami arra szolgál, hogy a társadalmat formálja annak érdekében, hogy szabályozza annak viselkedését. Itt kerül megfogalmazásra a ***„theory of social engineering"*** [28], a társadalmi tervezés, ami más helyeken szociális tervezés[1] [29], Karl Popper szociológiájában lépésenkénti társadalomjavítás [30, pp. XI-XII] [31] [32] elméletként is

[1] Chiang megemlíti könyvének 259. oldalán, hogy 1979-ben az angolra fordítva *Economic Management* folyóirat első számában közölt egy cikket a következő címmel: „A technológia, ami szervezi és irányítja a szocialista újjászervezést – társadalmi tervezés". A kínai címben „shehui gongcheng" kifejezéssel jelenik meg a „social engineering" fogalom

előfordul. A fent említett fogalmak lényege centralizált tervezés útján való beavatkozás a társadalom fejlődésének, illetve a jövőt illető szabályozás alakításába, valamint a társadalom ezekre való reagálásának befolyásolási kísérlete, amihez jogi, politikai, gazdasági és katonai eszközök alkalmazására egyaránt feltétlenül szükség van. Marklund 2008-as írása hasonló megközelítéseket feszeget, ahol az Egyesült Államokat és Svédországot hozza példaként, elemzésében kitér a politika és a tudomány kapcsolatára, valamint arra, hogyan lett kommunikálva az említett koncepció. [33] Általánosságban elmondható, hogy amikor pszichológiai manipulációról (social engineering) beszélünk, valamilyen informatikai csalási technikára gondolunk, amely arra ösztönzi az áldozatot, hogy olyan információkat adjon ki a támadó számára, amelyekhez alapértelmezés szerint nincs jogos hozzáférése. Ha azonban a pszichológiai manipuláció hatásait magasabb szinteken vizsgáljuk, akkor nyilvánvalóvá válik, hogy valójában az emberi döntési mechanizmusba való beavatkozásról van szó, és ezek a szintek csak a stratégia céljában térnek el egymástól. [34]

**Továbbfejlesztett definíció a social engineering fogalmára**

***A social engineering olyan pszichológiai manipulációs taktikák összessége, amelyek célja a gondolkodásmód (vagy felfogás) kompromittálása az egyén szintjétől a tömegekkel bezárólag. Más szóval, ez egy beavatkozás az emberi döntéshozatali algoritmusba.***

Pound elméletében a törvényhozók (jogalkotók) egyfajta mérnöki szerepet töltenek be a társadalomban, ahol ők azok, akik módszeresen megtervezik a társadalomra érvényes szabályokat. Joggyakorlatában hat olyan elemet határoz meg, amit társadalmi érdekeknek nevez, [35] amelyeknek közös alapelvei vannak az emberi biztonsággal.

A hat elem a felsorolásban említett fogalmakhoz fűződő érdekből fakad, mint

1. az általános biztonság
2. a szociális intézmények biztonsága
3. az általános erkölcsök
4. a társadalmi erőforrások megőrzése
5. az általános előrehaladás és
6. az egyén életének védelme

A társadalmi érdekek esetében **nem tesz különbséget köz- és egyéni érdekek között**, mert ezek általában átfedik egymást. A jog vége című részben azt is leszögezi, hogy a

társadalom működésének vizsgálata a fizikai tudományokhoz képest nem a „mi van” megfigyelésével foglalkozik, hanem a „minek lennie kellene” vizsgálatával. , azaz egy ideális társadalmi működés módszertanát igyekszik kutatni. [36]

- **Általános biztonság:** Ez azt jelenti, hogy a társadalmi életet biztosítani kell a társadalom létét veszélyeztető cselekedetekkel és magatartási formákkal szemben.
- **Szociális intézmények biztonsága:** Ez a társadalmi életben megkövetelt alapvető intézmények biztonságának igénye, mint például a hazai intézmények, a vallási intézmények, a politikai intézmények és a gazdasági intézmények.
- **Általános erkölcsök:** Ez azt jelenti, hogy nem szabad eltűrni az erkölcsi érzelmek elleni sértő magatartást, ideértve az olyan tevékenységeket is, mint a tisztességtelenség, a korrupció, a szerencsejáték és az erkölcstelenségre hajlamos dolgok.
- **Társadalmi erőforrások megőrzése:** Ez egy olyan közös erőforrás kezelésének igénye, amely nem az egyén tulajdonában van, ezért védeni kell a visszaélésektől és a pazarlástól.
- **Általános előrehaladás:** Ez az az igény, hogy az emberi hatalom és a természet feletti emberi kontroll támogassa a gazdasági, politikai és kulturális haladást, valamint a fejlődést.
- **Az egyén életének védelme:** Ez az a kinyilatkoztatás, amely szerint minden egyén képes legyen emberi életet élni egy civilizált társadalomban az adott társadalom normái szerint.

***A világháborúk korában***

A második világháborús terrorbombázások (London, Coventry, Rotterdam, Drezda) azaz az elsősorban a nem katonai célpontok, hanem a lakosság ellen irányuló szőnyegbombázások is a lélektani hadviselés eszközei közé sorolhatók. A sztálingrádi csatában a szovjet csapatok sikeresen alkalmaztak egy röplapot (*bulletin*), amelyen az állt, hogy három nappal azelőtt 24 ezer német katona adta meg magát, az előző napon 36 ezren, aznap, november 25-én 51 ezren. Három nappal azelőtt a német hadsereg 26 ezer katonát veszített, előző nap 41 ezret, aznap, november 25-én a veszteség 47 ezerre nőtt. Majd felhívás következett: a német katonák kövessék 51 ezer társuk példáját. [37] A Holokauszt a nácik számára egy modern társadalom kialakítását jelentette, ahol a nemkívánatos tényezőktől igyekeztek megszabadulni, mindezt tették úgy, hogy mérnöki

logikára épülő rendszert építettek ki a cél elérésére. Hasonlóan egy gyárhoz, aminek bemeneti elemei (input) és kimeneti elemei (output) vannak, a koncentrációs táborok is tervezett struktúra mentén üzemeltek. Egy hatékony mechanizmusnak bizonyult, amely tömeges mértékű emberi pusztítást szolgált. [38, pp. 28-29] A hidegháború ideje alatt pedig a két szuperhatalom, az Egyesült Államok és a Szovjetunió közötti versengés egyik kulcseleme volt. A háborús propaganda, a lélektani hadviselés a második világháborúban még csak kiegészítő jellegű volt a tényleges hadviselés mellett, 1945 után viszont kulcsszerepet töltött be. A szembenálló felek egyaránt tartottak egymás hírszerző szolgálataitól, valamint a nukleáris fegyverkezés és az űrverseny hajtóerejét képezte az egymás iránti kölcsönös bizalmatlanság is. [39]

### *Amerikai léggömb-propaganda a hidegháborúban*

A hidegháború alatt az egyik leghatékonyabb hírterjesztési eszköz a rádió volt. A vasfüggöny, mint műszaki akadály választotta el a nyugati világot a keleti blokktól. Az Egyesült Államok Információs Hivatala (továbbiakban: USIA) alkalmazásában számos eszköz volt, ami a lélektani hadviselés célját szolgálta. Az 50-es években indult Szabad Európa Rádió (SZER) is egy propaganda eszköz volt, amely az amerikai Központi Hírszerző Ügynökség (továbbiakban: CIA) támogatásával folytatta tevékenységét. Feladata mindkét szervezetnek elsősorban a kommunista vezetésű országok destabilizálása, valamint a lakosság informálása volt irányított és szervezett forgatókönyv alapján. Ebben az időszakban indult a ballon-hadművelet is, amely során propagandaröplapok terjesztése kezdődött légballonok segítségével. Az USIA havonta 2000 közlemény, 3000 újság, folyóiratok és szórólapok kerültek „bevetésre”. 1956-ig megközelítőleg 300 millió röplapot szórtak szét a moszkvai befolyási övezet tagállamai felett. [40] Az ***információs hadviselés*** fogalma a Perzsa-öbölben 1990. augusztus 2. és 1991. február 28. között zajló katonai konfliktushoz kapcsolódik, új fejezetet nyitott a hadműveletek történetében. Ez volt az első olyan háború, amelyben élőben számoltak be a folyamatban lévő eseményekről. A nézők valós időben nyerhettek betekintést a harci akciókba, a CNN riporterei a sokszor akadozó kommunikáció ellenére egy bagdadi szállodából próbálták tartani a kapcsolatot Washingtonnal. A háborúról szóló tudósításokban a televízió rendkívül korlátozott képet adott, a csatákról készült videofelvételek többségét továbbra is az Egyesült Államok Védelmi Minisztériuma biztosította. Az éjjellátó berendezéssel készített felvételek fantasztikusan és futurisztikusan néztek ki, sok nézőt egy videojátékra emlékeztetve. [41]

## 1.2 A kibertér és a kritikus infrastruktúrák szerepe a társadalmi biztonságban

**Kibertér:** *„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.”* [42]

***A kibertér elhelyezkedése a fizikai térben***

Számos definíció és megfogalmazás kering a kibertérről [43, p. 51] [44, p. 11], ami alatt a szerzők a számítógép-hálózatok által kialakított virtuális környezetét értik, amivel a fizikai térben zajló eseményekre támogató, építő, adott esetben káros, romboló hatásokat vagyunk képesek előidézni. Az automatizáció következéseképpen megjelentek olyan infrastruktúrák, amelyek a magját adják a komplex rendszerek működésének, folyamatos rendelkezésre állást biztosítva. Ezek a magyar jogalkotásban a létfontosságú rendszerelemek, másnéven **kritikus infrastruktúrák**, például erőművek, távvezetékek, adatközpontok, pénzintézetek stb., amelyek működésében bekövetkező hiba súlyos kihatással lehet a társadalom mindennapi életére. [45] [46] Ezért ezeknél a létfontosságú struktúráknál kiemelt figyelmet kell szentelni a védelmi megoldások kialakítása során, annak érdekében, hogy csökkentsük egy lehetséges anomália előfordulásának esélyét, valamint folyamatos felülvizsgálatokra van szükség. [47]

Az ENSZ Katasztrófakockázat-csökkentési Hivatalának meghatározása szerint:

**Kritikus Infrastruktúra:** Azok a fizikai struktúrák, létesítmények, hálózatok és egyéb eszközök, amelyek egy közösség vagy társadalom társadalmi és gazdasági működéséhez elengedhetetlen szolgáltatásokat nyújtanak. [48]

A magyar terminológiában „létfontosságú rendszerelemek” néven kerültek definiálásra a kritikus infrastruktúrák, amelyet a 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény szabályoz.

**Létfontosságú rendszerelem:** *„…szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához”* [49]

### *A kritikus infrastruktúrák*

A társadalmi biztonság a koppenhágai iskola [50] egyik szektora mely szektorban vizsgáljuk egy országban a szervezett bűnözés megjelenésének valószínűségét, az elhárító szervezetek ezekkel szembeni fellépőképességét, valamint fenyegetettségét esetleges terrorcselekményekkel szemben [51], illetve az ezek kiváltását előidéző politikai magatartást. [52] [53] A társadalom biztonságérzetére a legnagyobb hatást a kritikus infrastruktúrák elleni támadások gyakorolnak, hiszen sikerességük esetén a mindennapos működés bénul meg. Az angolszász országokban tizenhat [54], a magyar szabályozás esetében tíz szektort/ágazatot különböztetünk meg. Magyarország az Európai Unió keretein belül szerepet vállalt elsősorban a saját, valamint az összekapcsolt közösségi hálózatok védelme érdekében is. A védelem kialakításához szükséges volt a jogszabályi területen is megalkotni és elfogadtatni azon intézkedéseket, melyek megteremtették a feltételeket a hatékony fellépésre a kihívásokkal szemben. [55, p. 350]

Ezek védelmének fontosságára több olyan veszélyes incidens is felhívta a figyelmet, amelyek meggátolták, blokkolták, vagy zavarták olyan, elsősorban informatikai eszközökkel vezérelt hálózatok működését, amik biztosítják a bankszektor, az energiaellátás, a közigazgatási hálózatok, vagy más fontos infrastruktúrák szolgáltatásait. [56] A Magyar Telekom és az OTP Bank elleni támadások [57] rövidtávon megmutatták ennek jelentőségét. Előfordul az is, hogy ilyen rendszerek kerülnek pénzügyi haszonszerzés motivációja révén csalási szándékok célkeresztjébe. Erre volt példa a dél-ukrajnai atomerőmű esete, ahol egy munkavállaló kriptovaluta bányászatának céljával vitt be egy számítógépet az erőmű területére, amit a hálózatra kapcsolt. Az ukrán titkosszolgálat (SBU) számolta fel a tevékenységet. A napi szinten 1000 euróra tehető bevételszerzési tétel eltörpül annak a kockázata mellett, hogy az erőművi termelésbe potenciális sebezhetőség került az által, hogy egy dolgozó privát számítógépet kötött a helyi hálózatba. [58]

A zavartalan működéshez szükséges a célnak megfelelő kommunikáció biztosítása is. [59, p. 62] A kritikus információs infrastruktúrák olyan létesítmények, amelyek a létfontosságú rendszerelemek működésének ellehetetlenülését jelentik meghibásodás, vagy tartós kiesés során. A **hálózati** és **információs rendszerek biztonságáról** (NIS) az Európai Unióban egységesen magas szintjét biztosító intézkedésekről a 2016/1148/EU európai parlamenti és tanácsi irányelv (a továbbiakban: NIS-irányelv) ad útmutatást. [60]

### *A NIS2 irányelv*

2023. január 16-án hatályba lépett az (EU) 2022/2555 (NIS2) irányelv, amely felváltotta az (EU) 2016/1148 irányelvet. Az ENISA úgy véli, hogy a NIS2 különböző módokon javítja a jelenlegi kiberbiztonsági státuszt EU-szerte: [61]

- a szükséges kiberválságkezelési struktúra (CyCLONE) létrehozása
- a biztonsági követelmények és a jelentési kötelezettségek harmonizációjának növelése
- arra ösztönzik a tagállamokat, hogy vezessenek be olyan új érdeklődési területeket, mint az ellátási lánc, a sebezhetőségek kezelése, az alapvető internet és a kiberhigiénia nemzeti kiberbiztonsági stratégiájukban
- új ötletek, például szakértői értékelések bevezetése a tagállamok közötti együttműködés és tudásmegosztás fokozására
- a gazdaság és a társadalom nagyobb hányadának lefedése több ágazat bevonásával, ami azt jelenti, hogy több szervezetnek kell intézkedéseket hoznia a kiberbiztonság szintjének növelése érdekében.

A NIS2 számos jelentős új feladatot ruház az ENISA-ra, mint például:

- Egy európai sebezhetőségi nyilvántartás fejlesztése és karbantartása
- Az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatának (CyCLONE) titkársága
- Éves jelentés közzététele a kiberbiztonság helyzetéről az EU-ban
- A tagállamok közötti szakértői értékelések megszervezésének támogatása
- Nyilvántartás létrehozása és karbantartása határokon átnyúló szolgáltatásokat nyújtó jogalanyok, például DNS-szolgáltatók, TLD névregiszterek, tartománynév regisztrációs szolgáltatásokat nyújtó entitások, számítási felhő szolgáltatók és adatközpont-szolgáltatók számára.

### *Általános Adatvédelmi Rendelet (GDPR)*

A 2018. május 25. óta hatályos európai rendelet sok szempontból változtatta meg a hétköznapi berendezkedést. Először is azért, mert az eddig a szőnyeg alá söpört kérdés a közgondolkodásban nagyobb szerepet kapott. Az egyre szélesebb körben elterjedt digitális adatgyűjtés és kezelés, az internet nyújtotta kommunikációs és kereskedelmi lehetőségek térnyerése (elektronikus levelezés, e-kereskedelem, hivatali ügyintézés stb.) szükségszerűen egységes európai keretrendszer megalkotását szorgalmazta. A jogszabály

életbelépésével széles körben terjedt el az adatvédelmi nyilatkozatok és tájékoztatók közzététele, mely a vállalati és a közszféra szereplőit egyaránt kötelezte arra, hogy az általuk kezelt adatok jogos érdekhez fűződő mivoltából fakadóan adjanak tájékoztatást a felhasználók számára, hogy hogyan és miért gyűjtenek adatokat. Az általános adatvédelmi rendelet (GDPR) a természetes személyek adatainak védelmének érdekében alkotott uniós jogszabály, amely a magánszektor és a közszféra nagy része által történő adatkezelés szempontjából fontos. A bűnüldözési célra történő adatfeldolgozás külön irányelv hatálya alá tartozik. Rendszerezi azokat a szabályokat, amelyek korábban az adatkezelést szabályozták, lehetővé téve a vállalkozások és kormányzati szervek számára az adminisztratív terhek csökkentését, továbbá létrehozta a független felügyeleti hatóságok rendszerét, amely felelős a megfelelőség nyomon követeséért és a szabályok érvényesítéséért. [62]

Az informatikai terminológiában a felhasználói szintű biztonság (user-level security) alatt jellemzően az egyénre vonatkozó jogkörök leosztását értjük. Ez egy felhasználók csoportján belüli különbségtételt eredményez. Szervezeti szinten tekintve fontos, hogy ezek a felhasználók egyedileg azonosítottak, egyedi felhasználónév és jelszó párossal rendelkeznek. A klasszikus felhasználóazonosítási folyamatban (authorization process) ezek az adatok kerülnek ellenőrzésre, mielőtt egy felhasználó alkalmazásokat használ. Egy lépcsővel messzebb haladva, a biztonságérzet vizsgálatát nézve az a meghatározó különbség, hogy a biztonsági előírások és módszerektől függetlenítve a felhasználó mennyire érzi magát komfortosan egy olyan közegben, ahol számos fenyegetettségnek van kitéve a tevékenysége során. A kibertérben ma már az adathalászati és egyéb csalási tevékenységek természetes része a mindennapoknak, így folyamatos éberséggel kell a dolgunkat végeznünk.

## 1.3 A „social engineering” technikák az informatikában

Az informatikai biztonság területén a pszichológiai manipuláció, angolul ***„social engineering”*** kifejezés (továbbiakban: SE) azt jelenti, hogy az emberi tényezőket kiaknázva szerzünk jogosultságot (hozzáférést) olyan adatokhoz és/vagy információhoz, amelyekhez alapvető esetben nem lenne felhatalmazásunk.

Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) definíciója szerint:

*„A social engineering minden olyan technikára vonatkozik, amely arra irányul, hogy a célszemélyt konkrét információk felfedésére vagy törvénytelen okokból meghatározott művelet végrehajtására rávegyék.”* [63]

Kevin Mitnick, hacker legenda komoly eredményeket ért el a SE területén, több könyv szerzője a témában. [64] [65] Neve egybeforrott azzal az újszerű jelenséggel, amely során a modern eszközök adta lehetőségeket kihasználva lényegében hírszerzői tevékenységet végzett. A megtévesztés különböző eszközeit alkalmazva személyek irányítása, mely során bizalmas vagy személyes információ birtokába való jutást követően csalási szándékkal alkalmazható. Ezeknek a megszerzése lehetséges technológiai eszközökkel, de akár anélkül is. [66]

Az online és/vagy kibertérben ez a technika túlnyomó többségében adathalászati céllal jelenik meg. Ezeket a technikákat azért illetem a modern jelzővel, mert ugyan a modern korra jellemző alkalmazási területen, az informatikában honos manapság a kifejezés, ha jobban belegondolunk, akkor nyilvánvalóvá válik, hogy a technikák jelentős része közel sem új keletű, mint például az, hogy másnak adjuk ki magunkat, mint akik valójában vagyunk. Az egyik legismertebb kártékony kód elnevezése is a trójai (***trojan***) az ókori görög időkbe nyúlik vissza. A mondavilágban híres történetben a katonák egy fából készített lovat ábrázoló építményben bújtak meg, az informatikában pedig egy ránézésre ártalmatlan programba beágyazott kártékony kódról van szó. A zsarolás/lejáratás (***blackmailing***) egy olyan manipulációs technika, ahol a támadó olyan információk (jellemzően dokumentált tartalmak) birtokában van, amivel arra kényszeríti a célpontot, hogy az általa deklarált instrukciók mentén alakítsa tevékenységét. Az üzleti életben ez lehet üzleti titok kiszivárogtatása, negatív sajtómegjelenés, pénzügyi visszaélésekre, tisztességtelen piaci magatartásra vonatkozóan terhelő információk, kezelt adatokkal való visszaélés jelentheti a zsarolás tárgyát. Politikai vonatkozásban gyakoriak az anyagi

természetű zsarolások (pl. korrupció, sikkasztás, csalás), társadalmi megítélésre negatív hatást gyakorló cselekmények és hitelességi válságot okozó elemek alkalmazása. Mindkét esetben a leggyakoribb, hogy a támadó pénzügyi haszonszerzés céljával végzi tevékenységét, az utóbbi években pedig a kriptovalutákban történő teljesítés sem újkeletű.

Egy másik hasonlóan széles körben alkalmazott technika az adathalászat (***phishing***), ahol a támadó belépési azonosítók, jelszavak, fizikai réteg (***token***) ebben a vonatkozásban olyan eszköz, ami közvetítő szerepet tölt be egy folyamatban pl. azonosítás, bankkártyaadatok stb. után kutat. Leggyakoribb megjelenési helye az elektronikus levelezésben az úgynevezett kéretlen levelek (***spam***) között van, ahol a támadók általános esetben célzás nélkül, nagymennyiségben küldenek leveleket bennük kártékony kódokra mutató hiperhivatkozásokkal, amikre való kattintás után az áldozat számos kedvezőtlen kimenetnek lesz kitéve. [67] A gázlángozás a pszichológiai manipuláció egyik formája, ahol a bántalmazó megpróbál önbizalomhiányt és zavart helyzetet kelteni áldozata elméjében. A manipulátor a valóság eltorzításával az áldozat saját ítélőképességének és intuíciójának megkérdőjelezésére törekszik, amely által képes irányítást szerezni a megcélzott személy döntési képessége, így az áldozat önrendelkezése felett is.

A gázlángozás (***gaslighting***) kifejezés az 1938-as Angel Street című darabból származik, amelyet később Alfred Hitchcock a Gaslight című filmébe adaptált, amelyben egy férfi megpróbálja elhitetni a feleségével, hogy a nő megőrült, lehetővé téve azt, hogy lophasson tőle. Amikor a nő felkapcsolja a villanyt a padláson, hogy nekiálljon megkeresni az ékszergyűjteményét és ezzel egyidőben a földszinten elhalványulnak a gázlámpák, a férfi azt mondja neki, hogy mindez csupán a képzelete szüleménye, mely után a nő fokozatosan elkezdi megkérdőjelezni saját emlékezőképességét. [68]

### *Közkedvelt támadási típusok a kibertérben*

Ebben az alfejezetben ismertetem a pszichológiai manipuláció során alkalmazott informatikai módszereket [69] amikkel a kiberbűnözők csalási tevékenységük során igyekeznek az áldozatokat értékes információk átadására késztetni. Ez az a bizonyos technológiai háttér, ami a manipulatív módszerek mellett jelenik meg, mondhatni az informatikai támogatása a csalási technikáknak. Célpontjai jellemzően vállalatok és kormányzati szervek hálózatai, mivel ezek az intézmények rendelkeznek a legnagyobb valószínűséggel értékesíthető információkkal.

- Denial-of-service (DoS) and distributed denial-of-service (DDoS) támadások [70]

A ***szolgáltatás megbénítás*** (DoS) és az ***elosztott szolgáltatás-megtagadásos*** (DDoS) támadások célja a hálózati szolgáltatások megzavarása melyek során a webhelyeket és a kiszolgálókat célozzák meg és igyekeznek kimeríteni az adott alkalmazás erőforrásait.

- Man-in-the-middle (MitM) támadások (beékelődéses támadások) [71]

• **IP-hamisítás:** A kiberbűnözők megváltoztatják egy webhely, e-mail-cím vagy eszköz internet protokoll (IP) címét, és meghamisítják az entitást – így a felhasználó azt hiheti, hogy megbízható forrással kommunikál, amikor valójában információt ad át egy rosszindulatú szereplőnek.

• **DNS-hamisítás:** A Domain Name System (DNS) hamisítása esetén a spamküldő egy olyan hamis webhelyet üzemeltet, amelyet a felhasználók ismernek és ide is tereli őket annak érdekében, hogy felhasználói és hitelesítő adatokat vagy egyéb információkat szerezzenek meg.

• **HTTPS-hamisítás:** A felhasználó azt feltételezi, hogy egy webhely rendelkezik egy HyperText Transfer Protocol Secure (HTTPS) protokollal, ami azt jelenti, hogy számítógépe adatai titkosítva vannak a webhelygazda számára. Azonban titokban átirányították őket egy nem biztonságos HTTP-webhelyre, lehetővé téve a bűnözők számára, hogy nyomon kövessék az interakciókat és információkat lopjanak el.

• **E-mail-eltérítés:** A támadók titokban hozzáférnek egy banki vagy hitelkártya-társaság e-mail fiókjához, amit arra használnak, hogy figyelemmel kísérjék a tranzakciókat és információkat lopjanak el. Az ellopott e-mail fiókot vagy a ténylegestől némileg eltérő hamisított e-mail címet továbbá úgy hasznosítják, hogy hamis utasításokat adnak az ügyfeleknek például, hogy utaljanak át egy összeget egy új folyószámlára.

• **Wi-Fi lehallgatás:** A spammerek nyilvános Wi-Fi hálózatokat vagy hotspotokat hoznak létre, amelyek egy közeli vállalkozásnak vagy más megbízható forrásnak tűnnek. Azok a felhasználók, akik csatlakoznak ehhez a hálózathoz, minden tevékenységük és érzékeny adatuk ellopásra kerül.

**SSL-eltérítés:** A HTTPS-hamisítás kiterjesztett változata, amikor a támadó a Secure Sockets Layers (SSL) protokoll felett átveszi az irányítást, ami a HTTPS-kapcsolatok titkosításáért felel. Elfogja a közöttük és a kapcsolódni kívánt szerver között mozgó felhasználói adatokat.

**Munkamenet-eltérítés:** Böngésző sütilopásként (browser cookie theft) is ismert támadási forma, ahol a támadó ellopja a webböngésző sütijein tárolt információkat, mint például a mentett jelszavakat.

- Phishing and spear-phishing támadások [72]

***Adathalászat***

A szokásos adathalász kampányok alapesetben nagy szórást alkalmaznak, tehát arra törekednek, hogy minél szélesebb közönséget érjenek el vele, ezzel szemben a szigonyozásos adathalász e-mailek a számítógépes bűnözés célzottabb megközelítését jelentik. Ez azonban nem teszi kevésbé fenyegetővé a szokványos adathalászatot. Az adathalászok általában e-mailben terjesztik átveréseiket és habár véletlenszerű személyeket céloznak meg telefonhívások: ***„vishing"*** vagy szöveges üzenetek: ***„smishing"*** útján, az adathalászat végeredményében egy mennyiségi játék, több ezer próbálkozásból legalább egy előbb-utóbb sikeres lesz.

A szigonyozásos adathalászati módszert alkalmazó támadókkal ellentétben azonban a mezei csalók személytelen, de sürgető nyelvezetet használnak arra, hogy az olvasókat rosszindulatú melléklet letöltésére vagy nem biztonságos hivatkozásra való kattintásra késztessék, így személyes adatok, mint például hitelkártyaadatok vagy bejelentkezési adatok felfedésére manipulálják őket.

Az adathalászat sokféle módon történhet, többek között:

**Vishing:** az adathalászat telefonhívásokon vagy internetprotokollokon keresztüli hangátvitel, Voice over Internet Protocol (VoIP). Lényege a hangalapú eszközök használata.

**Smishing:** Adathalászat szöveges üzeneteken keresztül, más néven SMS adathalászat. A számítógépekhez hasonlóan a hackerek is megfertőzhetik a telefonokat rosszindulatú programokkal.

**Üzleti elektronikus levelezés kompromittálása (Business Email Compromise):** A szigonyozásos támadásokhoz hasonlóan az általános adathalászati kísérletek is hamisított vagy feltört e-mail-címeket használnak az áldozatok csalogatására.

**Banki átutalásos adathalászat:** Az adathalászat ezen formája csalárd szervezeteknek történő banki átutalásokra irányul.

***Szigonyozásos adathalászat***

A szigonyozásos adathalászat a módszer fejlettebb formája. A szigonyozás egy célzott támadás egy kiválasztott áldozat ellen, míg a szokványos adathalászat emberek tömegeinek átverésére tesz kísérletet. A szigonyozásos adathalászat során a csalók gyakran alkalmaznak manipulációt és hamisított e-maileket, hogy konkrét személyeket célozzanak meg egy szervezeten belül. Kiadhatják magukat családtagoknak, kollégáknak vagy üzleti ismerősöknek is akár. A csalók arra használják a közösségi médiát, hogy legitimálják a célpontjukkal kapcsolatos információk megszerzésére irányuló kéréseiket. Amikor kapcsolatba lépnek a célponttal, név szerint szólítják meg, személyes tényeket és hétköznapi nyelvezetet használnak. Rosszindulatú programokat is használhatnak személyes adatok gyűjtésére. Elsődleges céljuk az alkalmazottak manipulálása érzékeny adatok felfedésére vagy jogosulatlan műveletek, például a csalók által üzemeltetett cégeknek történő elektronikus átutalások végrehajtására buzdítják őket.

Az ilyen jellegű csalók általában kétféle támadást alkalmaznak:

**Bálnavadász támadások:** Ezek a támadások felsővezetők, azaz olyan személyek ellen irányulnak, akiknek nagy valószínűséggel van hozzáférése bizalmas információkhoz és (tudatlanul) lehetővé teszik az adatszivárgást, vagy például jóváhagyhatnak egy nagy összegű pénzátutalást.

**Vezérigazgatói csalás:** Célzott támadások olyan formája, ahol a támadó alsóbb szintű alkalmazottak ellen szervezkedik, vezető beosztású személynek (például vezérigazgatónak) vagy más magas szintű kollégának adja ki magát. Ezután rákényszerítik az áldozatot, hogy jogkörében illetéktelen lépéseket tegyen.

- Drive-by támadás [73]

A drive-by támadás, vagy drive-by-download támadás, olyan kibertámadásra utal, amelyben egy rosszindulatú szkript letölti és telepíti magát a felhasználói eszközre a felhasználó kifejezett engedélye nélkül. Ez a cselekmény operációs rendszertől függetlenül megtörténhet. Ezek a támadások gyakran akkor fordulnak elő, amikor a felhasználó feltört weboldalra navigál vagy egy olyan weboldalt böngészik, amelynek a biztonsági szintje kifejezetten alacsony.

Megvalósulása két jellemző esetre vezethető le:

**Engedély nélküli eset**

Ezekben az esetekben nincs olyan közvetlen felhasználói művelet, amely elindítja a letöltést. Más szóval, a támadás akkor indul el, amikor a felhasználó felkeres egy feltört weboldalt. Anélkül, hogy az oldallal bármiféle interakcióra lenne szükség, a támadás bekövetkezik, még akkor is, ha egyetlen kattintásra sem került sor. Egy ilyen támadás létrehozásához a hacker rosszindulatú kódot fecskendez be a weboldalba, kihasználva a webhely biztonsági hibáit. Amikor a felhasználó először keresi fel az oldalt, a kód azonosítja a biztonsági réseket akár a felhasználó webböngészőjében, akár a felhasználó eszközén és ezeken keresztül indítja el a rosszindulatú program letöltését.

**Felhatalmazással, hamis ürüggyel**

Néha előfordul, hogy a letöltéssel végrehajtott meghajtó felhasználói műveletet hajt végre, de hamis engedélykérési ürügy mentén teszi azt. Ennek néhány különböző módja van, például:

- Egy felugró hirdetés sarkában van egy „X” gomb, amely bezárás gombnak álcázza magát, de az valójában katalizátorként működik a rosszindulatú letöltés elindításához, miután megnyomásra kerül
- A hivatkozási alap egy felugró ablakban (pop-up window) jogosnak tűnhet, de ha rákattint a felhasználó, elindul a letöltés.
- A biztonságosnak tűnő e-mail-melléklet valójában rosszindulatú lehet, egy social engineering (például adathalász) módszer része, és rákattintva elindul a letöltés.

Mindhárom példa egyszerű kattintással vagy gombnyomással járt csupán. Ezek a műveletek lehetővé teszik a támadó számára, hogy azt állítsa, hogy a felhasználó engedélyezte a letöltést, miközben a felhasználó valójában nem vette észre tetteik következményeit, mivel a támadó valódi szándékait elrejtették. Ily módon a hacker megúszhatja a letöltést anélkül, hogy észlelnék. Ez a fajta ráutaló magatartás adatvédelmi tájékoztatók és sütik elfogadásakor gyakran jelenik meg a mindennapokban, európai vonatkozásban a GDPR révén.

- Jelszó támadás [74]

A jelszótámadás a jelszóval védett fiókok rosszindulatú azonosítására használt különféle módszerek bármelyikére vonatkozik. Ezeket a támadásokat jellemzően olyan szoftverek segítik elő, amelyek felgyorsítják a jelszavak feltörését vagy kitalálását. A leggyakoribb támadási módszerek közé tartozik a nyerserő alapú vagy teljes kipróbálás módszere (brute force), a szótáras támadások (dictionary attack), a jelszó-permetezés és a hitelesítő adatok kitöltése.

- A teljes kipróbálás módszere a jelszó kitalálására tett kísérlet a megengedett karakterkészlet összes lehetséges kombinációján keresztül
- A szótáras támadások gyakran használt jelszavakon, például a szótárban található szavakon és azok egyszerű változatán keresztül próbálnak kitalálni jelszavakat.

Ahelyett, hogy több jelszót próbálna ki egy fiókhoz, a jelszó-permetezés néhány gyakori jelszóval próbálkozik sok fiók ellen, annak reményében, hogy legalább az egyikhez hozzáfér. Ez a módszer segít elkerülni a fiókzárolási szabályokat és így nehezebbé válik észlelni is azokat. A kiberfenyegetések szereplői a végfelhasználók jelszavainak újbóli felhasználására való hajlamát használják ki hitelesítő adatokkal. Ez magában foglalja a már kompromittált felhasználónevek és jelszavak felhasználását arra, hogy nagyszámú bejelentkezési kérelmet kíséreljenek meg (vagy „tömjenek be") egy másik webhelyre, annak reményében, hogy az egyes felhasználók újra felhasználták azokat. Ezek a leggyakoribb frontend támadások, amelyek során a rosszindulatú szereplők bejelentkezési portálokon keresztül próbálják meg feltörni a fiókokat. Van egy másik támadási célcsoport, amely a jelszótárolást célozza meg. Mivel a támadók gyakran a legkisebb ellenállás útját választják, kulcsfontosságú, hogy mindkét típus ellen védekezzenek. A jelszavas támadások folyamatosan vezetik az adatszivárgás-támadási vektorok listáját. Bár viszonylag könnyen és alacsony költséggel csökkenthetők, sok szervezet nem rendelkezik megfelelő garanciákkal. Ha a szervezetek többtényezős hitelesítést (MFA) valósítanak meg, még akkor is előfordul, hogy a jelszavak általában az egyik tényezőt képezik a folyamatban. Ezen túlmenően a rosszindulatú szereplők jellemzően fel is törik a fiókokat, hogy megalapozzanak további cselekményeket, mint például adatszivárgást elősegítő intézkedéseket hajtanak végre, egyszerű adathalászatot vagy a rosszindulatú programok hálózatokra való bejutását készítik elő.

- SQL befecskendezéses támadás [75]

Az SQL befecskendezés (SQLi) egy webes biztonsági rés, amely lehetővé teszi a támadók számára, hogy megzavarják az alkalmazás általi adatbázisában végrehajtott lekérdezéseket. Általában lehetővé teszi a támadó számára, hogy olyan adatokat tekintsen meg, amelyeket alap esetben nem tud lekérni. Ez magában foglalhatja más felhasználók adatait, vagy bármely más olyan adatot, amelyhez az alkalmazás hozzá tud férni. Sok esetben a támadó módosíthatja vagy törölheti ezeket az adatokat, ami tartós változásokat okoz az alkalmazás tartalmában vagy viselkedésében. Egyes helyzetekben a támadó eszkalálhat egy SQL-befecskendezési támadást, ezáltal veszélybe sodorhatja a mögöttes kiszolgálót vagy más háttérinfrastruktúrát, vagy szolgáltatásmegtagadási támadást hajthat végre. Egy sikeres SQL befecskendezés érzékeny adatokhoz, például jelszavakhoz, hitelkártyaadatokhoz vagy személyes felhasználói adatokhoz való jogosulatlan hozzáférést eredményezhet. Az elmúlt években számos nagy horderejű adatszivárgás az SQL befecskendezéses támadások gyakori következménye, hogy azok hírnévkárosodáshoz és szabályozási bírságokhoz vezettek. Egyes esetekben a támadó tartós úgynevezett hátsó ajtót (***backdoor***) kaphat a szervezet rendszereibe, ami hosszú távú kompromittálódáshoz vezethet és hosszabb ideig észrevétlen marad.

Néhány gyakori SQL-befecskendezési példa

- **Rejtett adatok lekérése:** ahol módosíthatja az SQL-lekérdezést, elérve, hogy további eredményeket adjon vissza
- **Alkalmazáslogika felforgatása:** ahol megváltoztathatja a lekérdezést, hogy megzavarja az alkalmazás logikáját
- **UNION támadások:** ahol különböző adatbázistáblákból lehet adatokat lekérni.
- **Az adatbázis feltárása:** ahol információkat nyerhet ki az adatbázis verziójáról és szerkezetéről.
- **Vakon történő SQL befecskendezés:** ahol a felhasználó által vezérelt lekérdezések eredményei nem jelennek meg az alkalmazás válaszaiban.

- Cross-site scripting (XSS) támadás [76]

Az XSS (Cross-Site Scripting) egy olyan támadás, amelyben a támadó rosszindulatú futtatható szkripteket fecskendez be egy megbízhatónak minősített alkalmazás vagy webhely kódjába. A támadók gyakran úgy kezdeményeznek XSS-támadást, hogy rosszindulatú linkeket küldenek a felhasználóknak, és igyekeznek rábírni a felhasználót, hogy rákattintson. Ha az alkalmazás vagy webhely nem rendelkezik megfelelő adattisztítással, a rosszindulatú hivatkozás a támadó által kiválasztott kódot hajtja végre a felhasználó rendszerén. Ennek eredményeként a támadó ellophatja a felhasználó aktív munkamenet-sütijét.

Példa a webhelyek közötti szkriptelésre:

[ <script> i=new/**/Image();isrc=http://evilwebsite.com/log.php?'+document.cookie+'
'+document.location</script> ]

Míg a hasznos adat általában JavaScript, az XSS támadás bármely kliensoldali nyelv használatával megtörténhet.

Helyek közötti parancsfájl-támadás végrehajtásához a támadó rosszindulatú szkriptet fecskendez be a felhasználó által megadott bemenetbe. A támadók egy kérés módosításával is végrehajthatnak támadást. Ha a webalkalmazás sebezhető az XSS-támadásokkal szemben, a felhasználó által megadott bemenet kódként fut le. Például az alábbi kérésben a szkript megjelenít egy üzenetdobozt az „xss” szöveggel.

[ http://www.site.com/page.php?var=<script>alert('xss');</script> ]

Számos módja van az XSS-támadások kivitelezésére. Például a végrehajtás automatikusan elindulhat, amikor az oldal betöltődik, vagy amikor a felhasználó az oldal bizonyos elemei (például hiperhivatkozások) fölé viszi az egérmutatót.

A webhelyek közötti parancsfájl-támadások lehetséges következményei:

- A felhasználó billentyűleütéseinek rögzítése
- Felhasználó átirányítása rosszindulatú webhelyre
- Böngészőalapú sebezhetőségek futtatása (pl. a böngésző összeomlása)
- A webhelyre bejelentkezett felhasználó sütiinformációinak megszerzése, ezáltal veszélyeztetve az áldozat fiókját

Egyes esetekben az XSS-támadás az áldozat fiókjának teljes kompromittálásához vezet. A támadók rávehetik a felhasználókat, hogy hitelesítő adatokat adjanak meg egy hamis űrlapon, amely minden információt megad a támadónak.

***Webhelyek közötti szkriptelési esetek***

**A tárolt XSS** akkor történik meg, amikor a rosszindulatú hasznos adatot egy adatbázisban tárolják. Ha nincs kimeneti kódolás vagy fertőtlenítés, akkor más felhasználók számára megjeleníti, amikor adatokat kérnek.

**A tükrözött XSS** akkor fordul elő, amikor egy webalkalmazás támadó által biztosított karakterláncokat küld az áldozat böngészőjének, így a böngésző a karakterlánc egy részét kódként hajtja végre. A hasznos teher válaszként visszhangzik, mivel nem rendelkezik szerveroldali kimeneti kódolással.

**DOM-alapú XSS** akkor megy végbe, amikor a támadó parancsfájlt fecskendez a válaszba. A támadó elolvashatja és manipulálhatja a dokumentumobjektum-modell (DOM) adatait rosszindulatú URL létrehozása érdekében. A támadó ezt az URL-t használja arra, hogy rávegye a felhasználót, hogy rákattintson. Ha a felhasználó rákattint a hivatkozásra, a támadó ellophatja a felhasználó aktív munkamenet-információit, billentyűleütéseit stb. A tárolt XSS-től és a tükrözött XSS-től eltérően a teljes DOM-alapú XSS-támadás a kliens böngészőjén történik (azaz semmi sem kerül vissza a szerverre).

- Eavesdropping támadás [77]

Lehallgatási támadás akkor következik be, amikor egy hacker elfogja, törli vagy módosítja a továbbított adatokat, tehát két eszköz közé beékelődik. A lehallgatás, más néven szippantás vagy leskelődés a nem biztonságos hálózati kommunikációra támaszkodik az eszközök közötti adattovábbítás során.

A „lehallgatással megtámadott” eset általában akkor fordul elő, amikor a felhasználó olyan hálózathoz csatlakozik, amelyben a forgalom nem védett vagy titkosított, valamint érzékeny üzleti adatokat küld kollégájának. Az adatok nyílt hálózaton keresztül kerülnek továbbításra, ami így lehetőséget ad a támadónak, hogy kihasználja ezt a biztonsági rést, és különféle módszerekkel elfogja a továbbított adatokat. A lehallgató támadásokat nehéz észre venni. A kibertámadások egyéb formáitól eltérően a programhiba vagy a lehallgató eszköz jelenléte nem befolyásolhatja hátrányosan az eszközök és hálózatok teljesítményét, így a támadó könnyen tud észrevétlen maradni.

### *Lehallgatási módszerek*

A lehallgatással a támadók különféle módszerekkel indíthatnak támadásokat, amelyek jellemzően különféle lehallgató eszközök használatával folynak bele a kommunikációba és ellenőrizhetik a hálózati tevékenységet. Az elektronikus lehallgató készülék klasszikus példája a rejtett poloska, amelyet fizikailag elhelyeznek egy otthonban vagy egy irodában. A poloskát jellemzően egy szék alatt vagy az asztalon helyezik el, vagy a mikrofont egy nem feltűnő tárgyba, például tollba vagy táskába rejtik. Ez egy egyszerű megközelítés, viszont a kivitelezés szempontjából létezik asztali vagy mennyezeti lámpákban, könyvekben a könyvespolcon vagy képkereteken a falon történő elhelyezés. A számos technológiai fejlődés ellenére, amelyek manapság egyre könnyebbé teszik a digitális lehallgatást, sok támadás még mindig a telefonok lehallgatásán alapul. Ennek az az oka, hogy a telefonok rendelkeznek elektromos árammal, beépített mikrofonnal, hangszóróval, fizikai hellyel a lehallgató eszközök elrejtésére, valamint könnyen és gyorsan telepíthetők. A lehallgató támadók figyelemmel kísérhetik a beszélgetéseket abban a helyiségben, amelyben a telefon van, és képesek a világ bármely pontján lévő telefonra irányuló hívásokat is követni. A modern számítógépes telefonrendszer lehetővé teszi a telefonok elektronikus lehallgatását a készülékhez való közvetlen hozzáférés nélkül (mivel az információs csatorna van megfigyelve). A támadók jeleket küldhetnek a telefonvonalon, és továbbíthatnak bármilyen beszélgetést, amely ugyanabban a szobában zajlik, még akkor is, ha a telefonkagyló nem aktív. Hasonlóképpen, a számítógépek olyan kifinomult kommunikációs eszközökkel rendelkeznek, amelyek lehetővé teszik a lehallgató támadók számára, hogy elfogják a kommunikációs tevékenységeket, kezdve a beszédbeszélgetésektől, az online csevegéseken keresztül a billentyűzethibákig, mert az naplózzák a felhasználók által begépelt szöveget. A számítógépek elektromágneses sugárzást bocsátanak ki, amelyet a kifinomult lehallgatók felhasználhatnak a számítógép képernyőjének tartalmának rekonstruálására. Ezeket a jeleket rövidebb távolságokon el is lehet vinni és tovább lehet terjeszteni azokat kábeleken és telefonvonalakon keresztül, amelyek antennaként használhatók.

- Birthday támadás [78]

A módszer kriptográfiai algoritmusok feltörésére szolgál, és az úgynevezett hasító (***hash***) függvényekben található egyezésekre épít. A születésnapi paradoxonon azon alapul, hogy annak a valószínűsége, hogy két ember egy születésnapot oszt meg, jóval nagyobb, mint amilyennek gondolnánk, így például egy 23 fős csoport esetében ennek a valószínűsége 50%. Hasonlóképpen, a vártnál sokkal nagyobb a valószínűsége annak, hogy a cél hashfüggvény esetében ütközés lép fel, így a támadó képes kevesebb iterációval megtalálni a megfelelő töredékeket.

- Malware támadások [79]

A rosszindulatú támadások bármilyen típusú rosszindulatú szoftver, amelyet arra terveztek, hogy kárt okozzon egy számítógépben, kiszolgálóban, kliensben vagy számítógépes hálózatban és/vagy infrastruktúrában a végfelhasználó tudta nélkül. A számítógépes támadók számos különböző okból hoznak létre, használnak és adnak el rosszindulatú programokat, de leggyakrabban személyes, pénzügyi vagy üzleti adatok ellopására használják. Noha motivációik eltérőek, a kibertámadók szinte mindig taktikájukat, technikáikat és eljárásaikat (TTP) arra összpontosítják, hogy kiváltságos hitelesítő adatokhoz és fiókokhoz férjenek hozzá küldetésük végrehajtása érdekében.

A rosszindulatú támadások típusai, melyekben a legtöbb rosszindulatú program a következő kategóriák egyikébe sorolható be:

**Vírus:** Más programok módosításával és saját rosszindulatú kódjának beszúrásával képes lemásolni magát. Ez az egyetlen olyan rosszindulatú program, amely más fájlokat is „megfertőzhet” ezáltal *az egyik legnehezebben eltávolítható* rosszindulatú program.

**Féreg:** A féreg képes önmagát lemásolni a végfelhasználó közreműködése nélkül és gyorsan megfertőzheti a teljes hálózatot azáltal, hogy egyik gépről a másikra költözik.

**Trójai:** A trójai kártevők jogtiszta programnak álcázzák magukat, így *az egyik legnehezebben észlelhető* rosszindulatú program. Az ilyen típusú rosszindulatú programok rosszindulatú kódokat és utasításokat tartalmaznak, amelyek az áldozat által végrehajtott interakció után már a radar alatt működhetnek. Gyakran használják arra, hogy más típusú rosszindulatú programokat engedjenek be a rendszerbe. Ez a hátsó bejárat képzés egyik tipikus eszköze.

**Hibrid rosszindulatú programok:** A modern rosszindulatú programok gyakran rosszindulatú szoftvertípusok „hibridje” vagy kombinációja. Például a „botok” először trójaiként jelennek meg, majd a végrehajtás után féregként működnek. Gyakran használják egyedi felhasználók megcélzására egy nagyobb hálózatot átfogó kibertámadás részeként.

**Reklámprogramok:** A nem kívánt és agresszív reklámozás (***adware***) felugró ablakok (***pop-up***) segítségével jelenít meg hirdetéseket a végfelhasználó számára.

**Malvertising:** A rosszindulatú hirdetések legitim hirdetéseket használnak a rosszindulatú programok végfelhasználói gépekre való eljuttatására.

**Kémprogramok:** A gyanútlan végfelhasználók után kémkedő programok (***spyware***), amelyek hitelesítő adatokat, jelszavakat és böngészési előzményeket gyűjtenek.

**Ransomware:** A zsarolóvírus megfertőzi a gépeket, titkosítja a fájlokat és megőrzi a szükséges visszafejtési kulcsot amíg az áldozat nem fizeti meg a váltságdíjat. A vállalatokat és kormányzati szerveket célzó zsarolóvírustámadások egyre szaporodnak és milliókba kerülnek a szervezeteknek, mivel egyesek fizetnek a támadóknak a létfontosságú rendszerek helyreállításáért. A Cyptolocker, a Petya és a Loky a zsarolóvírusprogramok leggyakoribb és leghírhedtebb családjai közé tartoznak.

***Ismert példák rosszindulatú támadásokra***

**Pony malware:** a leggyakrabban használt rosszindulatú program jelszavak és hitelesítő adatok ellopására. Helyenként *„Pony Stealer”*, *„Pony Loader”* vagy *„FareIT”* néven is említésre kerül. A Pony kártevő Windows operációs rendszert futtatógépeket céloz meg és információkat gyűjt a rendszerről és a rendszerhez csatlakozó felhasználókról. Használható más rosszindulatú programok letöltésére vagy hitelesítő adatok ellopására és elküldésére a parancs- és vezérlőkiszolgálóra.

**Loki vagy *„Loki-Bot”*:** egy információtolvaj program, amely körülbelül 80 program hitelesítő adatait és jelszavait célozza meg, beleértve az összes ismert böngészőt, e-mail klienst, távvezérlő programot és fájlmegosztó programot. A számítógépes támadók 2016 óta használják, és továbbra is népszerű módszer a hitelesítő adatok ellopására és a személyes adatokhoz való hozzáférésre.

**Krypton Stealer:** először 2019 elején jelent meg és külföldi fórumokon kártevő szoftver, mint szolgáltatás (MaaS, ***malware-as-a-service***) néven árulják, mindössze 100 dollárért

kriptovalutákban. A 7-es és újabb verziót futtató Windows gépeket célozza meg, és rendszergazdai engedélyek nélkül lopja el a hitelesítő adatokat. A kártevő a hitelkártyaszámokat és a böngészőkben tárolt egyéb érzékeny adatokat is megcélozza, például a böngészési előzményeket, az automatikus kiegészítést, a letöltési listákat, a sütiket és a keresési előzményeket.

**Triton kártevők:** 2017-ben a Közel-Keleten bénítottak meg kritikus infrastruktúra-létesítmény működést az egyik első ilyen típusú támadás során. A rosszindulatú program az általa megcélzott rendszerről kapta a nevét – a Triconex Safety Instrumented System (SIS) vezérlőkről. Ezeket a rendszereket a nukleáris létesítmények, olaj- és gázüzemek működésének leállítására használják probléma, például berendezés meghibásodás, robbanás vagy tűz esetén. A Triton kártevőt úgy tervezték, hogy letiltja ezeket a hibabiztos mechanizmusokat, amelyek a kritikus infrastruktúra elleni fizikai támadásokhoz és potenciális emberi károkhoz vezethetnek.

***Részkövetkeztetés***

A fejezetben bemutatásra kerültek a téma megértését elősegítendő relevánsabb fogalmak, szabályozási elvek, illetve olyan történeti események, amelyek megadják azt a ***keretrendszert,*** amiben értelmezhetővé válik az a környezet, ahol a pszichológiai manipuláció működését vizsgálom. Látható, hogy a manipuláció alkalmazása több ezer éves múltra tekint vissza, valamint katonai alkalmazása sem újkeletű. Érdemes szem előtt tartani, hogy a történelem során a technológia fejlődésével mindig újabb és újabb eszközökkel kerül kivitelezésre, amikkel az emberi tevékenység kifinomultabb stratégiák mentén haladt előre. Ilyen volt a 20. században a távközlési technológia fejlődése, ami megalapozta a kódolt üzenetek (kriptográfia) alapjait, a kommunikációban szükséges, de nem elégséges feltétel kizárólag a technikai adottságok megteremtése, a hatékony terv szerinti működéshez szükség van további finomításokra, ilyen tényező a titkosítás, amire jó például szolgál a második világháború során az Enigma feltörésével bekövetkezett fordulat a háború lezárását illetően.

# 2 A KÖZÖSSÉGI MÉDIA SZEREPE ÉS HATÁSA A TÁRSADALMI FOLYAMATOKRA

*„Színház az egész világ, És színész benne minden férfi és nő:”*
Shakespeare

### *Bevezetés*

A közösségi média 2010 után szerte a világban megnövekedett befolyást szerzett, a történelem alakulásában pedig fontos szerepet tölt be. Értelmezhető egyrészről úgy is, hogy azok a vállalatok, amelyek ezeket az alkalmazásokat/platformokat működtetik, olyan termékeket üzemeltetnek, amelyek megfeleltethetők egy-egy globális médiumnak. Ilyenre korábban brit és amerikai nyomtatott sajtó és televíziós óriások esetében volt példa, mint a Washington Post, New York Times, Guardian, BBC stb., melyek elérései messze túlnyúltak saját országhatáraikon, azonban közel sem öltöttek olyan méreteket, mint amilyet a technológiai óriások értek el az elmúlt években.

**Közösségi média:** A Britannica szótár szerint a közösségi média az elektronikus kommunikáció formái (például webhelyek), amelyeken keresztül az emberek online közösségeket hoznak létre információk, ötletek, személyes üzenetek stb. megosztására. [80] A Cambridge szótár szerint a közösségi média olyan médiaforma, amely lehetővé teszi az emberek számára, hogy az interneten vagy mobiltelefonon keresztül kommunikáljanak és megosszák az információkat. [81]

### *Üzleti és politikai érdekek*

Kezdetben a közösségi oldalak csupán az ún. magánjellegű információcsere platformjai voltak, ezeken a tevékenységek a közösségi eseményeken készült fotók/videók megosztása, kapcsolatkeresés és az elérhetőségek megadásában merültek ki. Később pedig fokozatosan beszivárogtak a céges és politikai hirdetések, valamint már kampányesemények is követhetővé váltak egészen terrorszervezetek pénzgyűjtési szerveződéséig bezárólag. [82] A chatfelületek a közösségi média hajnalán nagy népszerűségnek örvendtek, valamint a web2 szabványra való átállás és a blogok népszerűségének növekedése is elősegítette az új platformok létrejöttét. Az online környezetben a hazugság nem egyedülálló, hiszen az internet az információs hadviselés csataterévé vált. Sok szereplő van rajta, és teljesen mindegy, hogy állami szintű

szereplőről (***state-level actor***), vagy csupán egy magánszemélyről van szó, hírek böngészése közben pár perc leforgása alatt találkozhatunk egy fabrikált történettel. Először is, ez magának az internet változásának köszönhető. Kezdetben létezett egy Web 1.0 nevű szabvány, ahol a weblapokat és a webes tartalmakat viszonylag kevés ember készítette. Az információáramlás statikus volt. Miközben ez a tevékenység tovább nőtt, a web is átalakult. A Web 2.0 vagy gyakran „közösségi internet”-nek hívják az interakciók új formáját. Ez a struktúra arra ösztönözte a felhasználókat (1. táblázat), hogy tartalmat hozzanak létre, véleményt alkossanak, és reagáljanak a tartalomra az interneten. Ez végül megnyitotta az utat a közösségi média létrehozása előtt is. Amikor ezek az új kommunikációs platformok megjelentek, a „fair használat” mellett rosszindulatú szereplők is megjelentek a pályán. Ezek a csatornák ugyanannyi kárt okozhatnak, mint hasznot a társadalmaknak. A félrevezetés és a hamis információk gomba módjára terjedhetnek az emberek alapvető kíváncsisága miatt. Annak érdekében, hogy ellenállóak legyünk a manipulációkkal szemben ezeken a platformokon, bizonyos lépéseket tehetünk. Először is fel kell tennünk magunknak a kérdést, hogy valójában milyen információkra vagyunk kíváncsiak, ha keresünk. A dezinformáció például alapértelmezés szerint az érzelmi visszacsatoláson alapul, tehát ha olyan címsort olvasunk, amely érzelmileg a szokásosnál jobban (vagy akár nagyságrenddel) magasabb szinten aggaszt bennünket, gyaníthatjuk, hogy az általunk megtekintett vagy olvasott tartalom egy nagyobb koncepció, más szóval narratíva része. Egy ismeretlen helyzetre a szokásos emberi reakció az, hogy félelemmel reagálunk. Ez kényelmetlenné helyzetbe szorít bennünket, mert a jövő ilyenkor ködbe burkolt. Ezeken az oldalakon vannak bizonyos beállítások, ahol személyre szabhatjuk hírfolyamunkat, amivel szabályozhatjuk, hogy milyen tartalom jelenjen meg, amit naponta böngészünk. A tudatosság kulcsfontosságú a rugalmasság kialakításában. Ez lehetővé teszi számunkra, hogy kívánatos módon reagáljunk a bizonytalanságokra és kihívásokra, mert érezni fogjuk magunkban, hogy mi irányítunk. Leggyakrabban a manipulátor megpróbál minket érzelmi hullámvasútra ültetni, ahol a döntéshozatali folyamat nehezen gyakorolható. Ha azonban a környezet nyugodt, és rendelkezésre állnak az értékeléshez szükséges információk, sokkal nagyobb a valószínűsége annak, hogy a megtévesztő taktika sikertelen lesz. [34]

### *A web2 szabvány*

A Web 2.0 leírja az internet jelenlegi, széles körben alkalmazott állapotát, amely korábbi változatához, a Web 1.0-hoz képest több felhasználó által generált tartalommal és a végfelhasználók általi használhatósággal rendelkezik. A Web 2.0 általában a 21. századi internetes alkalmazásokra utal, amelyek a „dotcom" buborékot követően átalakították a digitális korszakot, ami 1995 és 2000 között nagy mértékben befolyásolta a tőzsdei folyamatokat. [83] A Web 2.0 kifejezést először 1999-ben használták, amikor az internet egy olyan rendszer felé fordult, amely aktívan bevonja a felhasználót a működési folyamatba. A felhasználókat arra ösztönözték, hogy ahelyett, hogy csak nézték volna a weboldalakat, formáljanak véleményt, generáljanak tartalmakat. Az internet társadalmi aspektusa ezt követően különösen átalakult, általánosságban elmondható, hogy a közösségi média lehetővé teszi a felhasználók számára, hogy gondolataikat, nézőpontjaikat és véleményeiket megosszák és interakcióba lépjenek egymással. A felhasználók így címkézhetnek, megoszthatnak, közzétehetnek és kedvelhetnek tartalmakat. [84] Ez a fajta interaktív kommunikáció lehetőséget teremtett arra, hogy ami a korábbiakban nem volt látható egyes közösségek interakciói között, az mostanra hálózati szintű kiterjedésben, multimédiás eszközökkel megtámogatott formában működik és zajlik a mindennapokban.

*1. táblázat A web2 és a web1 szabványok összehasonlítása*

| **Web 2.0** | **Web 1.0** |
|---|---|
| Dinamikus információ (mindig változik) | Statikus információ (nehezebb változó) |
| Kevesebb kontroll a felhasználói bevitel felett | Ellenőrzöttebb felhasználói bevitel |
| Elősegíti a nagyobb kollaborációt, mivel a csatornák dinamikusabbak és rugalmasabbak | Az egyéni hozzájárulás kiemelt szereppel bírt; csatornák kevésbé voltak dinamikusak |
| Sokkal közösségibbnek és interaktívabbnak tekinthető | Sokkal informatívabb és adatközpontúbb működés jellemezte |

A jövőt illetően az irány a decentralizált működés és a blokklánc (blockchain) technológia alkalmazása felé halad. A különbség a ma alkalmazott szabványhoz képest az, hogy a felhasználók közösségi szinten irányítanák a platformokat, amiken keresztül kommunikálnak, ezáltal megszűnne a közvetítő szerepe. [85]

## 2.1 A tömegtájékoztatás korszakai

A tömegtájékoztatás rögzített formáinak változását tekintve az alábbi korszakokat különböztethetjük meg:

1. Nyomtatott sajtó
2. Rádió
3. Televízió
4. Hírportálok, blogok
5. Közösségi média

A felsorolt elemek közös jellemzője, hogy itt rögzített tartalmakról van szó, amelyek visszakereshetők, megismételhetők. A tömegkommunikáció kezdetleges formáihoz képest, mint a szónoklat vagy az ünnepi beszéd, az ellenőrizhetőség kulcsfontosságú különbség, legalábbis annak fényében, hogy az adott időpontban amikor az üzenet közvetítése zajlott és hogy éppen mi hangzott el.

**Véleményvezér (influencer):** Jellemzően a közösségi médiában olyan szereplő, aki a generált tartalma által széles tömegek elérésére képes, valamint szűk területén meghatározó világnézettel rendelkezik. Ebből kifolyólag tevékenységét az átlagosnál magasabb figyelem övezi, mely lehetőséget teremt arra, hogy üzleti érdekeltséget is végezzen fizetett hirdetések formájában.

***A tömegsajtó története***

A ***„penny press”*** kifejezést használták az egy centért eladott újságok előállításának forradalmi üzleti taktikájának leírására. 1833-ban jelent meg, amikor Benjamin Day megalapította a The Sun című New York-i újságot, ami a mai bulvárlapok előfutárjának számított. [86] Lapjai a szokásos hirdetési lapoknál kisebbek (kb. A/4) voltak, mindennapi témákat és rendőrségi híreket közöltek. Az ekkoriban 220 ezer fő lakosságú New Yorkban a legnépszerűbb lap a 4500 példányban megjelenő Courier and Enquirer volt. A Times ezzel szemben a 2 millió fő lakosú Londonban 10 ezer példányban fogyott. Az olcsó Sun példányszáma 2 év alatt 15 ezer darabra nőtt, ami a maximum volt, amit a nyomdagépek kapacitása megengedett. 1836-ban az olcsó lapok megérkeztek Franciaországba, ahol Emile de Girandin elindította La Presse című újságát. [87] A **tömeges pszichológiai manipuláció** (mass social engineering) a tömegek megnyerésére

irányul. Az az elképzelés, miszerint a kommunikációs, és a médiatechnológiák kulcsfontosságúak az Egyesült Államok kormányzási rendszerének kialakításában és fenntartásában, már az ország megalapításával kezdődött, az alapítók között konszenzus alakult ki abban, hogy különösen az újságok kiemelt szerepet játszottak a szétszórt tömegek tájékozott közvéleménnyé formálása során, ami elősegítette a közös megértés- és véleménytudat kialakítását. [88, pp. 37-41.] [89] [90] Napjainkban ugyanez a tendencia irányadó a világ számos országában, az Egyesült Államok vonatkozásában pedig a nagyméretű technológiai vállalatok révén továbbra is az élvonalban tölt be szerepet.

### *A rádiózás felfedezésének kalandos útja*

Jelentős előre lepésnek számítottak Henrik Hertz által felfedezett elektromágneses hullámok 1888-ban. Elektromos árammal alacsony frekvenciás elektromágneses hullámokat gerjesztett és azokat detektálta. Így lehetővé tette az elektromos hullámokkal működő távírót és felvázolta az utat Guglielmo Marconi találmányának, a drótnélküli távíró számára. Kevésbé ismert viszont, hogy Nikola Tesla szerb fizikusnak is úttörő szerepe volt a rádiózásban, méghozzá peres úton. 1901-ben Marconi sikeresen mutatta be a rádióhullámok vezeték nélküli sugárzását. A rádió feltalálásáért 1909-ben fizikai Nobel-díjat kapott. Tesla beperelte, azzal a váddal, miszerint Marconi ellopta a találmányát. A tárgyalások többször megszakadtak és elhúzódtak, végül 1943-ban, Tesla halála után az Amerikai Egyesült Államok Legfelsőbb Bírósága hivatalosan is Teslának tulajdonította a rádió feltalálását. Marconi, Tesla asszisztense volt Amerikában, ahol láthatta kutatásait és annak eredményeit. A jelentés alapján Tesla szabadalmát már 1896-ban, négy évvel korábban bemutatta. Ezért Marconitól megvonták a rádió feltalálásának elsőségét. [91] Oroszországban viszont, ha megkérdezünk bárkit, hogy ki találta fel a rádiót, azt fogják mondani, hogy Alekszandr Sztyepanovics Popov. 1895. május 7-én (Lodge után, de Tesla és Marconi előtt) Popov bemutatott egy rádióvevőt az Orosz Fizikai és Kémiai Társaságnak Szentpéterváron, és még abban az évben publikált egy tanulmányt a készülékéről. Állítólag Popov 1896 márciusában továbbította a "Heinrich Hertz" vezeték nélküli üzenetet a szentpétervári kampusz két épülete között Ez az állítás viszont sajnos nem ellenőrizhető, mivel a kísérletet az orosz haditengerészet rendelte meg, és évekig titokban tartották. 1945. május 7-én, Popov első demonstrációjának 50. évfordulóján, az orosz törvényhozás „rádiónapnak” nevezett ünnepnapot hozott létre, amelyet Oroszországban ma is minden május 7-én ünnepelnek. [92]

### *A képes műsorszórás, a televízió*

Kezdetben a rádiózás eszközeinek ötvözésével zajlottak az első adások, valamint előre felvett filmszalagot levetítésével. 1936-ban. a berlini olimpián készül el az első "filmklip" és ekkor kerül sugárzásra az első európai tévéadás. [93]

Néhány jelentősebb mérföldkő az Egyesült Államok televíziózásában [94]

- 1969: A Holdra szállás közvetítése élőben
- 1972: Megjelenik az első fizetős kábeltévé szolgáltatás az HBO (Home Box Office) Wilkes-Barre-ban, Pennsylvaniában.
- 1980: A CNN amerikai hírcsatorna indulása. Az első adását 2 millió kábeltévé néző követhette
- 1987: Az Egyesült Államokban a háztatások felében kábeltévé szolgáltatás elérhető
- 1991: A CNN élőben közvetíti az Öböl-háború eseményeit

1991. január 17-én, a légitámadások kezdetekor az iraki Információs Minisztérium munkatársai elvágták a külföldi tudósítók telefonvonalait és előbb a bagdadi Al-Rashid hotel óvóhelyére telepítették őket, majd másnap kiutasították őket az országból. Ekkor összesen 45 tudósítója volt az ABC, a CBS, az NBC csatornáknak, valamint a fő amerikai és európai újságoknak és hírügynökségeknek a helyszínen, hogy a harctéri eseményekről tudósítsanak. Egyetlen társaság kapott tartózkodási engedélyt, a Ted Turner által 1980-ban alapított, akkor még rövidéletű CNN volt, ami annak köszönhette maradását, hogy két héttel a harcok megkezdése előtt az irakiakkal titkos megállapodást kötött. [95] A 2001. szeptember 11-i terrortámadás lehetett az első globális esemény, amelyet valós időben emberek százmilliói éltek meg szerte a világon. Az első felvételek szinte azonnal megjelentek a WNYW-TV Fox 5.ös csatornán, a Good Day New York című reggeli műsorában. A CNN élő közvetítéssel jelentkezett az ikertornyokról 8:49-kor, alig három perccel az első gép becsapódása után. [96]

A rádiózás korszakában kevésbé, viszont a televíziózás esetében a képernyőkön gyakran megjelenő szereplők komoly befolyással bírtak a társadalmi véleményformálás során, ez pedig a későbbiekben is megmaradt az online szférában. Ezeket a szereplőket manapság véleményvezéreknek nevezik, akik a tartalomgyártás során aktív szerepet játszanak a közönség megszólításában és a társadalmi diskurzus alakításában egyaránt.

## 2.2 A blogok és a közösségi média történeti áttekintése

**Blog:** olyan weboldal, amelyen egy személy vagy csoport rendszeresen, gyakran minden nap új információkat tesz fel; weblog: [97]

### *Blogok az Egyesült Államokban és itthon*

A közösségi internetet a kezdetekben a blogok feltörekvő népszerűsége adta, hiszen újdonságnak számítottak az olyan írott tartalmak, amelyek nem a hagyományos hírszerkesztési elvek mentén kerültek publikálásra, valamint nem igényeltek intézményes kereteket. Az első blog megjelenése Jorn Bargerhez kötődik. [98] Az egész folyamat, amikor érdekes dolgokat gyűjtünk a világ minden tájáról és írunk róluk az interneten, új ötletnek számított, ezért új névre volt szükség. Jorn úgy döntött, hogy „logging the web"-nek nevezi, ami így a Robot Wisdom-ot tette az első webbloggá. Így lett belőle Robot Wisdom Weblog ezzel 1997. december 17-én megszületett a blogoszféra. [99] A blog (a „weblog" rövidített változata) egy online folyóirat vagy információs webhely, amely az információkat fordított időrendi sorrendben jeleníti meg, és a legfrissebb bejegyzések jelennek meg először, felül. Ez egy olyan platform, ahol egy író vagy írók csoportja megosztja véleményét egy adott témáról. [100] 2003. május 27-én Matt Mullenweg bejelentette a WordPress első verziójának elérhetőségét. [101] A közösség jól fogadta. Alapja a b2 Cafelog jelentős fejlesztésekkel. A WordPress első verziója új adminisztrátori felületet, új sablonokat és generált XHTML 1.1-kompatibilis sablonokat tartalmazott. [102] Hazai berkekben a weblapépítés és a blogok készítése a „G-Portál"-hoz és a „Blog.hu"-hoz kötődött. A G-Portál az Ivy Magyarország Kft.-vel és a Virtual Playground Kft.-vel kötött megállapodásoknak köszönhetően a tinédzser korosztály számára létrehozott portál a www.g-portal.hu címen volt elérhető, amely három nagyobb szolgáltatásból tevődött össze. A G-Portál eredeti funkciója az online weblapépítést jelentette, s ma már több mint 424 ezer regisztrált felhasználó több mint 63 ezer portálját szolgálta ki. [103]

### *Fórumok és moderátorok*

A webes kommunikáció egy másik formája a felhasználók közötti folyó csevegés szöveges formában. A műfaj jellemzője, hogy egy adott téma/kérdéskör területén időrendileg jellemzően visszafelé haladva váltanak üzeneteket egymással a hozzászólók. Hazánkban ennek legnépszerűbb terepe az 1997-ben alapult „Index fórum" volt, ami napjainkig is működik, valamint a fiatalabb korosztályok körében népszerűbb

„gyakorikérdések.hu” pedig 2006. október 21.-én nyílt meg a felhasználók számára. A regisztrált felhasználóknak lehetőségük van kérdéseket feltenni, amelyek felhasználónévvel vagy anonim módon kerülnek közzétételre, amelyet a regisztráció nélkül böngésző felhasználók is olvashatnak.

**Moderátor:** Egy olyan személy, aki gondoskodik arról, hogy az internetes beszélgetés szabályait ne sértsék meg, például eltávolít minden fenyegető vagy sértő üzenetet [104]

A moderáció, az információfolyam irányítása egy meglehetősen kényes téma, különösen olyan országokban, ahol a szólás- és véleményszabadság alkotmányos alapjog. Kezdetben a felhasználók alacsony számának köszönhetően nem váltott ki nagy elégedetlenséget, ha egy-egy üzenet akár súlyosabb ok nélkül eltávolításra került.

***SixDegrees.com és a MySpace.com***

Az internet növekedése lehetővé tette olyan online kommunikációs szolgáltatások bevezetését, mint a CompuServe, az America Online és a Prodigy. Bevezették a felhasználókat a digitális kommunikációba e-mailen, faliújságon és valós idejű online csevegésen keresztül. Ez hozta létre a legkorábbi közösségi média hálózatokat, kezdve a rövid életű Six Degrees profilfeltöltő szolgáltatással 1997-ben. Ezt a szolgáltatást 2001-ben követte a Friendster. Ezek a kezdetleges platformok több millió felhasználót vonzottak, és lehetővé tették az e-mail címek regisztrációját és az alapvető online hálózatépítést. A webnaplók vagy blogok, a digitális közösségi kommunikáció másik korai formája, a LiveJournal oldal 1999-es elindításával kezdtek népszerűvé válni. Ez egybeesett azzal, hogy a Pyra Labs technológiai vállalat elindította a Blogger közösségi platformját, amelyet a Google 2003-ban vásárolt meg. A LinkedIn-t 2002-ben alapították, a karrierorientált szakemberek közösségi hálózatát. 2020-ra világszerte több mint 675 millió felhasználóra nőtt (Ez nem azonos az aktív felhasználók számával). Továbbra is a közösségi média oldala marad az álláskeresőknek, valamint a képzett jelölteket kereső humánerőforrás-menedzsereknek. Két másik nagy oldal a közösségi médiában összeomlott a kezdeti siker kirobbanása után. 2003-ban elindult a Myspace, ami 2006-ra a leglátogatottabb webhely volt a bolygón, amelynek központi elemét az képezte, hogy a felhasználók közvetlenül a profiloldalukon oszthattak meg új zenéket. [105]

### *A közösségi média elterjedése Magyarországon*

Magyarországon a közösségi média elterjedése a széleskörben meglévő internetelérással egyidős, ami a 2010 utáni néhány évben zajlott le. Az infrastrukturális fejlesztések lehetővé tették az internetelérés kiszélesedését, ezáltal a közösségi média felületeinek elérésének növekedését is. Kezdetben az EU átlag (60%) alatt volt nem sokkal az internetelérés (58%), valamint ezek is főképp a fővárosra, Budapestre és a nagyvárosokra koncentrálódtak, kívül hagyva a vidék jelentős részét. A megoszlás a használatban jellemzően a felsőfokú végzettséggel rendelkezők és a szolgáltatási szektorban dolgozók körében volt magasabb. Nemek szerinti megoszlásban a különbség szintén tapasztalható volt a nők alacsonyabb foglalkoztatása[2] révén. A 15 és 24 év közötti fiatalok vezették a digitális átalakulás folyamatát hazánkban, amelyeket kormányzati törekvések is támogattak, mint például az informatikai beszerzések, amelyek az oktatás fejlesztését szolgálták. A közösségi kapcsolatépítés népszerűsödése elsősorban a hazai közösségi felületeknek[3] volt köszönhető, de a Facebook globális terjeszkedésében való hazai részvétellel is. 2011-ben a közösségi kapcsolattartásban a legnépszerűbb közösségi média tevékenységek a blogok használata volt, amely a teljes internetfelhasználói bázis 52%-át jelentette. Több közösségi oldal volt elérhető Magyarországon, ezek közül a legnépszerűbb a magyar tulajdonú IWIW.hu volt, amelynek 4,2 millió tagot számlált, többségük 15 és 29 év közötti volt. A MyVIP.com és a Baratikor.com szintén népszerű volt a maga 2,6 és 2,5 millió tagjával. Mindhárom magyar nyelvű helyi hálózatot takart, amelyet főleg tinédzserek és fiatal felnőttek használtak kapcsolattartásra, barátságok szerzésére, fotók és videók megosztására. További kisebb hálózatok a Hi5.com, a Hotdog.hu, a video.hu és az inda.hu. voltak. [106] Ebben az időszakban az MSN Messenger (későbbiekben: Windows Live Messenger) és a Skype dominálta a társas kommunikációt a magánéleti szférában, mely utóbbit 2012-ben úgyszintén a Microsoft vásárolta fel [107] 2010 után a közösségi platformok egyre nagyobb népszerűségnek örvendtek, ami az aktív felhasználók számának ugrásszerű növekedését eredményezte.

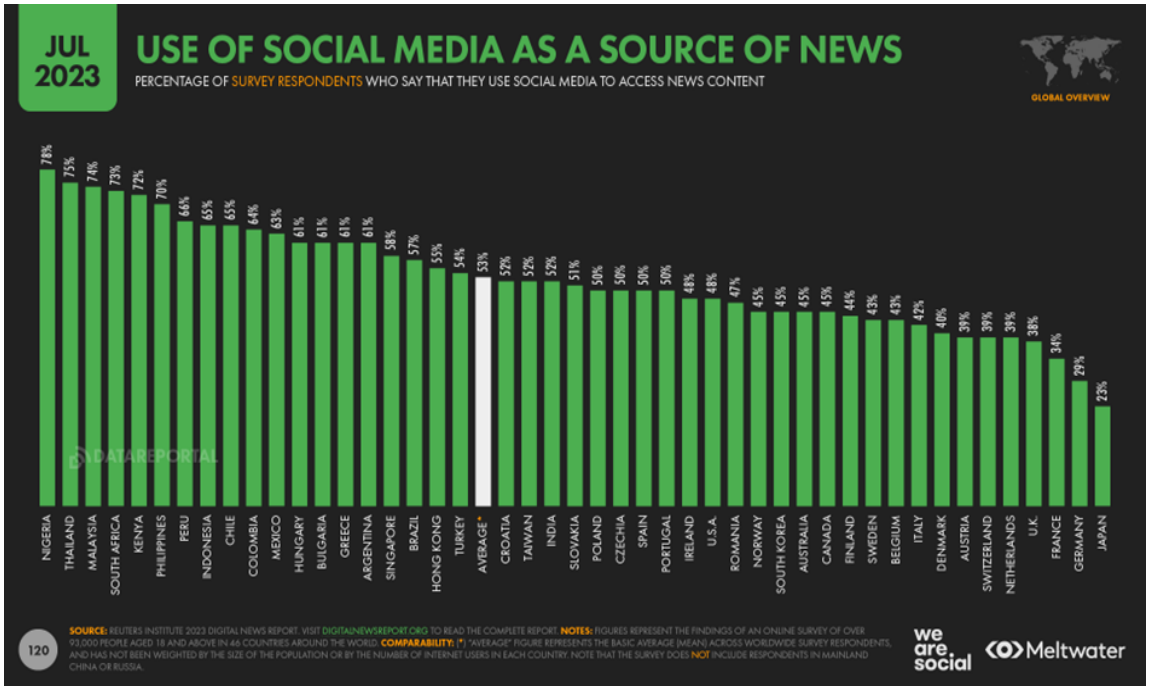
[2] Itt célszerűnek tartom megjegyezni, hogy ez az alacsonyabb foglalkoztatás a magyar állami transzferprogramok rendszerének is betudható, például: GYES,GYED alatti távolmaradás a munkahelytől
[3] Elsősorban az iWIW és myVIP

***Közösségi hálózatok: egy új korszak az információterjesztésben***

A Facebook még 2006-ban kezdett hirdetni a platformján, a Twitter 2010-ben engedélyezte a reklámozást. A LinkedIn, az Instagram, a Pinterest, a Snapchat és a TikTok a szponzorált hirdetések különféle formáival próbálták bevételt szerezni szolgáltatásaikkal. Amikor 2007-ben megérkezett az Apple első érintőképernyős telefonja, az ikonikus iPhone, a játék megváltozott, mert a hangsúlyt az online közösségépítésről a mobilalkalmazások területére helyezte. Ettől a pillanattól kezdve minden megváltozott. A technológiai fejlődés, például a telefonokba épített kiváló minőségű kamerák megváltoztatták a mobilalkalmazások irányát a videók és képek felé. Az írott üzenetek mellett a felhasználók valós időben is sugározhatnak. Az Instagram az utazás, a szórakozás, a divat és más vizuálisan orientált témák iránt érdeklődő közösségi média felhasználók által választott alkalmazás lett.

A Facebook, a Twitter, a Snapchat, az Instagram, a TikTok és más közösségi hálózatok felvirágoztak a mobilalkalmazások piacán, és a mai napig virágoznak. Ahogy a közösségi média felhasználói bázisa elérte a százmilliókat, elkezdtek formálódni a Facebook, Twitter és más közösségi platformok üzleti alkalmazásai. A közösségi média cégek a valaha létezett legszélesebb körű felhasználókövetési adatokhoz férnek hozzá. [108] „A felhasználók nem csak bejelentkeznek és weboldalakat böngésznek, hanem elmondják a platformoknak a nevüket, hol laknak, mit szeretnek és kit ismernek. a jelenleg lehetséges legélénkebb képet festeni azon marketingesek számára, akik konkrét fogyasztókat szeretnének megcélozni.” [109] A napi hírfogyasztási szokások az első okostelefon megjelenését követő első évtized után drasztikusan megváltoztak. Ennek az eszköznek köszönhetően olyan ipari ágazatok születtek, amelyek korábban nem léteztek, nevezetesen a mobilalkalmazások iparágát az okostelefonok alapozták meg. Az alkalmazások rövid időn belül olyan népszerűvé váltak, hogy hatásukra megváltozott a marketingstratégiák jellege és az információterjesztés módja. Ezzel az új lehetőséggel az üzleti és politikai szereplők is gyorsan megjelentek ebben a médiatérben, ahol megkezdték tevékenységük bővítését. Ezek a technológiák alapjaiban változtatták meg a mindennapi rutint, bevett napi cselekménnyé vált a ***görgetés*** (scrolling) jelensége, ami azt jelenti, hogy a felhasználó minden további utasítás nélkül, lényegében akadálytalanul folyamatosan böngészi a közösségi oldalakon fellelhető tartalmakat. További fontos tényező, hogy ezek az alkalmazások valós időben (rendelkezésre álló internetkapcsolat mellett) képesek kommunikálni a felhasználókkal úgynevezett ***push üzeneteken*** (push

messages) keresztül, amelyek értesítéseket küldenek a felhasználónak. Ezeket a telefonokba épített apró LED-lámpák és ***értesítési hangok*** (notification sounds) segítségével teszik, amelyek arra ösztönzik a felhasználót, hogy kapcsolatba lépjen az eszközzel. A cselekvés ösztönzésére kitalált ***mesterséges impulzusok*** (artificial impulses) a közösségi média alkalmazások olyan egyedi jellemzői, amelyekre a korábbi tömegkommunikációs eszközök nem voltak képesek. Ezeknek köszönhetően a szokások sok esetben **függőségek** (addictions) is, hiszen neurobiológiai alapokra épültek, és dopaminforrásként is szolgálnak. Ebből következik, hogy az érzelmi reakciókra gyakorolt manipulatív nyomás elsődleges fontosságú ezen alkalmazások használatában, valamint közvetett hatásuk vizsgálatában, mint például a **különböző narratívákra adott reakciók**. Ezek az érzelmi nehézségek félelmet ébreszthetnek a társadalomban pusztán azért, mert hogyan mutatták meg és hogyan érte el a célközönséget.




*1. ábra A közösségi média, mint hírforrás használata*

*Forrás: datareportal.com*

Elmondható, hogy a közösségi média, mint a hírfogyasztás viszonyítási pontja (1. ábra) ma már jelentős jelenléttel rendelkezik, ami meghatározó felelősséggel párosul. Az alkalmazásokat üzemeltető cégeknek és származási országuk jogalkotási mechanizmusainak kéz a kézben kell járniuk. Ami már a 230. §-nál is hangsúlyos érv volt, ezek a felületek korunk egyik társadalmi terét jelentik, amelyek a történelem korábbi időszakaiban az úgynevezett offline térben helyezkedtek el, ma már az információs ill. a

kibertér és a megfelelő szabályozási keretek [110] kialakítása még várat magára, szükségük van rájuk. Sajnos ezek az interfészek az elmúlt években nemcsak a hagyományos kapcsolatfelvételi lehetőségeket támogatták, hanem szélsőséges szervezetek és terrorista csoportok toborzóplatformjaiként is szerepet játszottak. [34] Ezeknek a platformoknak a szabályozása folyamatban van olyan területeken, mint a gyermekbántalmazás és a szexuális kizsákmányolás. [111] A döntéshozók megkérdőjelezték a közösségi média cégek azon képességét, hogy megfelelően szabályozzák platformjuk tartalmát. A szenátusi meghallgatásokon a Meta, a Snap, a TikTok, a Discord és az X (korábban Twitter) vezérigazgatói voltak jelen.

***A közösségi média, mint új támadási vektor***

A digitális világ fegyveressé tételének talán legfigyelemreméltóbb példája az Oroszország által az Egyesült Államok ellen indított közösségi média háború. Ez az Egyesült Államok elleni sokrétű digitális támadás a 2016-os amerikai elnökválasztás befolyásolását támogató célzott félretájékoztatási és dezinformációs kampányokat jelentette. Az Egyesült Államok Védelmi Minisztériumában dolgozó több mint 10 000 Twitter-felhasználónak kiküldött gondosan megtervezett üzenet rosszindulatú kódokat tartalmazó támadásokat szolgáltak. Egy Ukrajnában tartózkodó orosz katona sikeresen beszivárgott egy amerikai közösségi média csoportba azzal, hogy 42 éves amerikai háziasszonynak adta ki magát, és testre szabott üzenetekkel vett részt politikai vitákban. [112] A társadalom manapság arra van kondicionálva, hogy elsősorban a digitális világban tevékenykedjen – dolgozzon, kommunikáljon, iskolai tanulmányokat folytasson, alakítson ki kapcsolatokat, melyet javarészt a közösségi médián keresztül tesz. A közösségi média platformok létrejöttének céljai között szerepelt, hogy segítsék az információmegosztást, elősegítsék a kapcsolatteremtést és a kreativitást a felhasználók között, valamint lehetővé tegyék a felhasználók által generált tartalmak (UGC) létrehozását és népszerűsítését. Sokan azt feltételezik, hogy ezek a platformok biztonságos tereket jelentenek a kommunikációhoz és az információk megosztásához. Sajnos a különböző kifinomultságú rossz szereplők továbbra is fegyveres területté teszik a közösségi médiát, súlyos károkat okozva nemcsak az egyéneknek és szervezeteknek, hanem a kritikus infrastruktúráknak is.

***Digitális kukabúvárkodás***

A közösségi média megszületése előtt az ellenfelek aprólékosan gyűjtötték az emberi tevékenységből származó intelligenciát (HUMINT) utazások, cikkek, nyilvános események és a klasszikus földi megfigyelések révén. A digitális korszakban a közösségi média vált a HUMINT elsődleges felderítő eszközévé, egyfajta digitális szeméttelepp é, ahol az ügyes guberálók értékes információkhoz juthatnak. A felhasználók a közösségi médiában sokféle témájú tartalomban osztják meg személyes és szakmai életük ilyen például az iskolai végzettségük, politikai nézeteik, lakóhelyük, érdeklődési körük és egyéb területek intim részleteit teszik közzé, amelyekből alaposan fel tud készülni a hírszerzési tevékenységet folytató szereplő.

A Tessian Csoport ***'How to hack a human'*** tanulmánya [113, p. 8] szerint a válaszadók:

- 59%-a tesz közzé fényképeket/neveket gyerekekről.
- 38%-a posztol a születésnapi ünneplésről.
- 30%-a tesz közzé nevet/fotót háziállatokról.
- 27%-a tesz közzé partnere nevét/fényképét
- 36%-a tesz közzé információkat cégéről, munkahelyéről, kollégáiról, főnökéről stb.
- 32%-a tesz közzé frissítéseket és fényképeket üzleti utak során.
- 26%-a tesz közzé információkat az ügyfelekről.

Ezeket az információkat gyakran nem korlátozzák az adatvédelmi beállítások, és olykor nyilvánosan is elérhetők. Valójában az emberek körülbelül 55%-a esetében egyáltalán nincs aktiválva semmilyen adatvédelmi beállítás a tanulmány szerint. Az FBI továbbra is kongatja a vészharangot, és figyelmezteti azokat, akik biztonsági engedéllyel rendelkeznek (vagy rendelkeztek) az Egyesült Államokat és annak érdekeit célzó külföldi hírszerző szolgálatokkal kapcsolatban, erőteljes közösségimédia-felderítési erőfeszítésekkel, amelyek végső soron a SE támadásokat hivatottak megelőzni. Ezt már többször láthattuk a gyakorlatban, ilyenre volt példa Sapour Monian egykori biztonsági tanácsadó esete, akit bűnösnek találtak az Egyesült Államok szabadalmaztatott repülési technológiáját körülvevő titkok Kínának történő eladásában. Moniant először egy nő kereste meg, aki azt állította, hogy egy műszaki toborzó cégnél dolgozik és lehetőséget kínált neki, hogy adjon tanácsot a kínai repülési iparnak. [114]

***Legnépszerűbb webhely alapú közösségi média platformok***

- Facebook (Egyesült Államok)
- X (korábban Twitter) (Egyesült Államok)
- LinkedIn (Egyesült Államok)
- Threads (Egyesült Államok)
- Tumblr (Egyesült Államok)
- Reddit (Egyesült Államok)
- Sina Weibo (Kína)
- Ask.fm (Lettország)

***Legnépszerűbb kép- és videóalapú közösségi média platformok***

- YouTube (Egyesült Államok)
- Instagram (Egyesült Államok)
- Snapchat (Egyesült Államok)
- TikTok (Kína)
- Pinterest (Egyesült Államok)
- Flickr (Egyesült Államok)
- Tinder (Egyesült Államok)

***Legnépszerűbb közösségi média csevegő alkalmazások***

- Facebook Messenger (Egyesült Államok)
- Telegram Messenger (Oroszország)
- WhatsApp Messenger (Egyesült Államok)

***Egyéb kapcsolatépítő alkalmazások***

- Discord (Egyesült Államok)
- Rakuten Viber Messenger (korábban Viber) (Japán)

## 2.3 A pszichológiai manipuláció alkalmazása a politikában

### 2.3.1 A kritikus gondolkozás a döntéshozatalban

A kritikai gondolkodás az az intellektuálisan fegyelmezett folyamat, amelynek során a megfigyelésből, tapasztalatból, reflexióból, érvelésből vagy kommunikációból gyűjtött vagy ezek által generált információk aktívan és ügyesen fogalmi felépítését, alkalmazását, elemzését, szintetizálását és/vagy értékelését végzik, a hit és cselekvés iránymutatójaként. Példaértékű formában olyan egyetemes intellektuális értékeken alapul, amelyek túlmutatnak a tárgyi megosztottságon: letisztultság, pontosság, precizitás, következetesség, relevancia, megalapozott bizonyítékok, megfelelő indokok, mélység, terjedelem és méltányosság. [115] Az elmúlt évszázadban figyelmen kívül hagyták, valamint a kritikai gondolkodás értékeléséről festett kép túl rózsás, de vannak remények a jobb irányba fordulásra. Logikája a Blooms-féle oktatási célok taxonómiáján alapul: elemzés, szintézis és értékelés. A kritikai gondolkodást, mint fogalmat meghatározták már úgy is, mint: *„az állítások helyes értékelése”*. [116, p. 179] A kritikai gondolkodás egy alapvető kompetencia, mint ahogy az olvasást és az írást is meg kell tanítani a jövő generációinak. Három fő tényezője az értelmezési, elemzési és értékelési képesség. Van, akik szerint: *„a megfigyelések és a kommunikáció, az információ és az érvelés képzett és aktív értelmezése és értékelése”* jelenti ezt. [117] Olyan elképzelés is létezik, amely szerint a kritikai gondolkodás önkorrekció, kritériumai vannak, ill. érzékeny a kontextusra. [118]

***A kritikai gondolkodás logikai struktúrája***

1. Probléma meghatározása
2. Kutatás
3. Adatok relevanciájának meghatározása
4. Kérdések felvetése
5. Legjobb megoldás meghatározása
6. Megoldás bemutatása
7. Döntés kiértékelése

Lényegében a **tudományos kutatás módszerével** közel megegyező módszertan, annyi különbséggel, hogy a korábban alkalmazott módszerek nem kapnak szerepet a vizsgálat során, mondhatni ad-hoc jelleggel keresi a megoldást a felmerült problémára a legjobb gyakorlatokat (best practice) követve és előállítva egyéni gyakorlatát kimenetként.

*A hamis valóság: a „fake news" világa*

**Álhír:** (fake news, hoax news): A Cambridge szótár szerint a hamis hírek azok, amelyek hírnek tűnnek, az interneten vagy más médián keresztül terjednek, és általában politikai nézetek befolyásolására vagy viccből készültek. [119]

Az elmúlt években végbement változások alapjaiban változtatták meg a világról alkotott képünket. Korábban a dokumentáltság hitelességét közlemények, képi- és videótechnológiával készített anyagok kellőképpen alátámasztottnak bizonyultak, azonban manapság rengeteg esemény hamisítható meg, egy illúziót léptetve annak helyébe. A **mesterséges intelligencia** (továbbiakban: AI) fejlődésével és alkalmazásával akár már élő kapcsolatban közvetített videókommunikáció is meghamisítható, kihasználva az arcfelismerésen alapuló képalkotás adta lehetőségeket. Létezik már AI-alapú hanghatás manipuláció egy voice.ai alkalmazás [120] használatával, amely révén egy adott személy hangján vagyunk képesek megszólalni. A képek és videóanyagok szerkesztése során is régóta bevett gyakorlat, hogy bizonyos pozíciókból, kívánatos szögekből, fény és színkezeléssel dolgoznak a készítők, magasabban preferált hatások kiváltásának reménye érdekében. Az információkezelésben három általános elemet használnak az információ manipulálására társadalmi befolyásolás céljából:

• **Hiányzó kontextus:** Az információkat félrevezető módon jelenítik meg, vagy néhány lényeges tény hiányzik. Ez általában úgy nyilvánul meg a közösségi médiában, hogy olyan fényképet mutatnak be, amelynek semmi köze a felirathoz. Például egy kép, amely erőszakot ábrázol egy város utcájában, a következő felirattal: „Nézd meg, mi történik ma Amerikában!" De a kép valójában egy európai városban készült.

• **Megtévesztő szerkesztés**: Itt a fenyegetés szereplője olyasvalamit készít, ami egykor valódi fotó, videó vagy illusztráció volt egy médiatörténetről vagy eseményről, de kulcsfontosságú elemeket szerkeszt, így eltorzítja a valóságot, és más üzenetet hoz létre.

• **Rosszindulatú átalakítás:** Ez a három közül a legsúlyosabb. Az AI alapú videómódosítás célja, hogy valamilyen hamisítványt hozzanak létre, ami valódinak tűnik. Ezek az úgynevezett mély hamisítványok (deepfakes). A fenyegetés szereplői ezekkel a technikákkal napirendet hajtanak végre, legyen szó egy zsarolóvírus-kampányról pénzügyi haszonszerzés céljából, vagy a társadalmi eredmények, például a választások manipulálására. [121]

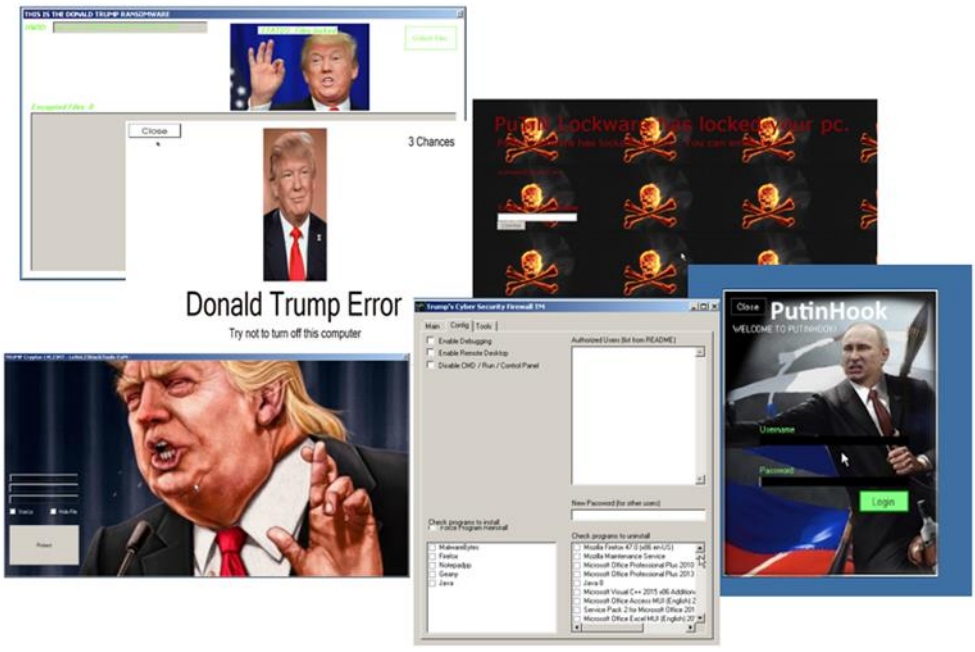
2020. április 2-án felgyújtottak egy vezeték nélküli tornyot Birminghamben. Több olyan eset is összefüggött az interneten pletykával, amely még a közösségi médiában is (például Facebook, Twitter, Instagram) terjedt el, hogy az 5G tornyok serkentik a Covid-19 fertőzéses eseteket. Volt egy videó a YouTube-on, ahol az Egyesült Királyságban egy mobilhálózati cég állítólagos korábbi vezetője vallotta, hogy a teszteket a vírus terjesztése érdekében hozták létre, és a világjárvány csak tévút volt a halálesetek elrejtésére, ami mobil technológiával hozható összefüggésbe. E hamis információ miatt a rendőrség és a távközlési cégek jelentései szerint [122] országszerte több mint 30 esetet jelentettek vandalizmusról és erőszakos cselekményről vezeték nélküli tornyok ellen a hónapban. A tornyok elleni támadások szimbolikus jellegűek voltak. [123] Az álkampány indítéka intellektuális kihívás volt, de inkább egy egyéni célpont vagy egy csoport ellen, az internetes közösséget célozta meg. A manipuláció sikere a járványhelyzet alatti éveket meghatározó bizonytalan helyzeten alapult, és a társadalom nem ismeri e technológiák tényleges működését. A járványhelyzet különösen egyedülálló esemény volt a modern kori történelemben. Napjaink kiterjedt kommunikációs lehetőségei megteremtették az alapot a világ kormányainak döntéshozói számára az összehangolt szabályozási eljárások kialakításához és alkalmazásához. Napjainkban a közösségi média meghatározó szerepet tölt be a tájékoztatásban, különösen, ha közeli ismerőseinkkel kapcsolatos eseményekről vagy a társadalmi életet érintő kérdésekről kell tájékozódni. A világjárvány elleni küzdelem komoly kihívást jelentett a kormányok számára világszerte, azonban a helyzet orvoslása más volt. Egyes országok, mint például a Kínai Népköztársaság, ahol az első fertőzötteket is azonosították, zéró tolerancia stratégiát alkalmaztak, és állampolgárok millióit kényszerítették arra, hogy otthon maradjanak, korlátozva mozgási szabadságukat.

Előre szóltak a találgatások a 2020-as amerikai elnökválasztással kapcsolatban, hogy lesz-e olyan körülmény, mint amilyen 2016-ban volt, ami kétségbe vonná a választás lezajlásának tisztaságát. A rossz megközelítés ebben az esetben is az, hogy **a cél manapság nem az eredmények meghamisítása, hanem a folyamatokba való beavatkozás** és a közvélemény hozzáállásának és reagálásának a formálása. Ugyanis, ha abból indulunk ki, hogy egy választás eredménye hamis, azaz nem tükrözi a választópolgárok kinyilvánított akaratát, akkor szükségszerűen meg kellene jelennie egy reakciónak (releváns utcai zavargások, magas létszámú tüntetések, sztrájk stb.) ami igazolhatná, hogy csalás történt. Ha eleve a közhangulat kerül befolyásolásra, akkor a törvényi keretek között a legitim játékszabályok feltételezett betartása (amennyiben

észrevétlenül maradnak a háttérben az adatközpontok felépítései, monitorizálások, szavazólisták készítése jogosulatlan adatszerzés mellett stb.) valósíthatók meg a kívánt kimenetek. Ebben az esetben már nem beszélhetünk az eredmények tükrében csalásról, viszont, hogy ezt az eredményt milyen eszközök alkalmazása révén érjük el, meglehetősen vitatható. [124]

### *A Talos Group elemzése a politikai tematikájú rosszindulatú szoftverekről*

Az Egyesült Államokban a Cisco Talos csoport által 2019 novemberében közzétett jelentésben néhány malware terjesztéssel kapcsolatos esetet vizsgált meg, ahol a támadók szervezetten politikai szereplőkkel hirdettek, különösképpen az éppen hivatalban lévő amerikai elnökkel, Donald Trumppal. A vírusok között ransomware és trójai típusok is megjelentek, mely előbbi díjfizetésre kényszeríti az áldozatot és zárolja, valamint titkosítja az adatokat, a trójai esetében pedig rejtett hozzáféréssel hátsó bejáratot biztosít a hálózaton belül. Az alábbi képen (2. ábra) néhány zsarolóvírus (Trump Crypter, PutinHook stb) és egy trójai program (Trump Cyber Security Firewall) látható, amely igyekszik az áldozattal elhitetni, hogy az említett politikai szereplők felelősek a számítógép zárolásáért vagy annak működésének kompromitálódásáért. [125]

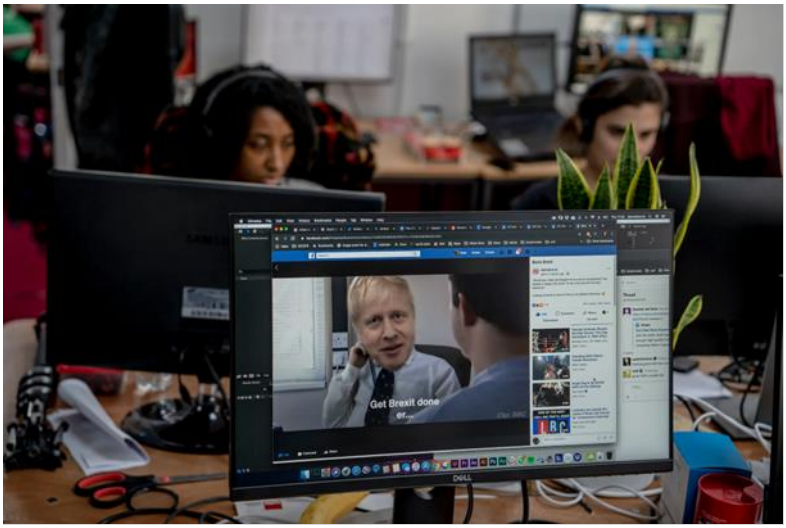



*2. ábra Malware/Ransomware példa 2020-ban politikai témában*

*Forrás: talosintelligence.com*

Egy esetleges külföldi beavatkozás híresztelése az online megtévesztés egyik leghatékonyabb forrása volt régebben sorsdöntő választások előtt. A 2019-es brit parlamenti választások során azonban néhány jelölt maga is ilyen manipulációs

taktikához fordult a brit választási kampányban. Hamis Twitter-fiókok, manipulált videók, trükkös weboldalak és természetesen a választásokba beavatkozó külföldi érdekeltségek kérdése is az asztalon volt. A választópolgárok egy „szelíd ízelítőt" kaptak az online kampányolás által nyújtott lehetőségek tárházából egy olyan fontos választás előtt, amely egy generáció sorsát döntheti el. [126] A **lejáratás** (blackmailing) egyik tipikus eszköze a **szabotálás**nak (sabotage). Jelen esetben a technika alkalmazásán van a hangsúly a politikában, legális forrásokon keresztül. Ismert politikai szereplő, ismert filmrészlet vagy jelenet (könnyebb azonosítás, amely segít a terjesztésben) és az időzítés, amely jellemzően a leginteraktívabb időszakban, a választási hajrában az utolsó héten jelenik meg. A Momentum (a brit Munkáspárt lobbiszervezete) által megszerkesztett videóban (3. ábra) a brit konzervatívok jelöltjét egy divatmagazin szerkesztőjének szerepébe öltöztették, melyhez tartozó hanganyagot Boris Johnson saját kampányvideója szolgáltatott, annyi különbséggel, hogy úgy szerkesztették meg a videót, hogy a végén Jeremy Corbynt javasolja a brit parlament következő miniszterelnöknek.




*3. ábra A brit Munkáspárt dezinformációs kampányvideójának pillanatképe*

*Forrás: nytimes.com*

Az internet adta lehetőségek között ott szerepel az is, hogy ezeknek a dolgoknak nem csupán a terjesztése adott, hanem utána is tudunk járni viszonylag gyorsan és egyszerűen a hírek valódiságának. Nem árt, hogy ha több forrásból tájékozódunk, összevetjük egymással őket, majd ezek után formálunk véleményt. Ez nem jelenti azt, hogy minden, amit elénk tesznek az csak és kizárólag megtévesztő jellegű, viszont tudnunk kell olvasni a sorok között. A példának bemutatott videón még jól fellelhető, hogy manipulált dologról van szó, azonban rendelkezésre állnak olyan szerkesztési metodikák is,

amelyeknél a szerkesztés ténye messze nem ennyire szembetűnő. A brit Guardianban jelent meg egy cikk 2019 novemberében a politikai hirdetések szereplésével kapcsolatban az online térben, mely cikkben a szerzők azt részletezik, hogy a politikai pártoknak el kellene számolniuk a közvélemény felé a finanszírozott hirdetések helyéről, tárgyáról és azok árával kapcsolatban a tiszta verseny érdekében. Számos szabályozási rés van azonban, amelyet a közösségi média felületek birtoklói és az adatbrókerek jó üzleti lehetőségnek tekintenek. A digitális politikai hirdetések piaca különbözik a hagyományos nyomtatott vagy televízióban sugárzott eszközöktől, mert az új generációs hirdetések adat alapúak, amelyek személyre szabottan fogyasztói magatartás függvényében jól szegmentálhatók a lakosságon belül. Nem lehetünk biztosak abban, hogy a környezetünk ugyanazokat a tartalmakat kapják, mint mi magunk, így fennáll a veszélye konfliktusok generálódásának számára, mert az egyes hirdetések más-más hallgatóságnak vannak címezve (politikai táborok). Az adat alapú hirdetések és a tartalom marketing multimilliárd dolláros iparággá nőtte ki magát az utóbbi években és a politikai pártok, valamint a hozzájuk kapcsolódó csoportok komoly összegeket fektetnek ebbe. [127]


*4. ábra A brit Konzervatív Párt dezinformációs kampányvideójának pillanatképe*

*Forrás: theguardian.com*

Ebben a videóban (4.ábra) a brit Konzervatív Párt azt állította a brit Munkáspárt képviselőről, hogy a pártnak nincs valós forgatókönyve a Brexit tárgyalások rendezéséről, az eredeti interjúban a riporter kérdésére adott választ egy néma hallgatásra és pislogásra cserélve, benne a konzervatívok politikai üzenetével: ellenfeleiknek nincs valódi válaszuk a kérdés rendezésére. Fontos itt megjegyezni, hogy ebben az esetben látszólag minden szereplő egymásra mutat, viszont a szálak összeérnek. A brit kampányban a két jelentősebb párt, a Konzervatív Párt és a Munkáspárt egyaránt alkalmazta a rendelkezésre

álló eszközöket a siker érdekében. Ami viszont lényegében változtatja meg a dolgokat az pedig az, hogy a nagy adathalmazok birtokában lévő szervezetek a technológiai szektorban jelentős befolyással bírnak a közhangulat alakításában, hiszen ezeken a felületeken jelennek meg a hirdetések, ők moderálják a tartalmat, valamint a választópolgárok adófizetői pénzét teszik el a szolgáltatásuk nyújtása során, az fizeti a számlát, akit befolyásolni szeretnének a valótlan tartalmakkal. Így a felvetés jogos lenne a választók részéről, hogy mégis mennyibe kerül ez nekik.

### 2.3.2 Beavatkozási kísérletek demokratikus folyamatokba

A 2016-os amerikai elnökválasztás, illetve az azt megelőző kampány időszaka mérföldkövet jelentett az informatikai támadások és médiaeszközök manipulatív használata szempontjából a választások befolyásolásának gyanúja népszerű és sokat foglalkoztatott téma volt. [128] Egy emlékezetes pillanat, ahonnan a „fake news" kifejezés, ami az eredeti szövegkörnyezetében álhírgyárként érdemes fordítani, 2017. január 11.-re datálandó. Donald Trump ekkor az Egyesült Államok 45. megválasztott elnöke (president-elect) beiktatása előtti napokban tartott sajtótájékoztatón megtagadta Jim Acosta, a CNN riporterének történő válaszadást. Itt hangzott el az azóta is sokszor előkerülő szállóige: „A szervezeted siralmas, álhírgyárosok vagytok." [129] A FoxNews hírcsatorna a New York Post által közzétett cikkre hivatkozik, amiben Hunter Biden üzleti ügyeiről van szó, ahol Ukrajna és Kína feltételezetten részese egy a nagyobb orosz dezinformációs próbálkozásnak a 2020-as választásokon. A laptop sztorit egy hamis narratívának értékelték, ami mögött a Kreml tevékenységét feltételezték [130] Az Egyesült Államokban a 2018-as félidős választások alkalmával a szabadúszó hackerek 20 különböző állam szavazói adatbázisait kínálták a **dark web**-en[4], ahol személyes adatokat, csakúgy, mint azonosítókat, teljes neveket, elérhetőségeket (telefonszámok és címek), a szavazók nemi identitása és akár nemzetiségükre vonatkozó információt. Ez jó kiindulópont lehet a direkt marketing kampányhoz. A jelentés emellett részletesen kitér a közösségi oldalak hackelésére, számokban kínálva követőinek számát, amivel befolyásolni lehetne a közvéleményt. Végül pedig DDoS támadásokat, e-mail listákat, banki és állami adatbázis-feltörést kínálnak, de hangsúlyozzák, hogy nem fogadnak el

[4] Dark web (sötét web): Az internethálózat azon szegmense, amely a megszokott eszközökkel való böngészés során nem fellelhető, valamint illegális tevékenységek folytatására hivatott felületek összessége

közösségi média fiókok feltörésére irányuló kéréseket. [131] [69] Egy másik esetben adatokat szivárogtattak ki az orosz biztonsági szolgálatoknak. „A Kreml belépett a chatbe” [132] című cikk Marina Matsapulina orosz ellenzéki aktivista történetét meséli el, akinek a Telegram privát csoportos chatjét a biztonsági erők olvasták. A cikkre válaszul a Telegram oldalán megjelent egy cikk, amelyben „kilenc hibát” említenek többek között azt, hogy az ellenzéki politikus azonosításához nincsen bizonyíték arra, hogy a hatóságoknak betekintése lett volna a levelezésbe, a helymeghatározás az orosz biztonsági szolgálat (FSB) hatékony eszközeinek köszönhető. [133]

Egy 2023-as felmérés szerint [134] az ukránok a háború idején nagymértékben támaszkodnak a Telegram csatornáira, hogy híreket kapjanak.

- Az ukránok 72%-a használja a Telegramot információk vagy hírek megszerzésére, amit a Facebook és a YouTube követ a sorban.
- A kiemelt fontosságú hírekhez való gyors hozzáférés lehetősége, a részletes utasítások megszerzését lehetővé tevő botok, a kis online boltok, valamint a privát chatekben és csoportokban történő hívások és üzenetek voltak azok a tényezők, amelyek 2023-ban a Telegram preferálását jellemezték.

### 2.3.3 A katonai tevékenység feltűnése a közösségi médiában

A hibrid hadviselés sajátja, hogy a körülményekhez való alkalmazkodás képessége magas. Célja minden esetben a társdalami destabilizáció, az ellenséges állam megszokott működésének az ellehetetlenítése. [135] Ezek eléréséhez olyan eszközökhöz fordulnak, amelyek társadalmi elégedetlenséget szülnek, és a társadalom ingerküszöbének megváltoztatásával egy későbbi időpontra tervezett művelet sikerességét készítik elő, az ingerküszöb befolyásolásával a társadalmi ellenállás mértéke is megváltozik. [136] Így a „Twitter-háborúk” is valós veszteségeket okozhatnak és a vírusként terjedő félretájékoztatás nemcsak a csaták eredményét, hanem a nemzetek sorsát is képesek megváltoztatni. A háború, a technológia és a politika egy újfajta csatatérré keveredett össze, amely okostelefonjainkon játszható. [137] A regionális feszültségek előfordulási gyakorisága változó félben van napjainkban, a hagyományos állam-állam elleni konfliktusoktól eltérő mintázatban jelenik meg. [138, p. 673] Ezeknek a katonai műveleteknek számos elnevezése forog a szakirodalomban, mint például az aszimmetrikus, irreguláris, felkelés elleni vagy hibrid hadviselés, illetve a kibertérben végzett műveletek is ide sorolandók. Ezeket gyűjtőfogalma a negyedik generációs

hadviselés, ahol a hadszíntéren a katonák mellett megjelennek civil szereplők is, ezáltal a műveleti területen a civilek is katonai műveletek érintettjeivé válnak. Innentől a konfliktus a társadalom egészét érinti, nem kizárólag a katonai szereplőket, így ezekben a műveletekben a nem állami szereplők és a lakosság befolyásolása is prioritást nyer. Jellemzően az adaptív információs fölény elérése a kezdeti cél, ahol nem az ellenséges erők kommunikációjának zavarás elsőrendű, hanem a célközönség élethelyzetének, gondolatainak és véleményének a befolyásolása, más szóval a háborús morál alakítása kulcsjelentőségű. [139] [140] [141] A közösségi média, mint digitális hadszíntér szorosan egybekapcsolódik a lélektani hadviseléssel, mivel nagy célközönségek gyűjtőhelyét jelenti. Olyan személyek is elérhetők ezeken a platformokon, akik alapvetően nehezen megközelíthetők, ami elsősorban a technológia magas szintű penetrációjának köszönhető. A közösségi média a civil-katonai együttműködés szempontjából is meghatározó szerepet játszik, hiszen egy-egy háborús konfliktus esetén segíthet a nem katonai feladatok ellátásában, így jó közvetítő eszköz lehet. [142] A közösségi média a műveleti biztonságot is képes közvetett módon befolyásolni, ami a nem megfelelő adat- és információbiztonságból ered. Előfordult, hogy műveleteket kellett elhalasztani, mert a katonák egy közösségi oldalon keresztül tárgyaltak meg az adott művelethez tartozó információt (bejegyzés létrehozása keretében is), amelyhez való hozzáférés révén támadást indítottak a katonák ellen a velük szemben álló ellenséges erők. [143] A közösségi média mindennapi életünk szerves része. Világszerte 4,8 milliárd közösségimédia-felhasználóval – ami a világ népességének 59,9%-át teszi ki – a közösségi platformok az információgyűjtés, a barátainkkal és szeretteinkkel való kapcsolatfelvétel, valamint a vállalkozásunk bővítésének szükséges csomópontjaivá váltak. A közösségimédia-felhasználók pedig egyre jobban bíznak és támaszkodnak preferált közösségi hálózataikra a valós idejű hírektől és frissítésektől kezdve az életviteli trükkökig (life hacks), a termékfejlesztésen keresztül még sok okból kifolyólag. [144] A felhasználók aktivitását (2. táblázat) és a havi aktív felhasználók számát tekintve 2020-óta az adatok folyamatosan növekvő tendenciát mutatnak.

*2. táblázat A 10 legnépszerűbb közösségi média weboldal*

| Oldal neve | Havi aktív felhasználók száma (MAU*) |
|---|---|
| 1. Facebook | 3 milliárd fő |
| 2. YouTube | 2,5 milliárd fő |
| 3. Instagram | 2 milliárd fő |
| 4. TikTok | 1,2 milliárd fő |
| 5. Snapchat | 750 millió fő |
| 6. X (Twitter) | 541 millió fő |
| 7. Pinterest | 465 millió fő |
| 8. Reddit | 430 millió fő |
| 9. LinkedIn | <350 millió fő |
| 10. Threads | 100 millió fő |

*Havi aktív felhasználók száma világszerte 2023 októberében mért adatok alapján

*Forrás: searchenginejournal.com*

***Részkövetkeztetés***

A fejezetben bemutatásra került az internet transzformálódásának köszönhető ***eszközhasználatban*** bekövetkezett változás. Az interaktív internethasználat lehetővé tette kezdetben közösségi oldalak, később pedig a közösségi média megszületését, amivel az információ terjesztésének módszerei új irányokat szabtak. Megszülettek a mobileszközök és alkalmazások iparágai, amelyek tovább ösztönözték a felhasználóbázisok növekedését ezeken a platformokon, amely napjainkra a Föld lakosságának arányaiban mérhetők. Változásokat hoztak a közéleti diskurzusokban is, hiszen az üzleti és magánszereplők mellett idővel a politikai szereplők is számottevő jelenléttel, valamint befolyásolási képességekkel vannak már jelen ezeken a tereken is. A közösségi média lehetővé tette, hogy a földrajzilag távol eső területek társadalmai időben és térben azonos síkon legyenek képesek mozogni (kommunikálni), egymásra kölcsönhatást gyakorolva. Bár a hírközlésben rövid információk korábban is terjedtek nagy távolságokon, az információ mennyisége radikális mértékben megnőtt. Manapság pár kattintással képek, videók és hangrögzítések könyvtárméretekben elérhetők az interneten keresztül, bár azok hitelessége sok esetben megkérdőjelezhető.

# 3 AZ EMBERI KAPCSOLATOK TERMÉSZETE, A BIZALOM SZERKEZETI FELÉPÍTÉSE

*„Mondottam ember: küzdj és bízva bízzál!”*
Madách

***Bevezetés***

A technológia és a kommunikáció fejlődésével robbanásszerű változások mentek végbe és zajlanak most is a világban a hírek terjedési sebessége, valóságtartalma, valamint hitelessége szempontjából. Egy olyan korban élünk, ahol a híreket jellemzően nem csak gyűjteni képesek az emberek, hanem megtervezni a tartalmát, megszervezni a környezetét és az elbeszélési módját (narratíváját) ezzel mesterséges keretbe helyezni, a szereplők körét, a gazdasági-társadalmi reakciókat és hatásokat, illetve azok eszkalációs forgatókönyvét is deklarálhatják. Ez köszönhető annak, hogy globális, azaz a bolygóra kiterjedő kommunikációs infrastruktúra van jelen a vezetékes hálózati megoldásoktól a műholdas rendszerekig, amelyek szünetmentesen állnak rendelkezésre, hogy azok a távolságok, amelyek a történelem során a nagyobb társadalmi közösségeket (civilizációkat) földrajzi, demográfiai és számos egyéb tényező révén elválasztották egymástól, azok ma már nem jelentenek akadályozó szerepet a kommunikációban.

**Bizalom:** *„a személynek a jövő felé irányuló érzése, érzelme, a jövőbe vetett hite, reménye, aki bízik hisz az események, körülmények kedvező alakulásában;”* [145]

Az embernek öt alapvető érzéke van: **tapintás**, **látás**, **hallás**, **szaglás** és az **ízlelés**. Az egyes érzékekhez kapcsolódó érzékelő szervek információkat küldenek az agynak, hogy segítsenek megérteni és érzékelni a minket körülvevő világot. [146] A közösségi média térnyerésével a bizalomépítés folyamata is átalakult, hiszen az első benyomás sok esetben már nem egy személyes találkozó alkalmával valósul meg. A közösségi oldalak felhasználói profiljai lényegében előszűrésekre adnak lehetőséget, az információk mennyisége szempontjából pedig alkalmasak lehetnek egy-egy döntés meghozatalához is. Azt viszont nem árt leszögezni, hogy ezeken a felületeken megtalálható tartalom az esetek nagy részében torzított információ, a fényképek színeffektusokkal módosítottak (filter), a hanganyagok szűrök segítségével megváltoztathatók. A virtuális térben a tapintás, a szaglás és ízlelés működésképtelen érzékelők, tehát a minket körülvevő

környezet 60%-át nem észleljük. Az embert döntéseiben érzelmei jelentős mértékben képesek befolyásolni és ezek a személyes kontaktus hiányában nem tudnak kialakulni. A digitális térben bizonyos értelemben viszont ezek szimulálhatók. A **tapintás** az érintőképernyős eszközök használatával az **ízlés** és a **szaglás** pedig a tartalomfogyasztásban ragadható meg, hiszen ugyanezeket a fogalmakat használjuk az attitűdök kialakulása során.

A bizalom alapelvei a kétoldalú kapcsolaton alapulnak. Amikor ez megtörténik, legalább az egyik fél bízik a másikban. Létezik egy egyenletmodell, amelyben négy elem a következő: hitelesség, megbízhatóság, intimitás és önorientáció. A bizalom nem csak egy dolgot takar, a szavak és a tettek kapcsolata, valamint az ehhez fűződő érzelmi viszony határozza meg. Amikor információt osztunk meg másokkal, a lelkiállapot vagy érzelmi állapot az információ továbbítására használt csatorna és/vagy módszerek kényelmét és ismertségét írja le. Más szavakkal, biztonságos csatornának tekintjük, függetlenül attól, hogy az információ valóban igaz-e vagy sem.

***Vélekedések a bizalom fogalmáról***

Egyes szerzők a bizalmat úgy írták le, mint az egyén hite és hajlandósága arra vonatkozólag, hogy mások szavaiban, tetteiben és döntéseivel kapcsolatosan cselekedjen. Megállapításuk szerint két fő terület köré csoportosítható: szakmai és személyes. A szakmai kapcsolatok általában feladat orientáltak és a célok elérésére irányulnak, míg a személyes kapcsolatok inkább a szociális/érzelmi szférával foglalkoznak, és magára a kapcsolatra összpontosítanak. [147] A bizalom kulcsfontosságú elem a vezetésben is; mivel elengedhetetlen az egyénekkel való kapcsolatok fejlesztéséhez. Azok a vezetők, akik nem tudnak bizalmat kelteni a munkatársaikban, nem vezethetnek; nem lesz követőjük Továbbá ahhoz, hogy egy kapcsolatot kapcsolatként kezelhessünk, annak alapfeltétele, hogy bizalomnak kell lennie. Minden kapcsolatra jellemző egyfajta állandó könyvelési folyamat, ami baráttól barátig, cégtől ügyfélig tart. Minden interakció után futtatjuk a bizalmi algoritmust. Ezek azok a szűrők, amelyek kiválasztják azokat az embereket, akiknek bizalmat szavazunk, és elválasztják azoktól, akiknek ezt nem adjuk meg. [148]

A Black Isle Group tanulmány alapján [149] a „bizalom” kifejezést néhány különböző okból használjuk:

- Amikor le akarjuk írni valakinek a viselkedését (azaz „megbízható-e” az adott személy vagy „megbízható forrásnak” ítéljük meg).
- Ha azt akarjuk felmérni, hogy jól érezzük-e magunkat az információ megosztásában egy egyénnel, valamint,
- Amikor a bizalomról alkotott saját elképzeléseinket szeretnénk felhasználni mások mondandójának értelmezésére és megértésére.

***A bizalom szerkezeti felépítése, a bizalmi egyenlet***

A „Bizalmi-egyenlet” egy matematikai modell, ami a *Trusted Advisor* [150] c. könyvben jelenik meg. A szerzők négy szempont köré rendezik a bizalom felépülésének jellemzőit, ami az alábbiakban testesül meg:

$$T_{rustworthiness} = \frac{C_{redibility} + R_{eliability} + I_{ntimacy}}{S_{elf-Orientation}}$$

*A “Bizalmi-egyenlet” Maister és szerzőtársai által (2000)*

Az évek során többen is megosztották gondolataikat a modellről és annak relevanciájáról. [151] [152] Egyszerre zseniálisnak és éleslátónak tűnik, mivel magában foglalja a bizalom megteremtésének négy alapvető tényezőjét – a hitelességet, a megbízhatóságot, az intimitást és az önorientációt. Az üzenet az, hogy gondoljunk mások szükségleteire, ne pedig önmagunkra, ami egy nyilvánvaló, viszont jól megfogalmazott szempont. [153]

Elméleti szinten osztják a bizalmi egyenlet logikáját, viszont sok más elméleti koncepcióhoz hasonlóan a logika gyakorlati alkalmazása nehéz lehet. [154] Kritika érte az önorientáció változóját is, amit erősen súlyozottnak ítéltek meg. [155] Ez azonban logikusnak tűnik, hiszen az egyén orientációja határozza meg a bizalomépítés irányát. A súlyozás gondolata innen indul. Ez egy iránytű, és ez határozza meg kockázatvállalási magatartásunkat is. Az emberek nagy általánosságban nem bíznak az intézményekben vagy szervezetekben, hanem inkább a szervezeteken belül, az **emberek felé** helyezik a bizalmukat. A vállalatokat gyakran hitelesnek és megbízhatónak nevezik – ez a bizalmi egyenlet első két eleme. Az utolsó kettő egyénekre vonatkozik. Ez az ötlet vonzó lehet,

mert a szervezetek kevésbé valószínű, hogy fizikai megjelenést varázsolnak, így ebből a szempontból nehezebb számon kérni őket. A szorosabb és bensőségesebb kapcsolatok azért felelnek meg az egyéneknek, mert könnyebben elképzelhetőek, ha nem elérhetőek és kapcsolatba léphetnek. De a négy elem terjesztése valójában meglehetősen átgondolt; „Az önorientáció az a tényező, amely csökkenti a vezetésbe vetett bizalmat." [156] Ami azt jelenti, hogy az egyének egymás közötti interakciójának módja meghatározza a megbízhatóság észlelését a szemükben. [157]

***A bizalomépítés kérdésének továbbfejlesztett modellje***

A felülvizsgált modell [158] ugyanazokat a tényezőket használja, mint az eredeti, viszont **megjelenik a faktorok súlyozása** a hitelességgel, megbízhatósággal, intimitással és önorientációval kapcsolatban. A bizalom alapköve az érintett felek közötti kommunikáció. Az adott szó a modell kulcseleme, ebből kifolyólag jelenik meg nagyobb súlyozással a tört számlálójában.

A ***kommunikáció*** (hitelesség) változó eredménye, hogy egy állítás lehet igaz vagy hamis mert a megbízó értékelése saját meggyőződésén és tapasztalatain alapul. Ez egy logikai döntés, amely az **50%** valószínűségen alapszik.

A ***cselekedetek*** (megbízhatóság) változó azon az elgondoláson alapul, hogy egy esemény három lehetséges eredményt hozhat, ha tervezésen alapul: a tervvel egyező kimenet, a tervvel ellenkező kimenet, vagy a terven kívüli eredmény születik. A kimenetek ezáltal a klasszikus három kimenetes formában alakulnak. Pozitív, negatív és semleges más szavakkal győzelem, vereség és döntetlen; ezek adják a **33%** valószínűséget.

A ***tudatossági*** (intimitás) változó értéke a fennmaradó **17%**, melynek előjele azért két irányú, mert az érzelmi változó képes pozitív és negatív irányba alakítani a bizalomépítés folyamatát. A döntéshozatalt követő kimenetek amennyiben számunkra pozitív benyomást keltenek, tovább erősítik a kapcsolatot, ellenben a negatív töltetű kimenetek romboló hatást eredményeznek, erodálják a bizalmat.

A ***célpont*** (önorientáció) változó **„r"-értéke** (kockázat) mindig a legkisebb számláló béli értékhez tartozó súlyt veszi fel. A kommunikációs és cselekvési tényezők nem vehetnek fel zérus értéket, mert ha nincs kommunikáció vagy cselekvés, akkor a célváltozót sem lehet meghatározni.

## 3.1 A bizalomépítés egyenlete : Trust – CAST modell

Trust – CAST modell

$$\boldsymbol{T_{rust}(\Omega)} = \frac{\boldsymbol{C_{ommunication}} * \ (\boldsymbol{\alpha = 50\%}) + \boldsymbol{A_{ctions}} * \ (\boldsymbol{\beta = 33\%}) \pm \boldsymbol{S_{elf-Awareness}} * \ (\boldsymbol{\gamma = \ 17\%})}{\boldsymbol{T_{arget}} \ (\boldsymbol{\delta = \frac{1}{1 - r}})}$$

- Communication: Kommunikáció
- Actions: Cselekedetek
- Self-Awareness: Tudatosság (Önismeret)
- Target: Célpont

***Szélsőértékek (extreme values)***

Érzelmi beavatkozás nélkül

$$\frac{0{,}50+0{,}33\pm0}{\frac{1}{1-0{,}17\ (Tudatosság\ maxiumum)}} = \frac{0{,}83}{1{,}20481927} = 68{,}89\%$$

A számláló összes változójával maximális értékkel (érzelmi interferenciával)

$$\frac{0{,}50+0{,}33\pm0{,}17}{\frac{1}{1-0{,}17\ (Tudatosság\ maximum)}} = \frac{0{,}66 < x < 1}{1{,}20481927} = 54{,}78\% \text{ és } 83{,}00\% \text{ között}$$

Kockázati faktorok értékei (risk factor values)

Tudatossági (**S**) kockázat: $\frac{1}{1-0{,}17\ (Tudatosság\ maximum)} = \frac{1}{0{,}83} = 1{,}20481927$

Cselekvési (**A**) kockázat: $\frac{1}{1-0{,}33\ (Cselekedetek\ maximum)} = \frac{1}{0{,}67} = 1{,}49253731$

Kommunikációs (**C**) kockázat: $\frac{1}{1-0{,}5\ (Kommunikáció\ maximum)} = \frac{1}{0{,}5} = 2$

Zéró összegű forgatókönyv, ha nem vállal semmilyen kockázatot (zero-sum scenario)

$$\frac{0+0\pm0}{\frac{1}{1-0}} = \frac{0}{1} = 0$$

Amennyiben egy öt fokozatú skálát használunk a *kommunikáció* és a *cselekedetek* faktor súlyozására, az alábbi *forgatókönyvek* mentén alakul a bizalom:

*A legrosszabb eset forgatókönyv*

- Kommunikáció: 1/5 (0,2*0,5 = 0,1)
- Cselekedetek: 1/5 (0,2*0,33 = 0,066)
- Önismeret: 0,17
- Célpont: 1,49253731

Bizalom: $\frac{0,1+0,066\pm0,17}{\mathbf{1,49253731}}$ = (-0,00268) között kb. **0%** és (0,22512) **22,51%**

*Visszafogott forgatókönyv*

- Kommunikáció: 2/5 (0,4*0,5 = 0,2)
- Cselekedetek: 2/5 (0,4*0,33 = 0,132)
- Önismeret: 0,17
- Célpont: 1,49253731

Bizalom: $\frac{0,2+0,132\pm0,17}{\mathbf{1,49253731}}$ = (0,10854) **10,85%** és (0,33634) **33,63%** között

*Középutas megoldás forgatókönyv*

- Kommunikáció: 3/5 (0,6*0,5 = 0,3)
- Cselekedetek: 3/5 (0,6*0,33 = 0,198)
- Önismeret: 0,17
- Célpont: 1,20481927

Bizalom: $\frac{0,3+0,198\pm0,17}{\mathbf{1,20481927}}$ = (0,27224) **27,22%** és (0,55444) **55,44%** között

*Optimális döntés forgatókönyv*

- Kommunikáció: 4/5 (0,8*0,5 = 0,4)
- Cselekedetek: 4/5 (0,8*0,33 = 0,264)
- Önismeret: 0,17
- Célpont: 1,20481927

Bizalom: $\frac{0,4+0,264\pm0,17}{\mathbf{1,20481927}}$ = (0,41002) **41,00%** és (0,69222) **69,22%** között

*Legjobb eset forgatókönyv*

- Kommunikáció: 5/5 (0,5)
- Cselekedetek: 5/5 (0,33)
- Önismeret: 0,17
- Célpont: 1,20481927

Bizalom: $\frac{0,5+0,33\pm0,17}{\mathbf{1,20481927}}$ = (0,5478) **54,78%** és (0,83) **83%** között

## 3.2 Definíciók a kortárs információs környezet megértéséhez

A számítógépes hálózatok folyamatos fejlődésével kialakult egy virtuális tér, egy alternatív valóság, ahol jól lehet szimulálni, illetve modellezni az „offline" térben, más szavakkal a fizikai valóságban tapasztalt élethelyzeteket. A kommunikáció, illetve az emberi interakciók, valamint a tájékozódás szempontjából hatalmas különbségekkel találjuk szembe magunkat két három évtized távlatában. Egyre inkább közvetítő eszközök alkalmazásával éljük a mindennapjainkat, az emberi tevékenység minden szegletét behálózza a munkavégzéstől a szórakozásig. Ezek az eszközök viszont új biztonsági és kockázati veszélyforrások, amelyek használata során a megtévesztés széles körű arzenálját alkalmazzák a rosszindulatú szereplők. Ebben a környezetben [158] való tájékozódáshoz adnak kapaszkodót az alábbi fogalmak:

**A fizikai valóság:** Ez az a környezet, ahol az események történnek. Collins szótára a következőképpen írja le a két szót: „A fizikai dolgok valódi dolgok, amelyek megérinthetők és láthatók, nem pedig ötletek vagy kimondott szavak" és „a valóságot arra használod, hogy valós dolgokra vagy a dolgok valódi természetére hivatkozz, nem pedig elképzelt, kitalált vagy elméleti ötletek." A következőkben az ellentétek ugyanilyen módon történnek. [159]

**Virtuális vagy alternatív valóság:** Ez egy olyan környezet, ahol cselekvések szimulálhatók, és amely közvetlen kapcsolatban áll a fizikai valósággal. A szótári meghatározás szerint ez a fajta valóság elképzelt, kitalált vagy elméleti.

**Tény:** Egy lezárt esemény leírása, amely a fizikai valóságban történt, a lehető legnagyobb pontossággal és részletességgel. A Collins szótár szerint „a tények olyan információk, amelyeket fel lehet fedezni". [160]

**Igazság:** Ez egy olyan kijelentés egy eseményről, amelyből hiányoznak a részletes információk. A részleges igazság gondolata egyet jelent az egy bizonyos nézőpont kifejezéssel. A Collins szótár azt mondja, hogy „az igazság olyasvalami, amiről azt hiszik, hogy igaz". [161]

**Hazugság:** Ez egy kijelentés egy olyan eseményről, amely soha nem történt meg. A szótár szerint „hazugság az, amit valaki mond vagy ír, és amiről tudja, hogy nem igaz". Ez tehát különbözik a hibától. [162]

**Félrevezetés:** Egy olyan esemény melléknévi kijelentése, amelyre vonatkozóan nincs garancia arra, hogy az pontosan a leírt módon történt, és/vagy olyan elméleti elemeket tartalmaz, amelyek valószínűleg meg sem történtek. Tartalmazhat tényleges tényeket, amelyek célja az állítás érvényesítése, de vannak olyan elemek is az állításban, amelyek nem elég egyértelműek ahhoz, hogy összességében érvényesek legyenek. A félrevezetés célja a téves elképzelés és/vagy benyomás keltése.

**Dezinformáció:** Ez egy olyan állítás, amely egy soha meg nem történt eseményről szól. Tartalmazhat olyan elemeket, amelyek akár tények is lehetnek, azonban egy másik narratívát vagy eseményt takarnak, aminek nincs összefüggése az eredeti kijelentéssel. A kulcsfogalom az, hogy a dezinformáció mögött mindig ártó szándék áll. Lehet, hogy alternatív valóságra épül, de a szabályokat a fizikai valóság alapján mutatják be. Valakit dezinformáció terjesztésével vádolni azt jelenti, hogy megtévesztés céljából hamis információkat tesz közzé.

***Részkövetkeztetés***

Az emberi kapcsolatok vizsgálatában fontos szem előtt tartani az alapvető anyagi érdekekből fakadó nézetkülönbségeket, amelyek rányomják a bélyegjüket a kapcsolatok alakulására. Legyen szó magánéleti, vagy szakmai kapcsolatokról ezek a nézetkülönbségek adják a bizalom felépülésének alapvető mozgatóit. A közösségekhez való tartozás alapvető emberi igény, és ezekbe a csoportosulásokba való csatlakozás során támadó és védekező stratégiák egyaránt jelen vannak. Az érdekek vonatkozásában akár egyéni akár csoportérdek érvényesítéséről van szó, a kommunikációban szükségszerűen megjelenik a bizalom, az interakciók és az információcsere vonatkozásában a biztonságos közvetítési csatorna megítélésének fokmérője. Az információgyűjtés módszereit tekintve megállapítható, hogy ebben az építkezési folyamatban megváltoztak a kiindulási pontok. A tájékozódás során egyre inkább teret nyernek a közvetítő eszközök és a személyes interakciókra már csak előzetes szűrések és próbák után kerül csak sor. Az összekapcsolt világ technológiai fejlődése új problémákat vet fel. Az emberi tevékenység már elérte azt a szintet, hogy egyes embercsoportok nemcsak egymás létére jelentenek veszélyt, hanem tevékenységük jelentős hatással lehet a bolygó egyensúlyi állapotára, ami közvetve az egész emberi létet veszélyeztetheti a Földön, ebből kifolyólag a biztonság és a bizalom közvetlen kapcsolatban állnak egymással.

# 4 A PSZICHOLÓGIAI MANIPULÁCIÓ GEOPOLITIKAI ESEMÉNYEKRE GYAKOROLT HATÁSAINAK VIZSGÁLATA 2019-2023

*„Minden siker belépő egy még nehezebb problémához.”*
Kissinger

***Bevezetés***

A 2009-es globális pénzpiaci összeomlást követő tíz évben olyan események formálták a világpolitika alakulását, mint az arab tavasz, a Krím-félsziget annektálása és a hozzáfűződő szankciós intézkedések, az európai menekültválság és a vele párhuzamban álló terrorcselekmények, az Egyesült Királyság kilépése az Európai Unióból, amiről szóló népszavazás később Brexitként híresült el, az orosz beavatkozás valószínűsége a 2016-os amerikai elnökválasztásba, valamint a klímakatasztrófával kapcsolatos híradások.

**Geopolitika:** *„politikatudományi és politikai irányzat, amely az állam társadalmigazdasági viszonyait, fejlődését, nemzetközi törekvéseit elsősorban földrajzi tényezőkre (földrajzi fekvés, területi tényezők, lakosság, természeti adottságok) vezetik vissza; azoknak meghatározó jelnetőséget tulajdonít.”* [163, p. 315]

A szabadmozgás korlátozása során az egyes országok más-más kihívásokkal találják szemben magukat, mindenki saját országának adottságainak függvényében. Erre kiváló példa az Egyesült Államok és az európai országok közötti számottevő különbség, mely előbbinek nem volt szüksége a hatalmi egyensúly eszközének alkalmazására, hiszen két hatalmas óceán között helyezkedik el az ország. [164] Mivel mind földrajzilag, mind pedig történelmileg más utakat járnak ezek a nemzetállamok, így más szokások és elvek mentén alakítják politikájukat és az azokat kiszolgáló intézkedéseiket. Ez a pandémia idején sem volt másképp. Az internethez való nyílt hozzáférés új lehetőségeket kínál a rosszindulatú szereplők számára az információgyűjtésre, a sebezhető célpontok elleni támadásokra, valamint a tömegek felfogásának és viselkedésének alakítására. Ezek kezelésére olyan módszerek szolgálhatnak megoldásként, mint például a jogi rendszerek megerősítése, beleértve a nemzetközi normákat, a bizalomépítő intézkedések bevezetése és a kibertérrel kapcsolatos készségek fejlesztése. [165]

## 4.1 Covid-19 világjárvány alatti események a kiber- és a fizikai térben

A SARS-2 CoV-2 (Covid-19) koronavírus világjárvány kirobbanása nagy vízválasztót jelentett a modernkori mindennapok megítélésében. Már évek óta meglévő technológiai megoldások rendszerszintű alkalmazását erőszakolta ki az új helyzet, mint például a távoli hozzáféréssel működtetett tevékenységek (otthonról és távolról végzett munka, videókonferenciák) és a napi szintű online bejelentkezések száma is megsokszorozódott, tekintettel a járványügyi esetszámokban bekövetkezett változásokra. Ezzel egyidejűleg a kibertérben zajló események is intenzitást váltottak, megszaporodtak az egészségügyi intézmények ellen történő támadások, többségében zsarolóvírusok által. [166]

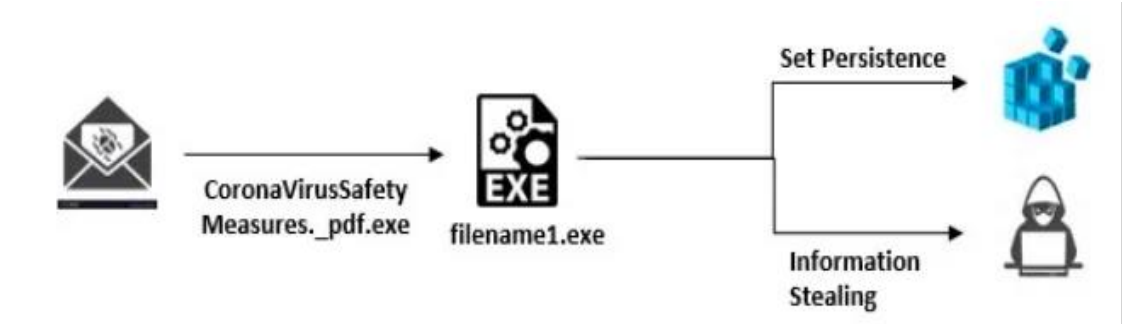
***Zsarolóvírusos támadások egészségügyi rendszerek ellen***

2018-ban az egészségügyi szervezetek a negyedik legáltalánosabb célpontjai (7%) voltak a **zsarolóvírus**os (ransomware) támadásoknak az iparági megoszlás alapján, egy 2019-ben megjelent a Cylance kiberbiztonsági vállalat elemzésében [167]. "Néha a zsarolóvírus olyan, mint az influenza. Amint a kórházak megoldást találnak a védelemre, egy új és kifinomultabb verzió üti fel a fejét." 2019 decemberében Hackensack Meridian Health csoport, amely 17 korházat számlál New Jerseyben lévő székhellyel, megerősítette, hogy fizetett a zsarolóknak annak érdekében, hogy újra hozzáférjen az informatikai rendszereihez. Ebből az következett, hogy a rendszerek két napig nem voltak elérhetők, és az osztályokat nem kritikus folyamatainak újra szervezésére, papíralapú dokumentálásra kényszerítette az elektronikus megoldások helyett. [168] „Ne vessük el azonnal a váltságdíj kifizetésének lehetőségét." mutatott rá Robert Garrett, a Hackensack Meridian Health igazgatója. Leszögezi, hogy sok esetben nem áll módunkban alkudozni a támadókkal, mert nem vagyunk abban a luxusban, hogy újraépítsük a rendszereinket, az idő szorít bennünket. [169] Amit ebben az esetben megfigyelhetünk, az a teljes kiszolgáltatottság. Egy kórházigazgató szemszögéből nézve az álláspont helytálló, viszont védelmi szempontból a kapitulációval egyenlő. Sokszor hivatkoznak ilyen típusú esetekben a szakértők véleményére a döntéshozók, hogy mennyire helyes vagy sem váltságdíjat fizetni.

Felmerül a kérdés, hogy a kibertevékenységek terrorista, adott esetben háborús cselekményeknek azonosíthatók-e, viszont az elkövető személy/csoport jellemzően rejtve marad. A kibertámadásokkal kapcsolatban általában elmondható, hogy a visszakövetési folyamatban (IP-címek visszakövetése) csak országokig jutunk el, tehát annyit tudunk

meghatározni, hogy melyik országból érkezhetett a támadás, a konkrét elkövető nemzetisége sem határozható meg sok esetben, ezért „casus belli” (háborús indok) sem fogalmazható meg.

A Yoroi olasz hátterű kiberbiztonsággal foglalkozó vállalat szokásos vizsgálatai során egy „CoronaVirusSafetyMeasures_pdf” állományra figyelt fel, amelynek jobban utána jártak. Itt egy átlagos SE taktikáról, egy adathalász **(phishing)** típusú támadásról beszélhetünk, a fentebb említett állomány egy email csatolmányát képezhette, egy külön erre kialakított tesztkörnyezetben hajtották végre a feltárást. A fájl megnyitása után több művelet zajlik le, először egy TLS alapú védett kapcsolatot alakít ki, amely egy “share.]dmca.]gripe” elérési útvonalú fájlmegosztóra mutat, ezt a fájlból kinyert mintából is ki tudták olvasni. Ezután néhány script fut le, amelyek megalapozzák a fertőzést, kulcsok generálódnak a beállításjegyzékben (5.ábra), amelyek segítenek elkerülni a számítógép újraindításával kapcsolatos eljárásokat. Végeredményképpen a felállított kapcsolat alapján adathalászatra kiválóan alkalmas fertőzéses támadásról van szó. [170]




*5. ábra A CoronaVirusSafety malware sematikus fertőzési útvonala*

*Forrás: yoroi.company*

Amit ebben az esetben láthatunk az a szokásos eszköztár: tömeges vagy célzott célpont irányába elkészített levél és egy vagy több álcázott melléklet az aktuális téma alapján. A COVID-19 keretei között éppen azért kiemelten veszélyesek ezek a próbálkozások, mert egy olyan világjárványról van szó, amellyel kapcsolatban minden egyes esemény egyenesen internetközpontú terjesztéssel is rendelkezik. A világ országaiban a meghatározó médiumok napi szinten számolnak be a „fejleményekről” idővel a társadalom teljesen elveszíti a napi rutinját a kitörést megelőző időkkel szemben. Felerősödik a „rugalmas” megoldások alkalmazása, széles körben terjednek el az internetalapú távoli hozzáférés útján történő munkavégzési megoldások, ezzel pedig újabb sebezhetőségek jelennek meg.

### *CISA ajánlás a COVID-19 keretében jelentkező kockázatkezelésben*

A kibertevékenységek elemzése során nem csak magukat a támadási eseményeket kell vizsgálni, hanem az érintett elemeket is, mint például a kritikus infrastruktúrák és az ellátási láncok; mert ezeknek a rendszereknek, intézményeknek, folyamatoknak a működtetése a rendkívüli helyzetben kiemelten fontos. A támadók potenciális célpontjainak számítanak, mellyel a megszokottnál magasabb intenzitású nyomást képesek gyakorolni. Az Egyesült Államok Védelmi Minisztériuma (DHS) márciusban mind a járványhelyzettel, mind a kiberbiztonsági eljárásokkal kapcsolatban tett javaslatokat, ahol több kulcsterületet határozott meg: [171]

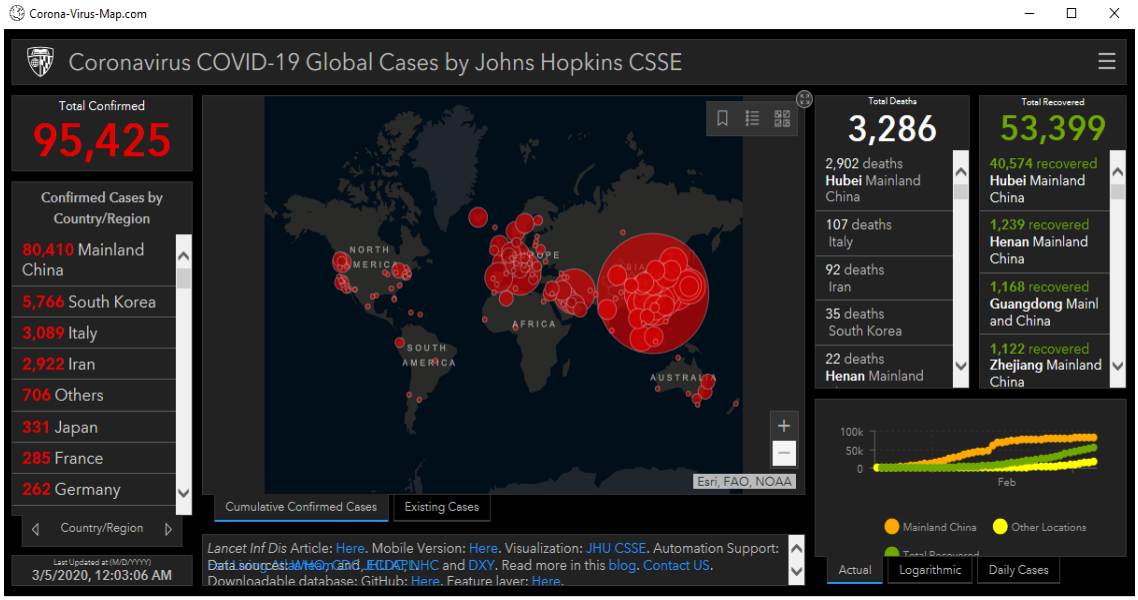
### *A „FormBook" malware a koronavírus köntösében*

A MalwareHunterTeam szakértői felfedtek egy kampányt, ami a COVID-19 kötelékében terjed. A támadók a WHO képviselőiként adják ki magukat, a kéretlen levélben egy .zip állományban van a FormBook elnevezésű információlopásra tervezett trójait letöltő futtatható program MyHealth.exe néven. Korábban kiberkémkedési céllal ezt a kártékony kódot alkalmazták már amerikai és dél-koreai célpontok ellen is. [172] A FireEye elemzése alapján a kártékony kód helyi jelszavakat, sütibeállításokat, vágólapon szereplő tartalmakat, valamint adatokat lop el http időszakokból. A kód továbbá képes parancsokat is végrehajtani egy távoli vezérlőszerverről (C2) többek között: letölteni és futtatni fájlokat, folyamatokat elindítani, leállítani és újraindítani a számítógépet. [173]

### *A COVID-19 terjedésével foglalkozó térkép weboldalának hamisítványa*

Egy grafikus felhasználói felület (Graphical User Interface) használatával a háttérben fut a rosszindulatú kód (malware) AZORult névvel fémjelezve. Ezt az információlopási technikát 2016-ban fedezték fel először, illegális orosz oldalakon közkedvelten árulták. Böngészési előzmények, bejelentkezési adatok, sütibeállítások és kriptovaluták lopására alkalmazták, valamint az ellopott adatokat további értékesítésre bocsátásának a lehetősége is adott. A kód többszintes összeállításban fut, multi-sub-process (azaz párhuzamosan és egymásra épülő, könyvtárrendszeri szinten) annak érdekében, hogy egy vizsgálat lefolytatását nehezebbé tegye. Annak érdekében, hogy a futása tartós legyen, a feladatütemezőt használja az operációs rendszerben. [174] A kártékony kódot tartalmazó GUI felület (6.ábra) az eredeti webes forrásból kapja az adatokat, így a gyanútlan szemlélőnek akár fel sem tűnik, hogy nem hivatalos helyről szerzi az információkat. Az

emberi természetet és a kíváncsiságra való hajlamosságot használja ki a támadó, altatva a célpont biztonságérzetét.




*6. ábra A Corona-Virus-Map.com grafikus felülete*

*Forrás: reasonsecurity.com*

### *Zsarolóvírus támadás egy cseh kórház ellen járvány közepén*

Helyi idő szerint reggel 5 óra körül kibertámadás érte a Brno-i Egyetemi Kórházat 2020 március 14.-én a járvány közép-európai terjedésének sűrűjében. A kórház kénytelen volt leállítani informatikai struktúráját az incidens alatt, valamint érintette két alszervezetét is. A központi hangosbemondóban fél óránként elhangzott, hogy minden dolgozó állítsa le a számítógépét kibernetikai biztonsági okokból. Reggel 8 óra magasságában pedig újabb üzenet került bemondásra a hangosbemondóban, mely szerint az aznapi összes orvosi beavatkozás szünetel. [175] Egy nappal később túlterheléses támadás érte az Egyesült Államok egészségügyi és szociális minisztériumát is, melynek során nem történt behatolás, illetve negatív fejlemény. A támadás, ami a HHS szervereit érte nem bizonyult eredményesnek, mert számottevő lassulást nem sikerült elérnie. [176]

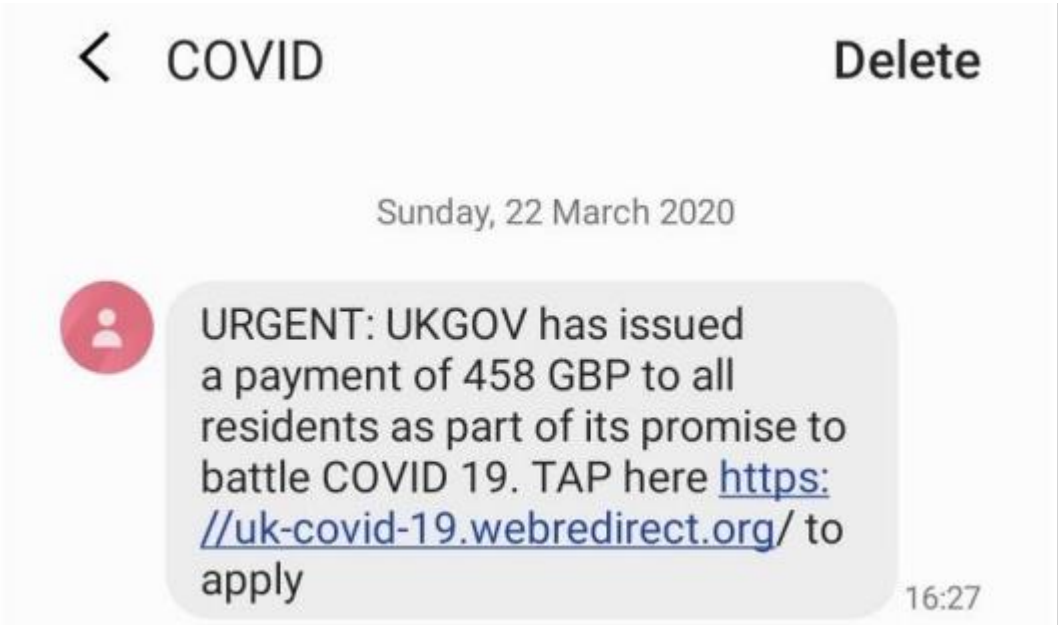
### *Iráni hátterű kibertámadások a WHO dolgozói ellen*

A Reuters 2020 márciusában megjelent közleménye alapján az ENSZ egészségügyi szervezetei és a hozzá kapcsolódó intézmények ellen elkövetett támadások megduplázódtak a COVID-19 járvány kezdete óta. A legutóbbi próbálkozás jelszavak ellopása volt a WHO dolgozóitól, előre elkészített emaileket küldve személyes emailpostafiókjaikra, melyekben álcázott Google webes szolgáltatásokkal igyekezték

megvezetni az áldozatokat. [177] A Foreign Policy 2020 áprilisi beszámolója szerint, a Covid-19 járványhelyzet miatt különösen fontos lenne, hogy globális szinten lévő fegyelmezettség legyen a kibertérben az egészségügyi szervezetek védelme érdekében. A lap továbbá beszámolt arról, hogy a világ végül kénytelen lépéseket tenni az egészségügyi infrastruktúra kiberbiztonsága végett. A fenyegetettség azonban nem újkeletű, 2017-ben egy New York állam béli, Buffaloban lévő kórház, az Erie County Medical Center ellen elkövetett zsarolóvírusos támadás során a ***NotPetya*** vírus használatával 10 millió USA dollár értékben követeltek Bitcoin kriptovalutát a támadók, a több, mint 6000 zárolás alatt álló számítógép feloldásáért cserébe. [178]

### *A National Cyber Security Centre tapasztalatai a COVID-19 kapcsán jelentkező kártékony szereplőkkel szemben*

Az Egyesült Királyság Kiberbiztonsági Központjának (NCSC) 2020 áprilisi kiadványában szerepel egy SMS-alapú adathalászati kísérlet (7. ábra), ahol a támadó az Egyesült Királyság kormányának adja ki magát, és egy hivatalosnak tűnő szöveg mellett egy külső weboldalra mutató linket küld az áldozat számára. A kiadvány a továbbiakban kitér arra is, hogy a támadók nem csak email alapon jelentkezhetnek, WhatsApp és egyéb chatalkalmazásokat is előszeretettel használnak.




*7. ábra COVID-19 témájú SMS-alapú adathalászat*

*Forrás: NSCS UK*

Jellemzően bejelentkezési adatok ellopására törekednek pénzügyi haszonszerzés céljával. További példaként megemlítenek egy ***phishing*** kampányt is 2020 március 19.-i kezdettel, ahol Dr. Tedros Adhanom Ghebreyesus feladótól a WHO főigazgatójának kiadva magukat az Agent Tesla nevű leütéskövető kémprogramot igyekeztek terjeszteni. Más kampányokban Excel fájlok is alkalmazásra kerültek, amelyek megnyitása után egy makró fut le, ami aktiválja a rosszindulatú kód letöltését, erre példa a 'EMR Letter.xls.' nevű állomány, amelybe egy beágyazott ***dinamikus csatolású könyvtár*** (DLL) telepíti a Get2 loader malware-t. Ez a kód pedig a GraceWire trójai programot telepíti a továbbiakban, ami a számítógép feletti irányítás átvételére hivatott. [179]

### *Adatszivárgási eset a Beaumontnál egészségügyi szolgáltatónál*

Az amerikai Michigan állam legnagyobb egészségügyi intézményében történt adatszivárgásról tett bejelentést 2020 április 17.-én a Beaumont Health Services, melynek során aktív és korábbi páciensek adatai kerültek illetéktelen kezekbe. A kikerült adatok természetét tekintve a páciensek neve, születési ideje, társadalombiztosítási azonosítója, egészségügyi állapotukra vonatkozó információ, valamint helyenként banki adatok, de még vezetői engedélyek adatai is kompromittálódtak. A kórház több, mint 1000 igazolt COVID-19 fertőzöttet kezelt ebben az időszakban. Ebben az évben ez a második eset, 2020 januárjában 1182 pácienst értesítettek, hogy egy munkavállaló jogosulatlan hozzáférése során kerültek ki adatok egy személyi sérülésekkel foglalkozó ügyvédi iroda számára. [180] A pénzügyi érdek (***financial gain***) ahogyan általában megfigyelhető az információlopás szándékával elkövetett kibertevékenységek során itt is jól tetten érhető, hogy a járványhelyzetet kihasználva a támadó könnyűszerrel ragadta meg a lehetőséget. Egy negyedéven belül két támadás egészségügyi adatok megszerzése céljával pedig intő jel a társadalom számára.

### 4.1.1 Államok és államcsoportok reagálása a világjárványra

A járványhelyzetre való reagálás az intézkedések tekintetében mind társadalmi, mind pedig kormányzati oldalon első ránézésre eltérő volt szerte a világon, néhány országot példaként említve az alábbiakban ismertetek. A területi adottságok, az adott ország lakossága, etnikai összetétele, a kulturális berendezkedés és a hatalomgyakorlás szerkezete csak néhány tényező, ami miatt nem is lehetséges egységes reakció a kialakult krízishelyzet kezelésére. Minden nép úgy oldja meg a krízishelyzeteit, ahogyan egyébként a mindennapi problémáival tenné.

*3. táblázat Pound-féle társadalmi érdekfaktorok vizsgálata*

| **Pound-féle társadalmi érdekek** | **Országkód (ISO[5])** | | | | | | |
|---|---|---|---|---|---|---|---|
| | EU | SE | AT | HU | US | CN | AU |
| 1. általános biztonság | 2 | 2 | 3 | 3 | 1 | 1 | 2 |
| 2. szociális intézmények biztonsága | 3 | 3 | 4 | 5 | 4 | 4 | 4 |
| 3. általános erkölcsök | 3 | 4 | 4 | 4 | 2 | 1 | 3 |
| 4. társadalmi erőforrások megőrzése | 4 | 4 | 3 | 3 | 4 | 1 | 3 |
| 5. általános előrehaladás | 3 | 3 | 4 | 5 | 5 | 5 | 2 |
| 6. az egyén életének védelme | 4 | 4 | 4 | 4 | 4 | 3 | 5 |

Jelmagyarázat

EU: Európai Unió

SE: Svédország

AT: Ausztria

HU: Magyarország

US: Egyesült Államok

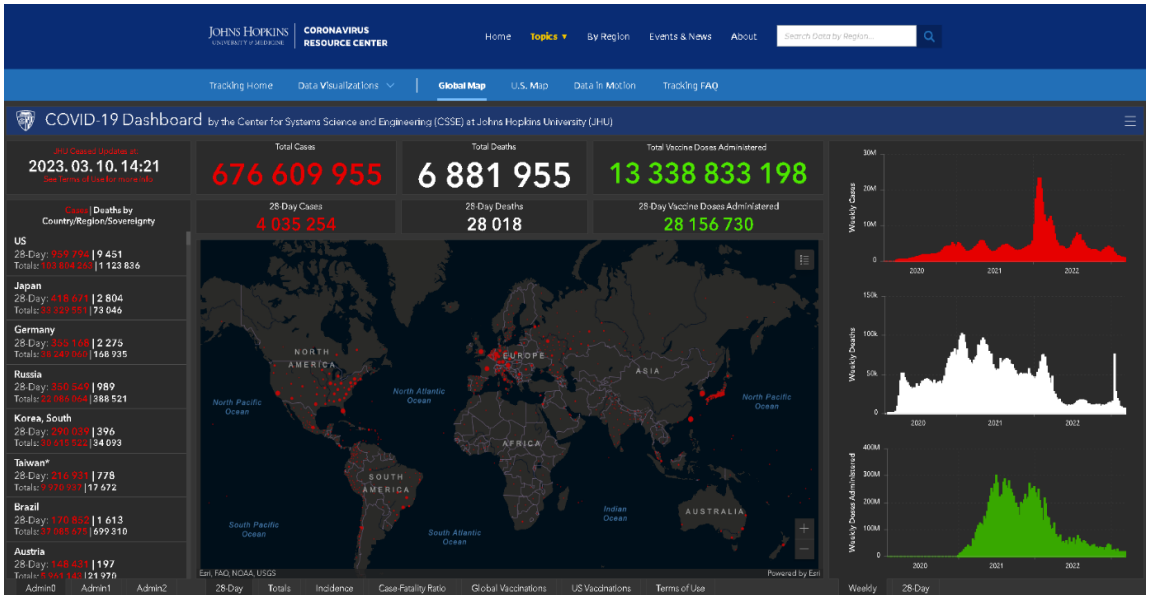
CN: Kína (Kínai Népköztársaság)

AU: Ausztrália

Skála értékek: 1 különösen szigorú - 5 különösen megengedő

[5] ISO 3166 alapján, az országkódok és alegységeik kódjaira vonatkozó nemzetközi szabvány

A Pound-féle társadalmi érdekek érvényesülését (3. táblázat) a 2020-as koronavírus világjárvány kezelésének tükrében elemzem. A krízishelyzet kezelése során világszerte voltak hasonló intézkedések, mindez köszönhető többek között annak is, hogy a közösségi médiában megjelenő társadalmi reakciókból informálódva (lényegében ezek megengedő megközelítéssel közvéleménykutatásoknak tekinthetők) az országok döntéshozói képesek voltak koordinált intézkedéseket meghozni, illetve hivatkozni egy-egy ország jó gyakorlatára. Erre volt hazai példa [181] amikor a magyar miniszterelnök a fertőzöttség szintjének mérlegelése során a szomszédos Ausztriát tekintette támpontnak.




*8. ábra SARS-CoV-2 (Covid-19) John Hopkins Egyetem térképe*

*Forrás: coronavirus.jhu.edu*

Pound társadalmi érdekszemléletében nyomon követhetjük, és azonosíthatjuk az elemeket: az **általános biztonság** iránti érdek a határok lezárásában és a mozgásszabadság korlátozásában mutatkozik meg; a **szociális intézmények biztonsága** iránti érdek az Egészségügyi Világszervezethez (WHO) a járvány korai hónapjaiban és a John Hopkins Egyetem megítélésével kapcsolatos viszonyban mutatkozik meg, amely a járvány kutatásában kezdett adatgyűjtésbe, melynek eredményeit weboldalán egy interaktív térképpel szemléltetett [182] és folyamatosan frissülő adatbázisa később világszerte széles körben lett alkalmazva (8. ábra); az **általános erkölcsök** iránti érdek a halálesetek emelkedésének és az orvoslási politikák (pl. betegellátás) elemzésében mérhető; a **társadalmi erőforrások megőrzése** iránti érdek nyilvánvaló a munkamódszerek változásainak értékelésében, természetessé vált a távmunka (home office) intézménye, mint lehetőség; az **általános előrehaladás** iránti érdek a gazdasági

növekedést helyreállítani igyekvő ellátási láncok összehangolásában és a járványhelyzet utáni időszakra kialakított pénzügyi alapok megszervezésében; az **egyén életének védelme** iránti érdek pedig megmutatkozik a fertőzöttek számának növekedését megakadályozó intézkedések (pl. védőtávolság tartása, vásárlási időszakok kialakítása, a közösségi rendezvények szervezése vonatkozó szabályok) kidolgozásában. Összességében megállapítható, hogy a különböző társadalmakban világszerte ugyanúgy vannak olyan tényezők, amelyek krízishelyzetben kifejezetten ösztönös megoldásokat követnek és kerülnek követelésre a lakosságtól.

### 4.1.2 A hegyi-karabahi másfél hónapos háború

Bár ennek a konfliktusnak az előzményei egészen 1991-ig nyúlnak vissza, a hidegháború utáni korszakban jelentős szerepe volt 2020-ban is. A NATO az év első negyedévében, 2020 március 27.-én Észak Macedónia személyében új, 30. tagjával bővült. [183] Ez az esemény katonai szempontból az egyik legrelevánsabb volt, a másik fejlemény az év második felében 2020. szeptember 27 és november 10. között zajló hegyi-karabahi háború volt. A konfliktus nem újkeletű, mert 1991-ben volt egy kiválási próbálkozás Azerbajdzsánból, ami katonai összetűzést eredményezett Hegyi-Karabah és Azerbajdzsán között. A nemzetközileg Azerbajdzsán számára elismert terület örmények által lakott, tehát a konfliktus természete etnikai. 2020 júliusában határvillongások kezdődtek meg Hegyi-Karabah és Örményország, illetve Azerbajdzsán között a területi kontrollért. Első körben szükségállapotot hirdetett Örményország, ami gyorsan eszkalálódott háborús állapottá. Végül a harcok november 10.-én Oroszország békefenntartói jelenlétével tűzszünettel zárultak, valamint Azerbajdzsán a háború alatt Hegyi-Karabahból elfoglalt területek feletti kontrollját megtartotta. 2020 júliusában azeri és örmény gyümölcsárusok között Moszkvában volt egy összezörrenés, ami „barackháború” címmel tett egy kört az interneten. [184] A növekvő ütemű nacionalista és ultranacionalista narratívák, valamint azok futótűz jellegű terjedése a közösségi médiában a szélsőséges szervezetek logikáját idézi. A fiatalok, akik jellemzően célkeresztjében vannak ezeknek az üzeneteknek, könnyen emészthető tartalmak révén, mint például mémek és rövid videókon keresztül vannak megszólítva olyan alkalmazások segítségével, mint a Twitter, Instagram, Tiktok és a Telegram. [185] A háború alatt a két ország kormányának üzenetei folyamatosan keringtek a közösségi oldalakon, erősítve a lakosság abbéli tudtatát, hogy a konfliktus szükséges és elkerülhetetlen. A lakosság oldaláról a kormányzatok pedig a háborúval kapcsolatos cselekmények támogatását

várták, amit hellyel közzel el is sikerült érniük. De mindez manipulatív eszközök nélkül alig lett volna kivitelezhető, mert alapesetben a lakosság nem szokott háborúpárti lenni. Erre példa egy azeri történész Facebook bejegyzése, aki annyit közölt csupán, hogy nem érdekli sem Zangezur, sem Jereván. Ez a rövid megjegyzés elég volt ahhoz, hogy az említett közösségi oldalon lejáratókampány[6] induljon ellene, ahol árulással vádolták. Egy Németországban elő újságíró, valamint a Musavat ellenzéki párt egy képviselője is hasonlóan járt. A bejegyzések a „#Khainitaniaq" kifejezéssel lettek ellátva, ami annyit jelent magyarul „tudd, hogy ki az áruló." [186] Tehát a kormányzati kontroll jelenléte a kommunikációs térben jól látható, a narratíva kontrollálása pedig fontos tényező volt a harcok legitimálása szempontjából. A modern kor háborúiban már kevésbé látszik az éles határvonal a frontvonal és a hátország között. Bár a harci cselekmények a fizikai térben távol vannak egymástól, a virtuális térben ezek mégis a kezünkben vannak (nevezhetjük karnyújtásra is) az okostelefonok révén. Bár ekkor még nem okostelefon címkével, de 2011-ben a Foreign Policy közölt egy bejegyzést, ahol a Nokia 1100-at az AK-47-essel hozta párhuzamba. [187] A közösségi média lehetővé teszi az egyének számára, hogy a propagandát felforgató módon irányítsák az információkat. Az emberek felfedezhetik, milyen közlekedési torlódások vannak a közelben és elkerülhetnek egy balesetet. A mobiltelefonok lehetővé teszik, hogy valaki egy idegen nyelven lévő szöveget lefordítson, majd hatékony orvosi ellátásban részesüljön. A társadalomnak lehetősége van az intézményes igazgatás elszámoltatásában, főleg oly módon, hogy kifejezetten kényes információkat tesznek közzé korrupcióról, igazságtalanságról vagy erkölcstelen cselekedetről. [188] Az egyén szerepe a kommunikációban átértékelődött. Az újságírás valódisága, az objektivitás, a tények és azok hitelessége manapság nem maguktól értendő kategóriák. Egy olyan információs térben, ami napjainkat jellemzi, a manipuláció és a befolyási kísérletek száma a végtelenhez közelít. Pulitzer József híres szállóigéje, miszerint „a hír szent, a vélemény szabad" már egyre kevésbé állja meg a helyét, mert az álhíreknek erősebb szárnya van. A videó és képkészítés egyszerűsége, illetve azoknak a könnyű továbbíthatósága katalizálja azt a folyamatot, ami a dezinformációs kampányok hatékonyságát adja.

[6] A lejáratókampány vagy zsarolás (angolul blackmailing) a pszichológiai manipuláció (angolul social engineering) egyik klasszikus eszköze, ahol a célpont hiteltelenítése a cél a kommunikációs térben

### 4.1.3 A 2020-as amerikai elnökválasztás körülményei

Ez az év számos tekintetben kiemelkedik történelmi jelentőségben, ugyanis világszerte tombolt a COVID-19, valamint az Egyesült Államokban egy olyan elnökválasztásra került sor, ahol a járványügyi korlátozások okozta társadalmi közeg és hangulat jelentős befolyást gyakorolt mind a kampányidőszak alatti kommunikációra, illetve a kialakult eredményekre is. A médiában a politikai riválisok sok esetben egymásnak teljes mértékben ellentmondó üzeneteket közvetítettek, valamint igyekeztek a közvélemény politikai vízióik mentén terelni a speciális körülmények között. Az információszerzést, a lakosság tájékozottságát illetően a közösségi média platformok, kiemelten a Twitter és a Facebook lényegében határozták meg a társadalmi diskurzus alakulását. Mivel a személyes találkozások lehetősége korlátozott, vagy kivitelezhetetlennek bizonyultak, szükségszerűen a fókusz a kibertérbe került. A járványügyi adatok napi szintű nyomon követése természetes beállítás volt ebben a bizonytalan időszakban, a világ többségében a John Hopkins Egyetem által készített adatbázisra támaszkodott. Az Egyesült Államokban volt a legtöbb tesztelés, fertőzött beteg és halálos áldozat hosszú időn át az első hullámokban.

A 2020-as amerikai elnökválasztás kapcsán is, de az elmúlt években szintén időről-időre előtérbe kerül a közösségi média és annak szerepe a társadalmi-gazdasági-politikai folyamatokra való hatásuk vizsgálatakor. A WeAreSocial és a Hootsuite által közösen készített DIGITAL 2020: JULY GLOBAL STATSHOT című jelentés [189] számadatokkal reprezentálja azt a jelenséget, amelyekkel kapcsolatban csak találgatni szokott az olvasóközönség. Ma már több, mint a Föld teljes populációjának fele (51%) használ valamilyen közösségi médiához köthető alkalmazást, a másik érdekesség pedig, hogy ez 99%-os arányban mobileszközökhöz kötődnek. A mobiltelefonnal rendelkezők penetrációja elérte a kétharmadot (66%) a teljes népesség körében. Nem meglepő tehát a trendek alakulása szempontjából, hogy a számok tükrében hogyan alakulnak a megoszlások a teljes populáció-internethozzáféréssel rendelkezők-közösségi média felhasználók hármasában. Az aktív felhasználók számának megoszlása viszonylag jól meghatározza a piaci súlyokat és az erőközpontokat is, azonban az egy-egy termékhez kapcsolódó felhasználókat fontos az anyaszervezetekkel való függőségi viszony figyelembevételével kezelni. Átfedések a szokások tekintetében vannak és ezek egyfajta árukapcsolási jelenségnek tudhatók be, például a Facebook és a YouTube egyidejű használatának irányába erősen elhajlanak az adatok, amelyek a tájékozódási pontokat jól

szemléltetik. Ezeknek a vállalatoknak a közösségi terekben felelőssége és jogállása bár a mai napig számos országban kérdéses világszerte, szabályozása az Egyesült Államokban idén a 47 U.S.C. § 230 módosításával megtörtént, amely alapesetben eddig felmentette a szolgáltatót a harmadik felek által közölt tartalmak hitelességének ellenőrzése szempontjából, viszont a 2020. május 28.-án hatályba lépett kormányrendelet [110] alapján, automatikusan nem hivatkozhat a korábbi időszakot meghatározó jogi védelemre. Név szerint is megnevezi azokat a közösségi média szolgáltatókat, akik ebben jelentősen érintettek, továbbá arra is kitér, hogy a közösségi terekben ezeknek a szolgáltatóknak az alkotmányban foglalt alapjogoknak eleget kell tenniük, ezért egyoldalú korlátozásokat a tartalmak megosztásának, törlésével, elfedésével, eltűntetésével stb. kapcsolatban nem alkalmazhatnak, mert számottevő társadalmi hatásokat fejthetnek ki ezekkel az intézkedésekkel. Ez az intézkedés 2021. május 14.-én visszavonásra került.

A kampánygyűlések során a közösségi médiában a választásokról és a szavazatszámlálásról szóló közvetítések és egyéb reakciók során több sztori is szárnyra kapott és körbejárta az internetet ebben az időszakban. Sok úgynevezett „tényellenőrző” (***fact-check***) weboldal még a tömegtájékoztatási (***mainstream***) média esetében is, pl. Reuters jelent meg nevezetesen a Facebookon, amik elkezdték cenzúrázni a szerintük hamis információkat tartalmazó tartalmakat. A fenti közösségi médiával kapcsolatos jelentés alapján is elmondható, hogy ezek a folyamatok a közeljövőben egyre láthatóbbak és gyakoribbak lesznek, hiszen a növekvő felhasználószám függvényében nem csak a véleményvezérek (***influencer***), hirdetők és egyéb szereplők számára bővül a piac, de a kibertérben csalási szándékkal rendelkezőknek is. A kockázatérzékeny megközelítés az egyik leghatékonyabb védekezési módszer az átverések kiszűrésére, viszont a történelem során az eszközök fejlődtek leginkább, mintsem azok a tényezők (átverési ötletek), amelyek a csalásokat működőképessé teszik. [166]

## 4.2 A visszarázódás első éve, a posztcovid időszak

Az évet több jelentős esemény mozgatta köztük: a SARS-CoV-2 (Covid-19) koronavírus világjárvány elleni küzdelem folytatása, az év elején a „Capitolium ostromának" nevezett zavargások, a nyugati erők kivonulása Afganisztánból, a kelet-közép európai „mesterséges menekültválság" és Angela Merkel német kancellár távozása négy ciklusos ideje után. [190] A koronavírus járvány második nagyobb időszakát a vakcinakampányok és azokkal kapcsolatos intézkedések jellemezték, világszerte különféle megoldási módszerekkel. Ami Európát érintette, ott jól megfigyelhető volt a katonai szövetségek mentén történő szabályozási gyakorlat, NATO-n kívüli országok, mint például az orosz Szputnyik vagy a kínai Sinopharm vakcina engedélyezésével és jóváhagyásával akadtak problémák, amiket jellemzően inkább politikai megfontolások eredményeztek mintsem szakmai érvek.

### 4.2.1 Az afganisztáni kivonulás

2000 és 2021 között az afganisztáni internethozzáférés 0 százalékról 22 százalékra emelkedett a teljes népességet tekintve. Szakértői becslések alapján az afgánok 70 százalékának van hozzáférése mobileszközökhöz és 11,2 százalékuk pedig jelen van valamilyen közösségi média platformon. Kabul elfoglalása utáni időszak szempontjából számottevően nőtt mind a Tálibok jelenléte közösségi médiában, valamint annak jelentősége is, amellyel hatalmukat igyekeznek legitimálni. A hatalomátvételt követő időszakban például a Twitteren keresztül oszlatták a kételyeket várható politikájukkal kapcsolatban. [191] A világ közvéleménye számára az emberi jogokkal kapcsolatos aggályok a Talibán hitelessége szempontjából nézve meghatározó kérdés volt, az ország új vezetése ezért lépéseket tett annak irányába, hogy a kor szempontjából kézenfekvő módon népszerűsítse álláspontját. Interjúk készültek Talibán vezetőkkel, hogy reagáljanak az interneten keringő aggodalmakra, valamint elképzeléseiket osszák meg Afganisztánnal kapcsolatos jövőbeli terveikkel kapcsolatban. Nagy figyelmet kapott a közösségi térben a kivonulás a nyugati erők részéről is, példaként említve az Egyesült Államokat, az amerikai Védelmi Minisztérium Twitter-bejegyzésben is tájékoztatta a nyilvánosságot az utolsó katona kivonulásáról és a küldetés befejezéséről Kabulban. [192] Az év elején Donald Trump amerikai elnök által aláírt kivonulási megállapodás az Egyesült Államok történetében példátlan légi szállítási műveletet jelentett. Az országban lévő katonai, diplomáciai és civil szakemberek, valamint a hatalomátvétel

következményeitől tartó személyek evakuálása komoly logisztikai tervezést követelt meg. Magyar érintettségben az akció fedőneve *Sámán hadművelet* volt, amely során a Magyar Honvédség 540 embert menekített ki Afganisztánból, közöttük magyar, osztrák, amerikai és afgán állampolgárokat Az akció során 14 alkalommal tették meg a MH gépei az Afganisztán-Üzbegisztán utat, ahol utóbbi helyen a Wizzair és az üzbég nemzeti légitársaság civil utasszállító gépei várták az utasokat egy magyar-üzbég megállapodás alapján. A különleges műveleti katonákat szállító két Airbus A319 típusú többcélú közepes csapatszállító repülőgép augusztus 25.-én késő este érkezett meg hazánkba. [193] A kivonulás eseményeihez még egy öngyilkos bombamerénylő támadása is tartozik, ami augusztus 26.-án történt a Kabuli nemzetközi repülőtér Abbey Gate ellenőrzőpontjánál. A támadás következményében 13 amerikai tengerészgyalogos katona veszítette életét, valamint legalább 170 afgán civil szerepelt az áldozatok között. Az elkövető az Iszlám Állam – Khorasan tartomány fegyveres csoport (ISIS-K) tagja volt. A bombából származó 5 milliméter átmérőjű csapágyakat a megközelítőleg 9 kilogramm tömegű, katonai minősítésű robbanóanyag továbbította a robbantás környezetében, a detonáció egy tűzharc illúzióját keltette, a katonák figyelmeztető lövéseket adtak le a tömeg oszlatásának szándékával a kialakult kaotikus helyzet következtében. [194] A szélsőséges szervezetek az ilyen típusú akciók révén kialakult kiemelt figyelmet a közösségi médiában nemcsak a tevékenységük reflektorfénybe állításával tudják hatékonyan kamatoztatni, hanem a hívekkel való kommunikációjuk során is. Erre példa az Al-Andalus Media (az al-Kaida Maghreb régióbeli testvérszervezetének médiája) ugyancsak Twitter használata. 2013 márciusában az al-Kaida anyaszervezet hirdetést tett közzé az afrikai „leányvállalatának" médiacsoportjának képviseletében, ami később dzsihadista fórumokon is megjelent az interneten. [195] Lehetőség, hozzáférés, meggyőzés. Ezekkel a jelzőkkel illeti az Egyesült Államok Igazságügyi Minisztériumának kutatóintézete (National Institute of Justice) az al-Káida által inspirált terrorizmus közösségi médiában betöltött szerepét. Maga a közösségi média, mint közvetítő eszköz relevanciája abban is megmutatkozik, hogy a régi és az új életforma közötti szakadékot hogyan képes áthidalni. Fiatal férfiak és nők oly módon csatlakoztak az Iszlám Államhoz, hogy a migrációs lánckialakítás logikája alapján követték eredeti lakhelyük környezetében lévők nyomdokait, keresve a család és barátok, valamint az újonnan szerzett ismerősök társaságát. Csupán a szélsőséges tartalmak követése az online térben nem elegendő egy életet meghatározó döntést meghozni, a csoportszellem erősítését célzó tevékenységek viszont kellő löketet adhatnak ahhoz, hogy kívánatos cselekménnyé váljon a

terrorszervezethez való csatlakozás szándéka az egyén számára. [196] [141] Az Egyesült Államok kivonulása Afganisztánból fordulópontot jelentett a közösségi média használatában és kezelésében. A tálibok sikerét nagyban befolyásolta a Twitter-profilok használata, amely a csatatéren elért sikerek gyors és hatékony közvetítésével valósult meg, ezzel is elősegítve a kormányerők védelmének és moráljának megtörését, ami jelentős ellenállás csökkentést eredményezett. [197] A tálibok által elindított pszichológiai hadművelet megadásra késztette az ANSF-et, ahol amnesztiát, pénzt ajánlottak nekik, néhány esetben pedig megfenyegették a családjukat, amennyiben nem hajlandók együttműködni. Ezek a tényezők nagy szerepet játszottak Kabul későbbi, 2021 augusztusában történő átvételében. A közösségi médiában az Egyesült Államok kormányának a kiürítéssel kapcsolatos kommunikációja is releváns volt, leginkább a Twitteren.


*9. ábra 2021-es kabuli légiszállítás*

*Forrás: U.S. Naval Institute*

Emlékezetes pillanat volt  az amerikai légierő gépei előtt futó tömeg (9. ábra), a kabuli reptér elhagyása során. [198] Az afgán kormány hirtelen összeomlása kétségbeesett kísérletekhez vezetett az online segélyezési és evakuálási erőfeszítések felgyorsítására. Nagyrészt a Google Forms, a WhatsApp és a privát közösségimédia-csoportok által szervezett erőfeszítések révén próbálták meg betölteni azt az űrt, amelyet az Egyesült Államok kormányának a sebezhető afgánok védelmének kudarca okozott. Sokaknak ez lehetett az egyetlen mentőöv, akik megpróbáltak elmenekülni az országból, ami nem volt mentes a veszélyektől, mivel a megfigyelők attól tartottak, hogy a tömegből leszűrt információkat a tálibok felhasználhatták a mentésre szorulók azonosítására. [199]

### 4.2.2 Ukrajna, Finnország és Svédország NATO csatlakozási kérdései

A Szovjetunió 1990-91 utáni szétesését követően három magállam Oroszország, Ukrajna és Fehéroroszország viszonya a továbbiakban is összefűződött. A kiindulópont, hogy Ukrajna hátrányban volt az európai országokkal (posztszovjet utódállamokkal) szemben a gázárral kapcsolatos kérdésekben, miközben ők 80 dollárt fizettek 1000 köbméterért, az európai országok 60 és 70 között fizettek, ami elkerülhetetlenül összetűzéshez vezetett Oroszországgal. Ukrajna képes volt megcsapolni a gázt a vezetékből, késleltetve a szállításokat, felhalmozta a készleteket, csökkentve Moszkva nyomásgyakorlását energiaproblémákkal kapcsolatban, miközben saját alkupozíciót alakított ki az árakon. [200] Ukrajna 1994. február 8. óta tagja a Partnerség a békéért (PfP) programnak, két év múlva 1996-ban lengyel közreműködéssel létrehozott kötelékben vett részt békefenntartó műveletekben ukrán zászlóalj. 1997-ben Ukrajna nyugati részén 10 napos hadgyakorlatot tartottak, amerikai, görög, román, moldvai, cseh és szlovák részvétellel, ahol megjelent a NATO dél-európai parancsnoksága is. [201]

***Ukrajna gáztárgyalásai Európával***

A Naftogaz ukrán állami energiacég szóvivője szerint 2006 januárjában volt egy időszak, amikor Ukrajna kénytelen volt több európai ország gázimportját blokkolni a különösen hideg időjárás miatt. [202] 18 országot érintett a gázáramlás leállása a nagy EU-tagországoktól kezdve, mint például Németország olyan kis nemzetig bezárólag, mint Moldova. [203] Akkoriban Magyarország, Románia és Lengyelország arról számolt be, hogy csökkent a nyomás szintje vezetékeikben. Az EU ellenőröket küldött Ukrajnába, hogy biztosítsák Oroszországot, hogy Ukrajna nem szippantja ki a gázt a vezetékből. Cserébe Oroszország ígéretet tett arra, hogy a megfigyelés megkezdésekor visszafordítja az áramlást. [204] Ezt követően Európa más alternatívákat kezdett keresni, nem csak helyettesítő partnereket, hanem más energiaforrásokat is, például megújuló és nukleáris energiaforrásokat. [205, pp. 77-78] Az Északi Áramlat-1 megépítéséig az Ukrajnán keresztül Európába továbbított orosz gázexport 80 százalék körül mozgott, ami az új vezeték miatt 50-60 százalékra esett vissza. A földgáz áramlása a téli időszakban körülbelül 12 milliárd köbláb, nyáron pedig 6 milliárd köbláb. [206] Az energiaügyek bizonytalansága időről időre felmerülő probléma volt és annak számít ma is az európai országokban. A pénzpiaci válságig fontos ütőkártyaként lehetett használni Ukrajna számára, hogy nyomást gyakoroljon külpolitikájának érvényesítése során. A felek közötti nézeteltérések politikai természetűek voltak, erre volt példa a Viktor Juscsenko vezette

NATO- és EU-barát kormány, akinek a nevéhez a „Narancsos Forradalom” is fűződik, riválisa pedig a Kreml-barát Viktor Janukovics volt, aki elutasította az EU folyamatban lévő közeledési politikájának előrehaladását, megpróbálva ezzel eltávolodni Európától és szorosabbra fűzni a viszonyokat Moszkvával. Zavaros életutak és korrupciós botrányok jellemezték akkori Ukrajna politikai életét. Ez részben annak volt köszönhető, hogy a Szovjetunió összeomlása után Oroszország nem mondott le az érdekszférájába tartozó területek feletti befolyásról. A politikában a vákuum ismeretlen fogalom. Ez volt az egyik oka annak a bizonytalan helyzetnek, ami végül a „Euromaidan”-tüntetésekhez vezetett, ahol a tüntetők összecsaptak a rendőrséggel a Függetlenség terén (Majdan Nezalezsnosztyi). [207] Néhány hét leforgása alatt ezek a megmozdulások forradalomba fordultak, ahol Janukovics legitimitása kérdőjeleződött meg aki végül elmenekült az országból. A kialakult helyzet a Krím 2014-es annektálásával zárult le. Az Orosz Föderáció elleni első EU-szankciók 2014. március 17-én léptek életbe. Azóta elkerülhetetlenül körvonalazódott egy Ukrajna és Oroszország közötti fegyveres konfliktus lehetősége. [147] [208]

Ukrajna NATO-tagsági törekvéseire a szövetségesek a 2008-as bukaresti csúcstalálkozón megállapodtak abban, hogy Ukrajna a NATO tagja lesz. Abban is egyetértettek, hogy Ukrajna következő lépése a tagság felé vezető úton a Tagsági Akcióterv (MAP), a NATO politikai, gazdasági, védelmi, erőforrás-, biztonsági és jogi reformprogramja volt a tagjelölt országok számára. 2009-ben az éves nemzeti programot Ukrajna kulcsfontosságú eszközeként vezették be euroatlanti integrációja és a kapcsolódó reformok előmozdítása érdekében. 2010 és 2014 között Ukrajna elállási politikát folytatott, amelyet Oroszország agressziójára válaszul felmondott. 2017 júniusában az ukrán parlament olyan jogszabályt fogadott el, amely stratégiai kül- és biztonságpolitikai célkitűzésként visszaállítja a NATO-tagságot. 2019-ben hatályba lépett az ukrán alkotmány megfelelő módosítása. 2020 szeptemberében Volodimir Zelenszkij elnök jóváhagyta Ukrajna új nemzetbiztonsági stratégiáját, amely a NATO-tagság érdekében a NATO-val való jellegzetes partnerség kialakítását írja elő. 2022 szeptemberében, miután Oroszország illegális annektálási kísérletet tett Ukrajna területén, Ukrajna megismételte NATO-tagság iránti kérelmét. A 2023-as vilniusi csúcstalálkozón a szövetségesek megerősítették azon elkötelezettségüket, hogy Ukrajna a NATO tagja lesz. Felismerve Ukrajna megnövekedett interoperabilitását és jelentős előrehaladását a reformok terén, úgy döntöttek, hogy Ukrajna útja a teljes euro-atlanti integráció felé már túllépett a

tagsági cselekvési terv szükségességén. A szövetségesek továbbra is támogatják és felülvizsgálják Ukrajna előrehaladását az interoperabilitás terén, valamint a demokratikus és biztonsági szektor további reformjait, amelyekre a jövőbeni tagság felé vezető úton van szükség. A NATO külügyminiszterei rendszeresen értékelni fogják az előrehaladást a módosított éves nemzeti programon keresztül; valamint fenntartja a lehetőséget, hogy meghívja Ukrajnát a Szövetségbe, amennyiben az egyhangú beleegyezés és a tagság feltételei teljesülnek. [209]

### *A finn és svéd NATO csatlakozás*

2022 májusában Finnország és Svédország vezetői megerősítették csatlakozási szándékukat a NATO-hoz, ami egy történelmi északi politikai váltást jelent, amelyet Oroszország Ukrajna elleni inváziója váltott ki, és amely átrajzolja Európa biztonsági térképét. A több évtizedes katonai elállástól felhagyva a két ország kormánya hétfőn terjeszti elő javaslatait saját parlamentje előtt, és várhatóan hivatalosan is benyújtja közös tagsági kérelmét a 30 tagú szövetséghez, amint a döntéseket ratifikálják. A finn elnök Sauli Niinistö kijelentette, hogy a döntés történelmi nap az északi ország számára, a miniszterelnök Sanna Marin, pedig reményét fejezte ki, hogy a parlament mihamarabb megszavazza a csatlakozást. [210] Finnország 2023. április 4.-én a NATO 31. teljes jogú tagjává vált. [211] Svédország csatlakozási folyamata valamivel hosszabb volt, mivel Törökország és Magyarország ellenvetésekkel élt. Törökország biztonsági garanciákat kapott a svéd alkotmánymódosítással, Svédország a PKK-val (Kurdisztáni Munkáspárt) szembeni fellépéssel kapcsolatos együttműködését bővítette, amely a terrorizmus elleni harcban játszik fontos szerepet, valamint folytatja fegyverexportját Törökországba. [212] Elemzők szerint pusztán politikai hatalmi játszmáról volt szó, hiszen korábban a török elnök Recep Tayyip Erdogan még az Európai Unióhoz való csatlakozáshoz kötötte a svéd NATO csatlakozási kérelem jóváhagyását. A háttérben nem hivatalos közlemények alapján F-16-os vadászrepülőgépek és egyéb katonai eszközök eladását szorgalmazó tárgyalásokat sejtenek Törökországgal. [213] Magyarország vonatkozásában is hasonló politikai játszma volt napirenden, méghozzá a JAS Gripen vadászgépekkel kapcsolatos bérleti szerződések megújítása és bővítése kapcsán. Orbán Viktor miniszterelnök az X-en (korábban Twitter) jelentette be [214], hogy levelet küldött Ulf Kristersson svéd miniszterelnöknek. Amit Törökország az Egyesült Államokkal szembeni pozíciójában használt ki, azt Magyarország a svédekkel szemben érvényesítette. [215] Svédország 2024. március 7.-én a NATO 32. teljes jogú tagjává vált. [216]

## 4.3 Az Orosz-Ukrán háború és következményei

Módszertanilag az esettanulmányok lezárt időszakok vizsgálatát követelik meg, így ennek a fejezetnek az idősíkja a háború kitörésének évétől kezdve a Fekete-tengeri gabonaegyezménnyel bezárólag 2023 júliusáig terjed.

2022. február 24-e után a világ ismét döntéshelyzet előtt állt. A látszólag befagyott konfliktus főszerepet kapott a világ diskurzusában az orosz-ukrán háború, ami számos szunnyadó folyamatot is indukált. Próbára tette a nemzetközi megállapodásokat, katonai szövetségeket, kereskedelmi tömböket, példaként említve az ENSZ Közgyűlését, ahol szövetségesi és diplomáciai kapcsolatok jól látszottak a heves viták során. Hasonló ellátási lánc problémák jelentkeztek, mint a járvány idején, de a háborús retorika és események miatt sokkal nagyobb hatékonysággal működtek. Infláció, gazdasági teljesítmény csökkenés, bizonytalan élelmiszerellátás és energiaválság érkezett Európába, magasabb fokozatba kapcsolt az érdekeltek közötti fegyverkezési verseny. Három nappal később a háború kitörése után Olaf Scholz német kancellár 100 milliárd eurós védelmi alapot jelentett be. [217] 2022 márciusában jelentették be a RePowerEU tervet [218], amelyben az EU célul tűzte ki a földalatti gáztároló kapacitások 90%-os feltöltését, valamint szisztematikus tervet az orosz fosszilis energiahordozók felhasználásának a földgázzal kezdődően az Ukrajna elleni inváziót reagálva. Ezeknek a döntéseknek azonban van egy érdekes előzménye, hiszen 2016 óta létezik az LNG-kereskedelem az EU és az USA között, és 2021-ben már a legnagyobb tételt, 22 milliárd köbméter cseppfolyósított gázt importálta. [219] Az európai vezetők több álláspontot foglaltak el a háború első évének diskurzusában, nemzetállamok léptek fel az energiafüggőség szemszögéből. Az év későbbi szakaszában az Északi Áramlat szabotázs-incidense megoldatlan maradt, máig nem világos, hogy valójában kik vettek részt egy ilyen akcióban, a médiateret azonban elárasztották a lehetséges elkövetőkről szóló elméletek.

### 4.3.1 Az Északi Áramlat elleni szabotázsakció

A gázvezetékek elleni támadások körüli titokzatosságra a hibrid hadviselés jellemvonása adhat magyarázatot. *„A szinkronizálás következtében a támadások (különösen a kezdeti szakaszban) jó eséllyel a felderítési és a reakcióküszöb alatt maradnak.”* [136] 2022. szeptember 26.-án az Északi Áramlat-1 két vezetékét, az Északi Áramlat-2 egy vezetékét érte robbantásból származó találat, melynek következtében a vezetékben lévő gáz a Balti-

tengerbe kezdett szivárogni. Az eseményre a környező országok hatóságai a nyomáscsökkenés következtében figyeltek fel, majd a helyszínre érkezve a légifelvételeken rögzített információk nemsokkal utána jelentek meg mind a tradicionális, mind a közösségi médiában. Az elkövetők személyével kapcsolatosan már a kezdetekben voltak találgatások, azonban hivatalos közlemény annak azonosításában nem került publikálásra. A történet sajátossága, hogy az orosz-ukrán háború következtében amúgy is puskaporos hangulat további bizalomvesztést és kételkedést hozott a konfliktusban direkt és indirekt módon résztvevő szövetségi rendszerek között. Egy lengyel EP-képviselő Radosław Sikorski Twitter-bejegyzésben oldalán a következő megjegyzést tette: „Thank you, USA!" ami további spekulációkra adott alapot. Ez a megjegyzés természetesen felkeltette az oroszok figyelmét is, az Orosz Külügyminisztérium szóvivője Mariia Zakharova Telegram-csatornáján kommentálta a bejegyzést, melyben egy „hivatalos nyilatkozatot feltételezett egy terrorcselekmény elismerésével kapcsolatban" [220] A Kreml szóvivője, Dmitry Peskov szerint azok a jelentések, amelyek egy ukrán támogatást feltételező csoportot sejtenek az Északi-Áramlat elleni támadás mögött egyértelmű félretájékoztatási kampányról részét képezik. Ukrajna tagadta, hogy bármilyen szerepet töltött volna be a szabotázsban. [221] Az Oroszországi Föderáció ENSZ képviselője indítványt nyújtott be, aminél egy nemzetközi, független vizsgálatot kért a bizottságtól a csővezetékek elleni akciót érintően. A szavazás három támogató (Brazília, Kína, Oroszország) és tizenkét tartózkodó szavazat (a három ország kivételével más nem vett részt a szavazáson), valamint elutasító szavazat hiánya mellett a Biztonsági Tanács a résztvevők létszámának elégtelen mivoltából fakadóan elutasította a vizsgálóbizottság felállítását. [222] A találgatásokat tekintve több forgatókönyv felmerült az elkövető kilétével kapcsolatban, azonban több forrás szerint is az esemény volumenét tekintve az állami szereplő (angolul state-level actor) általi kivitelezés a valószínűbb.

### 4.3.2 Minősített iratok kiszivárgása a Pentagonból

A Discord egy ingyenes, VoIP (Voice over Internet Protocol) alkalmazás, ami magyar fordításban internetprotokollon keresztüli hangátvitelt jelent. Lényegében egy olyan távközlési forma, ahol telefonhálózat helyett az internet szolgál közvetítő csatornaként. Bár helyenként közösségi média felületként hivatkoznak rá, a klasszikus értelemben vett hírfolyam, valamint a decentralizált jellege miatt nem sorolható egyértelműen a közösségi média kategóriába. Eredetileg az alkalmazás videójáték-közösségek számára lett

tervezve, mint kiegészítő kommunikációs eszköz, azonban az évek során az érintettek köre folyamatosan bővült. Felépítését tekintve a szerkezeti szintek a szerverek, csatornák, közvetlen üzenetek és a felhasználói profilokra bonthatók le. Az alkalmazáson keresztül a főbb funkciókat kiemelve, lehetőség van szöveges, kép-, videó-, valamint audió kommunikációra. Korábbi hasonló alkalmazásokkal szemben, mint a Teamspeak újdonsága a felületnek, hogy ingyenesen létrehozhatók szerverek, valamint szöveges- és hangcsatornák alakíthatók ki. A felhasználók számára szerepkörök határozhatók meg, a csatornák közötti barangolások és interakciók jogosultságok kialakításával korlátozhatók. Az utóbbi években megjelentek számítógépes „botok" is, amelyekkel parancsok segítségével kommunikálhatunk, játszhatunk le zenét vagy videót akár a Youtube-ról, amit a felhasználók közösen nézhetnek együtt.

2023 márciusában kerültek ki dokumentumok részletei egy Discord szerven keresztül, minősített katonai információk szerepeltek. A kiszivárogtatott információk megerősítették azt a feltételezést, amit a hírszerzési szakértők régóta sejtettek, hogy az Egyesült Államok jobban tisztában van Oroszország stratégiai helyzetével, mint az ukrán vezetés. A dokumentumok között, amik az online térben megjelentek szerepelt olyan is, ami felvázolta a helyzetét az orosz-ukrán konfliktusnak, beleértve csapatmozgásokat meghatározott dátummal. Ami pedig további diplomáciai problémákat szült, hogy nem csupán ellenfelei, hanem szövetségeseivel szemben is így jár el (Angela Merkel lehallgatási botránya [223] is hasonló eset volt) kémkedési tevékenységet folytat. [224] A 21 éves Jack Teixeira a Massachusettsi Air National Guard (az Egyesült Államok Légi Erejének föderális tartalékos szervezete) tagja hivatalosan is vád alá lett helyezve minősített dokumentumok és nemzetbiztonsági információk kiszivárogtatásáért a szövetségi bíróság által Bostonban. [225] Az eset sajátossága, hogy olyan biztonsági résre derült fény, amivel korábban az érintett szervezetek akár a Pentagon is, valószínűleg kevésbé számoltak. Nem az első alkalom viszont, hogy a platform látszólag anonim jellegét tekintve olyan tevékenységek támogatására volt használva, amiket alapvető esetben más mérlegelési szempontok követtek volna és feltételezhetően nem is ez volt az utolsó eset. A jelenlegi feszült geopolitikai helyzet következtében, valamint az információs hadviselés eszköztárát tekintve a helyzetértékelés továbbra is kétséges, ugyanis több lehetséges forgatókönyv is adott.

***Kibertámadás az OTP netbankja ellen***

Az OTP Bank külföldről érkező túlterheléses támadásnak (DDoS) lett a célpontja, ami miatt leállt az új internet- és mobilbankja, valamint a honlapja sem volt elérhető rövid ideig. A pénzintézet közölte, hogy a szakemberek sikeresen elhárították a támadást, és a rendszerek megfelelően működnek. [226] A tárcavezető az európai uniós külügyminiszterek informális tanácsülésének szünetében hangsúlyozta, felháborító, hogy miközben Magyarország részt vesz abban a programban, amelynek keretében a blokk havonta másfél milliárd euróval támogatja Ukrajna működését, az ukrán nemzeti korrupciómegelőzési ügynökség nemrég „a nemzetközi háborús szponzorok" listájára helyezte az OTP Csoportot, amiért a pénzintézet továbbra is jelen van Oroszországban. Ez a támadás azért példaértékű, mert egy olyan időszakban történt, amikor az üzleti/politikai/stratégiai(katonai) érdekek meglehetősen szembetűnő módon esnek egybe. Ezeket a híreket a katonai cselekmények alakulásának fényében érdemes értékelni, így az egyes megnyilatkozásokban azonosíthatók a véleményformálási szándékok.

### 4.3.3 Fekete-tengeri gabonaszállítási egyezmény

2022. július 27-én jött létre a fekete-tengeri gabona-kezdeményezés (***Black Sea Grain Initiative***) az ENSZ és Törökország közvetítésével az Oroszországi Föderáció és Ukrajna között, amely lehetővé tette a gabona és a hozzá kapcsolódó élelmiszerek, valamint műtrágyák szállítását Ukrajnából. [227] Az ukrán gabonaexportnak a Fekete-tengeren keresztül történő újraindítása a folyamatban lévő háború közepette "reménysugár" egy olyan világban, amelynek égető szüksége van rá - mondta Antonio Guterres ENSZ-főtitkár július 27-én a törökországi Isztambulban tartott aláírási ceremónián. Az ENSZ elképzelése alapján az orosz élelmiszereket és műtrágyákat a világpiacokra juttatják, ami segít stabilizálni a növekvő élelmiszerárakat világszerte, és megakadályozza, hogy emberek milliói haljanak éhen. A kezdeményezés különösen lehetővé teszi a kereskedelmi élelmiszerek és műtrágyák (beleértve az ammóniát) exportját a Fekete-tenger három kulcsfontosságú ukrán kikötőjéből – Odesszából, Csernomorszkból, Juzsnij/Pivdennyijből. Egy Közös Koordinációs Központot (JCC) hoztak létre a kezdeményezés végrehajtásának nyomon követésére. A Közös Koordinációs Központ Isztambulban kapott helyet, melyben Oroszország, Törökország, Ukrajna és az Egyesült Nemzetek Szervezete képviselői végeznek feladatokat. Az ENSZ a Központ titkárságaként is szolgál. Ukrán hajók terelgetik a teherhajókat a Fekete-tenger nemzetközi vizeire, elkerülve az elaknásított területeket. A hajók ezután a megállapodás

szerinti tengeri humanitárius folyosón Isztambulba utaztak. Az ukrán kikötőkbe belépő és onnan kilépő hajókat a KKK-csoportok, köztük orosz, török, ukrán és ENSZ-ellenőrök ellenőrzik. 2022 áprilisában a főtitkár találkozott Vlagyimir Putyin orosz és Volodimir Zelenszkij ukrán elnökkel, hogy javaslatot tegyen erre a tervre. A tárgyalásokkal párhuzamosan két ENSZ-munkacsoportot hoztak létre – az egyik az ukrán gabona Fekete-tengeren történő szállításával, amit Martin Griffiths ENSZ humanitárius főnök és az OCHA vezetője irányított, a másik pedig az orosz élelmiszer- és műtrágyaexport szállításának megkönnyítésével foglalkozott. Rebeca Grynspan, az Egyesült Nemzetek Kereskedelmi és Fejlesztési Szervezetének (UNCTAD) főtitkára. A kezdeményezést nem újították meg a harmadik cikluson túl, amely 2023. július 17-én zárult le. [228] Szergej Sojgu orosz védelmi miniszter és Alekszandr Kubrakov ukrán infrastrukturális miniszter által tavaly júliusban az isztambuli Dolmabahce palotában aláírt megállapodás biztonságos folyosót teremtett az ukrán gabona exportjához három ukrán kikötőből - Odesszából, Juzsnijból és Csernomorszkból. A megállapodás értelmében a török, ukrán és az ENSZ munkatársaiból álló koalíció felügyelte a gabona hajókra rakodását az ukrán kikötőkben, mielőtt az előre megtervezett, az ukrán és orosz csapatok által erősen elaknásított Fekete-tengeren áthaladó útvonalon elindult. Az ukrán pilótahajók az ukrán fél által biztosított biztonságos csatornák térképe segítségével irányították a gabonakereskedő hajókat a part bányászott területein. A hajók ezután átkeltek a Fekete-tengeren a törökországi Boszporusz-szoros felé, az ENSZ, Ukrajna, Oroszország és Törökország képviselőiből álló isztambuli Közös Koordinációs Központ szoros megfigyelése alatt. Az Ukrajnába belépő hajókat ugyanazon közös koordinációs központ irányítása alatt ellenőrizték, hogy a fedélzeten ne legyenek fegyverek. [229] A megállapodás köztes megoldást jelentett a magasabb szintű problémák átmeneti kezelésére, hiszen a részt vevő felek egyformán érdekeltek voltak benne, de nem nyújtott stabil, hosszú távú megoldást a térségben uralkodó feszültségek enyhítésére.

### *Adományok afrikai országok számára*

Az Afrikai Unió rendkívüli ülést hívott össze az ENSZ közvetítésével létrejött gabonamegállapodás helyreállítása érdekében, amely lehetővé tette Ukrajnának, hogy több millió tonna gabonát exportáljon, amelyet Oroszország nevében vágtak le. "A gabona és a műtrágya problémája mindenkit foglalkoztat" - mondta Azali Assoumani Comore-szigeteki elnök, az 55 tagú Afrikai Unió vezetője a RIA Novosztyi orosz állami televíziónak. Szentpéterváron beszélt, ahol Vlagyimir Putyin orosz elnök csúcstalálkozót

tartott afrikai vezetőkkel. [230] Az ENSZ Élelmezési Világprogramja (WFP a világ legnagyobb humanitárius szervezete) a fekete-tengeri kikötőkből is szállított búzát. 2023 júliusára a program gabonatartalékának 80%-át Ukrajnából vásárolták, szemben a háború előtti 50%-kal. A kezdeményezés megvalósítása során több mint 725 ezer tonna búzát szállítottak Ukrajna kikötőiből Etiópiába, Jemenbe, Afganisztánba, Szudánba, Szomáliába, Kenyába és Dzsibutiba. Az EU jelentős búzatermelő és -exportőr, a becslések szerint a 2022/23-as gazdasági évben 31 millió tonna búzát exportált olyan célországokba, mint Algéria, Marokkó, Egyiptom, Pakisztán és Nigéria. [231] Putyin ingyenes gabonát ígért hat országnak [232] az afrikai vezetők júliusi csúcstalálkozóján, röviddel azután, hogy Moszkva kilépett abból a megállapodásból, amely lehetővé tette Ukrajnának, hogy az Oroszországgal vívott háború ellenére gabonát szállítson fekete-tengeri kikötőiből. Putyin azonban azzal érvelt, hogy nem tudja ellátni azokat az országokat, amelyeknek a legsürgetőbb segítségre van szükségük. Az orosz elnök szerint Oroszország tavaly mintegy 60 millió tonna gabonát exportált. Antonio Guterres ENSZ-főkapitány „maroknyi adománynak" nevezte az ingyenes gabona ígéreteit. Kijev szerint a megállapodásból való kilépést követően Oroszország többször is bombázta az ukrán kikötőket és gabonaraktárakat, több százezer tonna gabonát semmisítve meg. Pénteken azonban Ukrajna közölte, hogy 4,4 millió tonna rakományt, köztük 3,2 millió tonna gabonát sikerült átszállítania az augusztusban létrehozott új tengeri folyosón keresztül. [233] „Az év végéig további 200 ezer tonna búzát tervezünk szállítani hat afrikai országba, Szomáliába, a Közép-afrikai Köztársaságba, Burkina Fasóba, Zimbabwébe, Maliba és Eritreába" – mondta Alekszej Poliscsuk, az orosz külügyminisztérium második FÁK-igazgatója. osztály. Azt is elmondta, hogy Moszkva jelenleg az ENSZ Élelmezésügyi Világprogramjával dolgozik együtt az adományozáson, és már 20 000 tonna műtrágyát szállított Malawinak és 34 000 tonna műtrágyát Kenyának. Hozzátette: Zimbabwébe 23 ezer tonna műtrágyát szállítanak a közeljövőben, Nigériába 34 ezer tonnát, Srí Lankára pedig 55 ezer tonnát. [234] A vitában többször is felmerült, hogy a gabonaegyezmény fényében a szállított mennyiség hány százaléka jut el ténylegesen azokhoz a célországokhoz, ahol a legnagyobb szükség van az éhezés elkerülésére. Az orosz-ukrán háború eseményei továbbra is aktívan tematizálják a világ közvéleményét, a konfliktus eszkalációjának veszélyét napirenden tartva.

# ÖSSZEGZETT KÖVETKEZTETÉSEK

*„Határozz, és kimondtad sorsodat.”*
Vörösmarty

***Befejezés***

Kutatásom során három alapvető kérdésre adtam választ: (1) Milyen összefüggés áll fent a manipuláció és a geopolitika között? (2) Milyen tényezőket kell vizsgálni ebben az összefüggésben? (3) Hogyan jelenik meg mindez a gyakorlati alkalmazásban? Széles körű irodalmi megalapozást követően a kutatómunka célkitűzésében megfogalmazott elvek mentén vizsgáltam meg a tudományos probléma tárgyát.

A kutatási cél elérésének érdekében tézisként fogalmaztam meg, hogy **a pszichológiai manipuláció jelentőségének és a geopolitikai folyamatokra gyakorolt hatásainak tanulmányozása során szükséges legalább négy tényezőt figyelembe venni** és ezek mentén vizsgálni az összefüggéseket. Ez a szempontrendszer elegendő alapot nyújt ahhoz, hogy a fontosabb ok-okozati viszonyok kifejtésre kerülhessenek a téma kapcsán.

Az értekezés *első fejezetének* alapvetése volt, hogy meghatározza a ***keretrendszert,*** ami a biztonság koncepciójából kiindulva a kibertérben alkalmazott korszerű támadási technikákig ível. Behatároltam a teret, amely a vizsgálatom tárgyát képezte, azonosítottam azokat a folyamatokat és intézkedéseket, ahol a pszichológiai manipuláció érintettsége fellelhető. Alkalmazása már az ókori idők óta meghatározó elem a konfliktuskezelésben, újdonság viszont az informatikai technológiákkal megtámogatott támadási módszerek sokszínű alkalmazása. A kibertér viszont olyan műveletek végrehajtására kínál lehetőséget, ahol a támadás és a védekezés már nem annyira nyilvánvaló folyamatok, mint azok a történelem korábbi periódusaiban voltak.

A *második fejezet* amellett érvel, hogy az ***eszközhasználatban*** bekövetkezett változások jelentős méreteket öltenek, ahol a közösségi média térnyerésére helyeztem a hangsúlyt. A tömegtájékoztatás korszakainak rövid ismertetése után górcső alá vettem a közösségi internet fejlődéstörténetét, amely a dolgozat technológiai hátterének alapját adja. Az elmúlt évtizedben ezeken a platformokon az üzleti élet képviselői és a magánszemélyek mellett megjelentek a politikai szereplők, valamint a katonai tevékenység is felütötte a fejét. A szakirodalom gyűjtőfogalomként számos meghatározással illeti a nem

szokványos hadviselés megjelenésének formáit; a nyilatkozatháborúk, félretájékoztatási kampányok, propagandaműveletek eddig is jelen voltak, azonban intenzitásuk és a terjedési/terjesztési sebességben, valamint a célközönség elérésében óriási különbségek vannak. Ez az utóbbi tényező adja az eszköz újszerűségét, amely a megelőző korszakok tájékoztatási módszereit ötvözi.

A *harmadik fejezet* célja volt, hogy ***modellalkotás*** eszközével mutassam be a bizalomépítés folyamatát, amely során egy már meglévő modellt használtam a bizalom szerkezetének felépüléséről. Az emberi tényező a legvédettebb rendszerekben is ott van, így kockázati szempontból mindig biztonsági rést képez a védelmi struktúrákban. Mivel az emberi közösségek közötti interakció a közvetítő eszközök miatt gyökeresen megváltozott, bizonyos hagyományosnak mondott eljárások vagy egyszerűen nem működnek, vagy működésük akadályozva van.

A *negyedik fejezet* tézise, hogy a pszichológiai manipuláció jelentősége, valamint azok geopolitikai folyamatokra gyakorolt hatása egyértelműen azonosítható, melyet ***esettanulmányok*** segítségével elemeztem. A SARS-CoV-2 koronavírus világjárvány (Covid-19); a 2020-as hegyi-karabahi háború, majd az év végén az amerikai elnökválasztás; az afganisztáni kivonulás; az ukrán, finn és svéd NATO csatlakozás kérdései és az orosz-ukrán háború eseményein keresztül vizsgáltam a pszichológiai manipuláció megjelenését és alkalmazását. A világjárvány idején a kibertérben számos incidens történt, amelynek látszólagos érintettsége volt csupán a járványkezeléssel kapcsolatos küzdelemnek, ami a bizonytalan környezet biztonsági gyengeségek kiaknázását tette lehetővé. A kritikus infrastruktúrák, egyértelmű példaként említve az egészségügyi szektort, ebben az időszakban intenzívebb támadásoknak voltak kitéve. A közelmúltbeli fegyveres konfliktusokban és a diplomáciai vitákban egyenes ágon érintettek voltak a közösségi média és egyéb kommunikációs alkalmazások.

Összességében megállapítottam, hogy a négy tényező: a történelmi háttér, a technológiai változás, a bizalomépítés folyamatának modellje és a gyakorlati alkalmazások elemzése megfelelő szempontrendszernek bizonyult a pszichológiai manipuláció jelentősége és geopolitikai hatásai közötti összefüggés megértéséhez.

# Új tudományos eredmények

**T1: A kritikus infrastruktúrák védelme nélkül a társadalmi biztonság nem értelmezhető**

Ismertettem, hogy eddig a kibertéren keresztül végrehajtott támadások a működés akadályozását szolgálták, a koronavírus világjárvány és az orosz-ukrán háború alatti események viszont egyértelműen új megvilágításba helyezték a kritikus infrastruktúrák védelmének jelentőségét. [T4][T6][T9]

**T2: A tömegkommunikációban szignifikáns változás történt az elmúlt évtizedben**

Bizonyítottam, hogy a közösségi média használat és a hírfogyasztási szokásokat tekintve jelentős szintlépés történt a korábbi korszakokhoz képest. [T2][T5][T8][T11]

**T3: Az álhírek azonosítására és szűrésére szemlélet/modell alkotható**

Megállapítottam, hogy az álhírek az érzelmi alapokat célzó stratégiájuk miatt kiszűrhetők a kommunikációs csatornákon. Továbbfejlesztett modellt alkottam a bizalomépítés folyamatának vizsgálatához. [T2][T5][T7]

**T4: A pszichológiai manipuláció szerepe meghatározó a geopolitikai események alakulásában**

Bemutattam, hogy az orosz-ukrán háború és az abból következő európai energiaválság számos példával igazolja a pszichológiai manipuláció szerepét a geopolitikai folyamatok alakításában, a törésvonal-konfliktusok kicsúcsosodása mentén a közvélemény tájékoztatásában a modern kommunikációs csatornák újszerű lehetőségeket biztosítanak. [T1][T3][T6][T8][T9][T10]

**Tézisekhez kapcsolódó publikációk**


[T1] T. Kun, “The European Migration Crisis and the aspects of Security Politics,” In: Fehér-Polgár, Pál; Garai-Fodor, Mónika (szerk.) FIKUSZ 2018 - Symposium for Young Researchers Proceedings, Óbudai Egyetem, Keleti Károly Gazdasági Kar (2019) pp. 271-279.

[T2] T. Kun, "Critical Thinking and Trust: The Art of Decision Making," in Ninth International Scientific Web-conference of Scientists and PhD. students or candidates : Trends and Innovations in E-business, Education and Security : TIEES 2021, Bratislava, The Slovak Society for Economic Informatics, 2021, pp. 73-80.

[T3] T. Kun, "Which one of us is the ‘Phisherman’and which one is the Trout?," in Eight International Scientific Web-conference of Scientists and PhD. students or candidates, Z. Rajnai, P. Schmidt and P. Jurik (eds.)., Bratislava, The Slovak Society for Economic Informatics, 2020, pp. 184-192.

[T4] T. Kun, "Események a kibertérben a COVID-19 járvány idején," Biztonságtudományi Szemle, vol. 2., no. 3., pp. 67-76., 2020.

[T5] T. Kun, "A pszichológiai manipuláció jelenléte a politikában," in Mérnöki Szimpózium a Bánkin előadásai : Proceedings of the Engineering Symposium at Bánki (ESB 2019), Budapest, Óbudai Egyetem, 2019, pp. 89-94.

[T6] T. Kun, "Critical Infrastructures: The Bottleneck of Societal Security," National Security Review, vol. 5, no. 1, pp. 56-65, 2019.

[T7] T. Kun, "The War on Disinformation: The Structure of Trust," In: Frédéric, Labarre; George, Niculescu (eds.) Understanding the Contemporary Information Landscape: A Handbook, Vienna, Landesverteidigungsakademie, 2022, pp. 153-165.

[T8] T. Kun, “Katonai tevékenységek megjelenése a közösségi médiában és egyéb kommunikációs alkalmazásokban,” Honvédségi Szemle, vol. 153, no. 5, 2023.

[T9] T. Kun, “Social Engineering in Europe’s Energy Crisis?,” Sodobni vojaški izzivi/Contemporary Military Challenges, vol. 25, no. 1, pp. 73-88, 2023.

[T10] T. Kun & I. Takács „The Change in Fertilizer Prices Due to the Russo-Ukraine War”, Connections QJ, vol. 22, no. 2. (2023)

[T11] T. Kun, “Threats and Risks of Psychological and Social Manipulation” in Building Resilience against Human Security Threats and Risks: From Best Practices to Strategies, Vienna, Landesverteidigungsakademie, 2024 -- *megjelenés függőben* --

## Ajánlások

Az értekezésben foglaltak a téma jövőbeni kutatásában hasznos ismereteket nyújthatnak a hazai irodalom magyar nyelven történő bővítése által. Írásomat ajánlom elsősorban a védelmi szektorban érintett **kutatók**, **döntéshozók** és **véleményformálók** számára, akik a **geopolitika** kérdéseit vizsgálják főképp a **technológiai változások** tükrében, viszont jó alapot tud nyújtani egyéb határterületek kutatói számára is. Javaslom a modellalkotási fejezetben megfogalmazott elképzelések további kutatásokban való felhasználását. Felismerve a kapcsolódási pontot a szakirodalom feldolgozása során, továbbfejlesztettem egy már meglévő modellt a bizalom szerkezeti felépítésére vonatkozólag, ami mérhetővé és összehasonlíthatóvá teszi a bizalomépítés folyamatából adódó helyzeteket. Alkalmazási területként olyan események vizsgálatát tartom célszerűnek, ahol a döntési folyamatban az **érzelmi tényezőnek** kiemelt jelentősége van, ilyen például az álhírek terjedése és az arra adott társadalmi reakciók vizsgálata.

# IRODALOMJEGYZÉK


[1] K. D. Mitnick, The Art of Deception: Controlling the Human Element of Security, Hoboken, New Jersey: John Wiley & Sons, 2002.

[2] BBC, "The war to end all wars," bbc.com.uk, 10 11 1998. [Online]. Available: http://news.bbc.co.uk/1/hi/special_report/1998/10/98/world_war_i/198172.stm. [Accessed 30 03 2023].

[3] H. A. Kissinger, Világrend, Budapest: Antall József Tudásközpont, 2017.

[4] S. P. Huntington, "The Clash of Civilizations?," *Foreign Affairs,* vol. 72, no. 3, pp. 22-49, 1993.

[5] Országgyűlés, "94/1998. (XII. 29.) OGY határozat a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről," mkogy.jogtar.hu, 29 12 1998. [Online]. Available: https://mkogy.jogtar.hu/jogszabaly?docid=998h0094.OGY.. [Accessed 20 06 2019].

[6] T. Babos, Az európai biztonság öt központi pillére: doktori értekezés, Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2004.

[7] P. Gallis, "NATO in Afghanistan: A Test of the Transatlantic Alliance," *Connections,* vol. 6, no. 3, pp. 10-32, 2007.

[8] R. N. McDermott, "Brothers Disunited: Russia's Use of Military Power in Ukraine," in *The Return of the Cold War,* London, Routledge, 2016, pp. 77-107.

[9] L. Berek, L. Berek and Z. Rajnai, A tudományos kutatás folyamata és módszerei, Budapest: Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2022.

[10] L. Kovács, "A kiberbiztonság stratégiai megközelítése. Akadémiai doktori értekezés," 2018. [Online]. Available: http://real-d.mtak.hu/1180/7/dc_1600_18_doktori_mu.pdf. [Accessed 07 02 2023].

[11] Online Etymology Dictionary, “secure | Etymology of secure by etymonline,” etymonline.com, 06 04 2022. [Online]. Available: https://www.etymonline.com/word/secure. [Accessed 10 02 2023].

[12] F. Gazdag and P. Tálas, “A biztonság fogalmának határairól,” *Nemzet és Biztonság,* vol. 1, no. 1, pp. 3-9, 2008.

[13] T. A. Johnson, Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, Boca Raton, FL: Taylor and Francis Group, 2015, pp. 70-72..

[14] Huncert, “Mi a biztonság?,” 2023. [Online]. Available: https://web.archive.org/web/20230531031834/https://www.cert.hu/mi-a-biztonsag. [Accessed 17 03 2023].

[15] Z. Haig, “Katonai műszaki tudományok a 21. században,” *Hadtudomány,* vol. 26, no. 1-2, pp. 115-116, 2016.

[16] L. Muha, “Az informatikai biztonság egy lehetséges módszertana,” *Bolyai Szemle,* vol. 17, no. 4, pp. 137-156, 2008.

[17] K. Turcsányi and F. Vasvári, “A biztonságtudományról és szerepéről a korszerű menedzsmentszemlélet kialakításában,” *Hadtudomány,* vol. 9, no. 1, pp. 56-76, 1999.

[18] Z. Haig, “Információs támadás és hatásai,” in *Kommunikáció - 2006,* Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2006, pp. 119-130.

[19] T. Babos, “A biztonság globális és európai összefüggései,” *Hadtudomány,* vol. 29, no. 4, pp. 16-29, 2019.

[20] Z. Haig, L. Kovács, L. Ványa and S. Vass, “Elektronikai Hadviselés,” Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[21] P. Sipos and I. Ravasz, Magyarország a második világháborúban • Lexikon A-ZS, Budapest: PETIT REAL Könyvkiadó, 1997.

[22] American Psychological Association, “APA Dictionary of Psychology - Manipulation,” dictionary.apa.org, 19 04 2018. [Online]. Available: https://dictionary.apa.org/manipulation. [Accessed 06 04 2022].

[23] North Atlantic Treaty Organization (NATO), “AJP-3.10 ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS,” 23 11 2009. [Online]. Available: https://info.publicintelligence.net/NATO-IO.pdf. [Accessed 21 03 2023].

[24] Joint Publication 3-13.4, “Military deception (redacted),” 14 02 2017. [Online]. Available: https://irp.fas.org/doddir/dod/jp3_13_4.pdf. [Accessed 17 03 2023].

[25] T. Shallice, “Psychology and social control,” *Cognition,* vol. 17, no. 1, pp. 29-48, 1984.

[26] B. Révész, “Macskák háborúja,” 25 04 2020. [Online]. Available: https://honvedelem.hu/hatter/multidezo/macskak-haboruja.html. [Accessed 06 04 2023].

[27] F. Tőkei, “Szun-Ce: A hadviselés törvényei,” [Online]. Available: https://mek.oszk.hu/01300/01345/01345.htm. [Accessed 18 06 2023].

[28] V. D. Mahajan, Jurisprudence and Legal Theory., Lucknow: Eastern Book Company, 1983.

[29] Y.-c. Chiang, Social Engineering and the Social Sciences in China, 1919-1949, Cambridge: Cambridge University Press, 2001.

[30] K. Popper, The Open Society and Its Enemies With a preface by Václav Havel, London and New York: Routledge, 2011.

[31] K. S. Nagy, Szociológia közgazdászoknak, Budapest: Typotex, 2007.

[32] Mandiner, “Ryszard Legutko: Európa konzervatív politikusai letették a fegyvert,” mandiner.hu, 08 03 2021. [Online]. Available: https://mandiner.hu/kulfold/2021/03/ryszard-legutko-europa-konzervativ-politikusai-letettek-a-fegyvert. [Accessed 18 04 2024].

[33] C. Marklund, Bridging Politics and Science: The Concept of Social Engineering in Sweden and the USA, Circa 1890-1950, European University Institute, 2008.

[34] T. Kun, “Threats and Risks of Psychological and Social Manipulation,” in *Building Resilience against Human Security Threats and Risks: From Best Practices to Strategies*, Vienna, Landesverteidigungsakademie, 2024.

[35] J. A. Gardner, “The sociological jurisprudence of Roscoe Pound (Part I),” *Villanova Law Review*, vol. 7, no. 1, pp. 1-26, 1961.

[36] L. J. McManaman, “Social Engineering: The Legal Philosophy of Roscoe Pound,” *St. John's Law Review*, pp. 1-47, 1958.

[37] T. Nyíri, “A „lélektani hadviselés” tömegpszichológiai aspektusai,” *Új Honvédségi Szemle,* vol. 8, no. 3, pp. 92-100, 1998.

[38] G. Ritzer, The McDonaldization of Society 6, London: Sage Publications Ltd., 2011.

[39] D. W. Larson, “Was the Cold War a Spiral of Mistrust?,” *International Studies Review*, vol. 8, no. 2, pp. 300-302, 2006.

[40] L. Borhi, “Hadüzenettől rendszerváltásig Az Egyesült Államok és Magyarország, 1941–1991. Akadémiai doktori értekezés,” 2010. [Online]. Available: http://real-d.mtak.hu/369/4/borhilaszlo_5_mu.pdf. [Accessed 18 03 2023].

[41] American Foreign Relations, “Television - The persian gulf war,” americanforeignrelations.com, 2023. [Online]. Available: https://www.americanforeignrelations.com/O-W/Television-The-persian-gulf-war.html. [Accessed 15 06 2023].

[42] Magyarország Kormánya, “Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf,” 21 03 2013. [Online]. Available: https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf. [Accessed 20 06 2019].

[43] Z. Haig and L. Kovács, Kritikus infrastruktúrák és kritikus információs infrastruktúrák, Budapest: Nemzeti Közszolgálati Egyetem, 2012.

[44] I. Legárd, “A kiberhadviselés fogalma, nemzetközi jogi háttere, történeti áttekintése,” in *In: Krasznay, Csaba (szerk.) Taktikák és stratégiák a kiberhadviselésben*, Budapest, Ludovika Egyetemi Kiadó, 2023, pp. 11-40.

[45] L. Muha, A kritikus információs infrastruktúrák védelme, Budapest: RelNet Technológia Kft., 2015.

[46] Z. Haig, B. Hajnal, L. Kovács, L. Muha and Z. Sik, A kritikus információs infrastruktúrák meghatározásának módszertana, Budapest: ENO Advisory Kft., 2009.

[47] T. Babos and A. L. Beregi, “Technological and information warfare in the XXI. century,” *Biztonságtudományi Szemle,* vol. 3, no. 1, pp. 123-135, 2021.

[48] UNDRR - United Nations Office for Disaster Risk Reduction, “Critical infrastructure,” undrr.org, 2021. [Online]. Available: https://www.undrr.org/terminology/critical-infrastructure. [Accessed 23 06 2021].

[49] Országgyűlés, “2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről,” net.jogtar.hu, 2012. [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1200166.tv. [Accessed 20 03 2021].

[50] B. Buzan, People, states and fear, Great Britain, Brighton, Sussex: Wheatsheaf Books Ltd., 1983.

[51] J. Besenyő, “Barry Buzan’s Securitization Theory and the Case of Iraqi Kurdish Military Action Against ISIS in 2014,” *Journal of Security and Sustainability Issues,* pp. 295-306, 2019.

[52] B. Buzan, O. Wæver and J. de Wilde, Security: A New Framework for Analysis., Boulder, Colorado: Lynne Rienner Publishers, 1998.

[53] A. Collins, Contemporary Security Studies, New York: Oxford University Press, 2016.

[54] Cybersecurity and Infrastructure Security Agency, “Critical Infrastructure Sectors,” cisa.gov, 2023. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors. [Accessed 13 05 2023].

[55] Z. Rajnai and B. Fregan, “Kritikus infrastruktúrák védelme (jogi szabályozás),” *Műszaki Tudományos Közlemények,* vol. 3, no. 5, pp. 349-352, 2016.

[56] T. Babos, “The First Critical Infrastructure Protection Research Project in Hungary,” in *In: Nádai, László; Padányi, József (szerk.) Critical Infrastructure Protection Research : Results of the First Critical Infrastructure Protection Research Project in Hungary*, Zürich, Springer-Verlag, 2016, pp. 1-22.

[57] hvg.hu, “Telekom: Példátlan mértékű hackertámadás érte Magyarországot a Szuperkupa-döntő idején,” hvg.hu, 25 09 2020. [Online]. Available: https://hvg.hu/tudomany/20200925_szuperkupa_donto_hackertamadas_magyar_telekom. [Accessed 28 02 2024].

[58] T. Kun, “Critical Infrastructures: The Bottleneck of Societal Security,” *National Security Review*, vol. 5, no. 1, pp. 56-65, 2019.

[59] Z. Rajnai and A. Végh, “A bevetésirányítási rendszerekbe integrált beszédcélú eszközök fejlődése, jelene,” *Biztonságtudományi Szemle,* vol. 3, no. 1, pp. 55-64, 2021.

[60] A. P. Bodó, R. Haddad, T. Marsi and P. Pongrácz, Kritikus információs infrastruktúrák védelme, Budapest: Nemzeti Közszolgálati Egyetem, 2019.

[61] ENISA - European Union Agency for Cybersecurity, “NIS Directive,” enisa.europa.eu, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new. [Accessed 09 04 2024].

[62] European Commission, “General Data Protection Regulation (GDPR),” eur-lex.europa.eu, 27 04 2016. [Online]. Available: https://eur-lex.europa.eu/HU/legal-content/summary/general-data-protection-regulation-gdpr.html. [Accessed 28 02 2024].

[63] ENISA, “What is "Social Engineering"?,” enisa.europa.eu, 2005. [Online]. Available: https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering. [Accessed 25 10 2023].

[64] K. D. Mitnick and W. L. Simon, The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers, New York: John Wiley & Sons, 2005.

[65] K. D. Mitnick and R. Vamosi, The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data, Boston, Massachusetts, USA: Little, Brown and Company, 2017.

[66] C. Kollár and Á. Zakar, “A social engineering és a manipulációs technikák és módszerek,” *Biztonságtudományi Szemle,* vol. 2, no. 2, pp. 23-38, 2020.

[67] B. R. Barna, C. Kollár and E. D. Oroszi, “A social engineering helye az információbiztonsági auditban,” *Biztonságtudományi Szemle,* vol. 5, no. 1, pp. 25-41, 2023.

[68] Newport Institute, “How to Tell If Someone Is Gaslighting You,” Newportinstitute.com, 04 11 2021. [Online]. Available: https://www.newportinstitute.com/resources/mental-health/what_is_gaslighting_abuse/. [Accessed 18 06 2023].

[69] T. Kun, “Which one of us is the ‘Phisherman’and which one is the Trout?,” in *Eight International Scientific Web-conference of Scientists and PhD. students or candidates*, Z. Rajnai, P. Schmidt and P. Jurik, Eds., Bratislava, The Slovak Society for Economic Informatics, 2020, pp. 184-192.

[70] Microsoft, “Mi az a DDoS-támadás?,” Microsoft.com, 2023. [Online]. Available: https://www.microsoft.com/hu-hu/security/business/security-101/what-is-a-ddos-attack. [Accessed 30 04 2023].

[71] A. Magnusson, “Man-in-the-Middle (MITM) Attack: Definition, Examples & More,” Strongdm.com, 21 04 2023. [Online]. Available: https://www.strongdm.com/blog/man-in-the-middle-attack. [Accessed 30 04 2023].

[72] Valimail, “Spear Phishing vs Phishing: The Differences and Examples,” Valimail.com, 08 03 2023. [Online]. Available: https://www.valimail.com/blog/phishing-vs-spear-phishing/. [Accessed 30 04 2023].

[73] Ericom, “What is a Drive-By Attack?,” Ericom.com, 2023. [Online]. Available: https://www.ericom.com/whatis/drive-by-attack/. [Accessed 30 04 2023].

[74] Center for Internet Security, “Election Security Spotlight – Password Attacks,” Cisecurity.org, 2023. [Online]. Available: https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-password-attacks. [Accessed 30 04 2023].

[75] PortSwigger, “SQL injection,” PortSwigger.net, 2023. [Online]. Available: https://portswigger.net/web-security/sql-injection. [Accessed 30 04 2023].

[76] Synopsys, “Cross-Site Scripting (XSS),” Synopsys.com, 2023. [Online]. Available: https://www.synopsys.com/glossary/what-is-cross-site-scripting.html. [Accessed 30 04 2023].

[77] Fortinet, “What is Eavesdropping?,” Fortinet.com, 2023. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/eavesdropping. [Accessed 30 04 2023].

[78] Kaspersky, “Birthday attack,” Encyclopedia.kaspersky.com, 2023. [Online]. Available: https://encyclopedia.kaspersky.com/glossary/birthday-attack/. [Accessed 30 04 2023].

[79] Cyberark, “What is a Malware Attack? - Definition - CyberArk,” Cyberark.com, 2023. [Online]. Available: https://www.cyberark.com/what-is/malware/. [Accessed 30 04 2023].

[80] Britannica, “The Britannica Dictionary - Social Media,” britannica.com, 2024. [Online]. Available: https://www.britannica.com/dictionary/social-media. [Accessed 11 04 2024].

[81] Cambridge Dictionary, “SOCIAL MEDIA | English meaning - Cambridge Dictionary,” dictionary.cambridge.org, 2024. [Online]. Available: https://dictionary.cambridge.org/us/dictionary/english/social-media. [Accessed 11 04 2024].

[82] U.S. Department of Justice, “Global Disruption of Three Terror Finance Cyber-Enabled Campaigns,” 13 08 2020. [Online]. Available: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns. [Accessed 30 10 2020].

[83] B. Duignan, “Britannica - dot-com bubble,” britannica.com, 20 02 2024. [Online]. Available: https://www.britannica.com/event/dot-com-bubble. [Accessed 08 04 2024].

[84] W. Kenton, “What Is Web 2.0? Definition, Impact, and Examples,” investopedia.com, 30 07 2023. [Online]. Available: https://www.investopedia.com/terms/w/web-20.asp#toc-web-20-vs-web-10. [Accessed 08 04 2024].

[85] McKinsey & Company, “What is Web3?,” mckinsey.com, 10 10 2023. [Online]. Available: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-web3. [Accessed 08 04 2024].

[86] R. McNamara, “Penny Press - Cutting the Price of Newspapers to a Penny Was a Startling Innovation,” thoughtco.com, 31 08 2017. [Online]. Available: https://www.thoughtco.com/penny-press-definition-1773293. [Accessed 06 05 2023].

[87] MMI ELTE - Művészetelméleti és Médiakutatási Intézet, “A nyomtatott sajtó nemzetközi története,” mmi.elte.hu, 18 06 2015. [Online]. Available: https://mmi.elte.hu/szabadbolcseszet/mmi.elte.hu/szabadbolcseszet/index2f52.html?option=com_tanelem&id_tanelem=544&tip=0. [Accessed 06 05 2023].

[88] R. W. Gehl and S. T. Lawson, Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication, Cambridge, Massachusetts, Egyesült Államok: MIT Press, 2022.

[89] E. Bernays, Crystallizing Public Opinion, New York: Liveright Publishing Corporation, 1923.

[90] W. Lippmann, Public Opinion, New York: Harcourt, Brace and Company, 1922.

[91] E. Kollár, "A rádiózás története," radiomuseum.hu, 2009. [Online]. Available: https://www.radiomuseum.hu/torteneti_m.html. [Accessed 06 05 2023].

[92] W. B. Ashworth, "Scientist of the Day - Alexander Popov," lindahall.org, 16 03 2021. [Online]. Available: https://www.lindahall.org/about/news/scientist-of-the-day/alexander-popov/. [Accessed 06 05 2023].

[93] MMI ELTE - Művészetelméleti és Médiakutatási Intézet, "A televízió története," mmi.elte.hu, 18 06 2015. [Online]. Available: https://mmi.elte.hu/szabadbolcseszet/mmi.elte.hu/szabadbolcseszet/index9ea5.html. [Accessed 06 05 2023].

[94] S. Forgó, "3.6. A televízió története," forgos.uni-eszterhazy.hu, 2011. [Online]. Available: https://forgos.uni-eszterhazy.hu/wp-content/tananyagok/tamop/mediumismeret_II/27_04/36_a_televzi_trtnete.html. [Accessed 07 05 2023].

[95] A. Kapornaki, "Háború élő adásban," mediakutato.hu, 2012. [Online]. Available: https://mediakutato.hu/cikk/2012_01_tavasz/04_haboru_elo_adasban. [Accessed 07 05 2023].

[96] G. M. Graff, "Pagers, Pay Phones, and Dialup: How We Communicated on 9/11," wired.com, 11 9 2019. [Online]. Available: https://web.archive.org/web/20190917060206/https://www.wired.com/story/pagers-pay-phones-and-dialup-how-we-communicated-on-911/. [Accessed 07 05 2023].

[97] Cambridge Dictionary, “BLOG | English meaning - Cambridge Dictionary,” dictionary.cambridge.org, 2024. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/blog. [Accessed 14 04 2024].

[98] R. Blood, “Weblogs: A History And Perspective,” rebeccablood.net, 07 09 2000. [Online]. Available: http://www.rebeccablood.net/essays/weblog_history.html. [Accessed 14 04 2024].

[99] J. Berger, “Robot Wisdom WebLog for December 1997,” robotwisdom.com, 17 12 1997. [Online]. Available: https://web.archive.org/web/20000817183237/http://www.robotwisdom.com/log1997m12.html. [Accessed 14 04 2024].

[100] A. Minaev, “What is a Blog? – Definition of Terms Blog, Blogging, and Blogger,” firstsiteguide.com, 04 10 2023. [Online]. Available: https://firstsiteguide.com/what-is-blog/. [Accessed 14 04 2024].

[101] M. Mullenweg, “WordPress Now Available,” wordpress.org, 27 05 2003. [Online]. Available: https://wordpress.org/news/2003/05/wordpress-now-available/. [Accessed 14 04 2024].

[102] S. Balkhi, “The History of WordPress from 2003 – 2024 (with Screenshots),” wpbeginner.com, 03 01 2024. [Online]. Available: https://www.wpbeginner.com/news/the-history-of-wordpress/. [Accessed 14 04 2024].

[103] SG, “Elindult a T-Online tiniportálja, a G-Portál,” sg.hu, 06 01 2006. [Online]. Available: https://sg.hu/cikkek/41852/elindult_a_t_online_tiniportalja_a_g_portal. [Accessed 14 04 2024].

[104] Cambridge Dictionary, “MODERATOR | English meaning - Cambridge Dictionary,” dictionary.cambridge.org, 2024. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/moderator. [Accessed 14 04 2024].

[105] Maryville University, “The Evolution of Social Media: How Did It Begin, and Where Could It Go Next?,” maryville.edu, 28 05 2020. [Online]. Available: https://online.maryville.edu/blog/evolution-social-media/#history. [Accessed 11 04 2024].

[106] U.S. Department of State, “(U//FOUO) U.S. State Department Social Media Landscape: Hungary,” publicintelligence.net, 24 01 2011. [Online]. Available: https://publicintelligence.net/ufouo-u-s-state-department-social-media-landscape-hungary/. [Accessed 20 03 2023].

[107] D. Goodin, “Skype replaces P2P supernodes with Linux boxes hosted by Microsoft (updated),” arstechnica.com, 05 01 2012. [Online]. Available: https://arstechnica.com/information-technology/2012/05/skype-replaces-p2p-supernodes-with-linux-boxes-hosted-by-microsoft/. [Accessed 10 04 2024].

[108] S. Shah, “The history of social networking,” 14 05 2016. [Online]. Available: https://www.digitaltrends.com/computing/the-history-of-social-networking/.

[109] IAS team, “The evolution of social media advertising,” 19 12 2017. [Online]. Available: https://integralads.com/insider/evolution-of-social-ads/.

[110] “47 USC 230: Protection for private blocking and screening of offensive material Ex. Ord. No. 13925, May 28, 2020, 85 F.R. 34079 Preventing Online Censorship,” 28 05 2020. [Online]. Available: https://uscode.house.gov/view.xhtml?req=(title:47%20section:230%20edition:prelim).

[111] U.S. Senate Committee of Judiciary, “Protecting Children Online,” 31 01 2024. [Online]. Available: https://www.judiciary.senate.gov/protecting-children-online.

[112] M. Calabresi, “Inside Russia’s Social Media War on America,” time.com, 18 05 2017. [Online]. Available: https://time.com/4783932/inside-russia-social-media-war-america/. [Accessed 30 05 2023].

[113] Tessian Research, “How to Hack a Human,” [Online]. Available: https://f.hubspotusercontent20.net/hubfs/1670277/%5BCollateral%5D%20Tessi

an%20Research/%5BTessian%20Research%5D%20How%20to%20Hack%20a%20Human/%5BTessian%20Research%5D%20How%20to%20Hack%20a%20Human.pdf?__hstc=170273983.5a52778ae3ec548b43f13d9c6d234270.1657. [Accessed 28 02 2024].

[114] C. Moravec, “The weaponization of social media,” Security Magazine, 14 10 2022. [Online]. Available: https://www.securitymagazine.com/articles/98476-the-weaponization-of-social-media. [Accessed 26 03 2023].

[115] Foundation for Critical Thinking, “Defining Critical Thinking,” criticalthinking.org, 2019. [Online]. Available: https://www.criticalthinking.org/pages/defining-critical-thinking/766. [Accessed 23 10 2023].

[116] R. H. Ennis, “Critical thinking assessment,” *Theory into practice,* vol. 32, no. 3, pp. 179-186., 1993.

[117] A. Fisher, Critical Thinking: An Introduction, Cambridge: University Press, 2011.

[118] M. Lipman, “Critical thinking: What can it be?,” *Analytic Teaching,* vol. 8, no. 1, pp. 5-12., 1987.

[119] Cambridge Dictionary, “FAKE NEWS | English meaning - Cambridge Dictionary,” dictionary.cambridge.org, 2024. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/fake-news. [Accessed 12 03 2024].

[120] Voice.ai, “Real-Time AI Voice Changer,” [Online]. Available: https://voice.ai/. [Accessed 11 02 2023].

[121] S. Poremba, “Propaganda as a Social Engineering Tool,” securityboulevard.com, 13 07 2021. [Online]. Available: https://securityboulevard.com/2021/07/propaganda-as-social-engineering-tool/. [Accessed 16 10 2023].

[122] A. Hern, “YouTube moves to limit spread of false coronavirus 5G theory,” 05 04 2020. [Online]. Available: https://www.theguardian.com/world/2020/apr/05/youtube-to-suppress-content-spreading-coronavirus-5g-conspiracy-theory.

[123] A. Satariano and D. Alba, “Burning Cell Towers, Out of Baseless Fear They Spread the Virus,” 10 04 2020. [Online]. Available: https://www.nytimes.com/2020/04/10/technology/coronavirus-5g-uk.html.

[124] T. Kun, “A pszichológiai manipuláció jelenléte a politikában,” in *Mérnöki Szimpózium a Bánkin előadásai : Proceedings of the Engineering Symposium at Bánki (ESB 2019)*, Budapest, Óbudai Egyetem, 2019, pp. 89-94.

[125] N. Biasini and E. Brumaghin, “How adversaries use politics for compromise,” 05 11 2019. [Online]. Available: https://blog.talosintelligence.com/2019/11/political-malware.html. [Accessed 07 12 2023].

[126] A. Satariano and A. Tsang, “Who’s Spreading Disinformation in U.K. Election? You Might Be Surprised,” 10 12 2019. [Online]. Available: https://www.nytimes.com/2019/12/10/world/europe/elections-disinformation-social-media.html.

[127] L.-M. Neudert and P. Howard, “Online politics needs to be cleaned up – but not just by Facebook and Twitter,” 11 11 2019. [Online]. Available: https://www.theguardian.com/commentisfree/2019/nov/11/online-politics-facebook-twitter-social-media-political-parties.

[128] L. Kovács and C. Krasznay, “„Mert övék a hatalom”: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során,” *Nemzet és Biztonság,* vol. 10, no. 3, pp. 3-15, 2017.

[129] D. Slack, “Trump to CNN: ‘You are fake news’,” eu.usatoday.com, 11 01 2017. [Online]. Available: https://eu.usatoday.com/story/news/politics/onpolitics/2017/01/11/trump-cnn-press-conference/96447880/. [Accessed 06 05 2023].

[130] N. Lanum and B. Flood, “CNN's long history of pushing disinformation, here are five examples,” foxnews.com, 12 04 2022. [Online]. Available: https://www.foxnews.com/media/cnn-disinformation-examples-smollett-collusion-covington-rogan-media. [Accessed 06 05 2023].

[131] Carbon Black, “Destructive Cyberattacks Increase Ahead of 2018 Midterm Elections,” 2018.

[132] D. Loucaides, “The Kremlin Has Entered the Chat,” wired.com, 03 02 2023. [Online]. Available: https://www.wired.com/story/the-kremlin-has-entered-the-chat/. [Accessed 15 06 2023].

[133] Telegraph, “9 Errors Wired Chose to Make,” telegra.ph, 03 02 2023. [Online]. Available: https://telegra.ph/Wired-Errors. [Accessed 15 06 2023].

[134] USAID/Internews, “Ukrainians Increasingly Rely on Telegram Channels for News and Information During Wartime,” internews.org, 01 11 2023. [Online]. Available: https://internews.org/ukrainians-increasingly-rely-on-telegram-channels-for-news-and-information-during-wartime/. [Accessed 15 04 2024].

[135] G. Koós and G. Szternák, “A katonai stratégia és a hadművészet fejlődésének irányai az Oroszországi Föderációban,” *Szakmai Szemle,* vol. 18, no. 1, pp. 24-36, 2020.

[136] Z. Somodi and Á. P. Kiss, “A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban,” *Honvédségi Szemle,* vol. 147, no. 6, pp. 22-28, 2019.

[137] P. W. Singer and E. T. Brooking, LikeWar: The Weaponization of Social Media, Boston, New York: Eamon Dolan Books Houghton Mifflin Harcourt, 2018.

[138] J. Besenyő, A. Gulyás and D. Trifunovic, “Hezbollah and the Internet in the Twenty-First Century,” *International Journal of Intelligence and CounterIntelligence,* vol. 36, no. 3, pp. 669-685, 2023.

[139] T. Babos, “„Globális közös terek” a NATO-ban,” *Nemzet és Biztonság,* vol. 4, no. 3, pp. 34-46, 2011.

[140] Z. Haig, “Kibertéri kognitív befolyásolás az információs műveletekben,” *Hadtudományi Szemle,* vol. 15, no. 2, pp. 115-130, 2022.

[141] T. Kun, “Katonai tevékenységek megjelenése a közösségi médiában és egyéb kommunikációs alkalmazásokban,” *Honvédségi Szemle,* vol. 153, no. 5, 2023.

[142] C. Németh, “A közösségi média mint legújabb hadszíntér,” biztonsagpolitika.hu, 03 12 2021. [Online]. Available: https://biztonsagpolitika.hu/elemzesek/a-kozossegi-media-mint-legujabb-hadszinter. [Accessed 15 04 2024].

[143] P. Bányász, “A közösségi média, mint az információs hadszíntér speciális tartománya,” *Hadmérnök,* vol. 12, no. 2, pp. 108-121, 2017.

[144] S. Walsh, “The Top 10 Social Media Sites & Platforms,” searchenginejournal.com, 03 04 2024. [Online]. Available: https://www.searchenginejournal.com/social-media/social-media-platforms/. [Accessed 11 04 2024].

[145] G. Bárczi and L. Országh, A magyar nyelv értelmező szótára, Budapest: MTA, 1959-1962.

[146] A. Bradford, "The Five (and More) Senses," 24 10 2017. [Online]. Available: https://www.livescience.com/60752-human-senses.html. [Accessed 20 01 2022].

[147] R. Lewicki and C. Wiethoff, "Trust, Trust Development, and Trust Repair," in *The Handbook of Conflict Resolution: Theory and Practice,* San Francisco, Jossey-Bass Publishers, 2000, pp. 86-107..

[148] R. Mayson, "Wonky Wonga: a failure to understand trust," blackislegroup.com, 05 09 2018. [Online]. Available: https://web.archive.org/web/20210922072956/https://blackislegroup.com/2018/09/wonky-wonga-a-failure-to-understand-trust/. [Accessed 29 05 2021].

[149] Black Isle Group, "The Trust Equation," 7 09 2017. [Online]. Available: https://web.archive.org/web/20210922083304/https://blackislegroup.com/2017/09/the-trust-equation/. [Accessed 29 05 2021].

[150] D. H. Maister, C. H. Green and R. M. Galford, The Trusted Advisor, New York, NY: Simon and Schuster, 2000, pp. 69-78..

[151] G. M. Vogel, “The trusted advisor,” *Public Integrity,* vol. 17, no. 2, pp. 221-222, 2015.

[152] J. Baldoni, "How Trustworthy Are You?," 15 05 2008. [Online]. Available: https://hbr.org/2008/05/how-trustworthy-are-you. [Accessed 29 05 2021].

[153] J. Lawrence, “Book review: The Trusted Advisor by David Maister, Charles Green and Robert Galford,” hrzone.com, 02 07 2013. [Online]. Available: https://hrzone.com/book-review-the-trusted-advisor-by-david-maister-charles-green-and-robert-galford/. [Accessed 26 04 2021].

[154] C. Hansen, N. Worziger and C. Salling, "Become a trusted finance business partner," 08 2020. [Online]. Available: https://web.archive.org/web/20221025165605/https://implementconsultinggroup.com/article/become-a-trusted-finance-business-partner/. [Accessed 29 05 2021].

[155] R. Greiner, "The Trust Equation," 10 04 2013. [Online]. Available: https://robertgreiner.com/the-trust-equation/. [Accessed 29 05 2021].

[156] B. Brearley, "Why Building Trust Is Better Than Authority," 11 2019. [Online]. Available: https://www.thoughtfulleader.com/building-trust-leadership-strategy/. [Accessed 29 05 2021].

[157] T. Kun, “Critical Thinking and Trust: The Art of Decision Making,” in *Ninth International Scientific Web-conference of Scientists and PhD. students or candidates : Trends and Innovations in E-business, Education and Security : TIEES 2021,* Bratislava, The Slovak Society for Economic Informatics, 2021, pp. 73-80.

[158] T. Kun, "The War on Disinformation: The Structure of Trust," in *In: Frédéric, Labarre; George, Niculescu (eds.) Understanding the Contemporary Information Landscape: A Handbook,* Vienna, Landesverteidigungsakademie, 2022, pp. 153-165.

[159] Collins English Dictionary, “PHYSICAL REALITY definition and meaning,” collinsdictionary.com, 2021. [Online]. Available: https://www.collinsdictionary.com/dictionary/english/physical-reality. [Accessed 28 05 2021].

[160] Collins English Dictionary, "FACT Definition and meaning," collinsdictionary.com, 2021. [Online]. Available: https://www.collinsdictionary.com/dictionary/english/fact. [Accessed 28 05 2021].

[161] Collins English Dictionary, “TRUTH Definition and meaning,” collinsdictionary.com, 2021. [Online]. Available: https://www.collinsdictionary.com/dictionary/english/truth. [Accessed 28 05 2021].

[162] Collins English Dictionary, “LIE Definiton and meaning,” collinsdictionary.com, 2021. [Online]. Available: https://www.collinsdictionary.com/dictionary/english/lie. [Accessed 28 05 2021].

[163] Z. Krajnc, Hadtudományi lexikon – Új kötet, Budapest: Ludovika Egyetemi Kiadó, 2020.

[164] H. Kissinger, Diplomácia, Budapest: Panem Könyvkiadó, 2008.

[165] S. S. Costigan and T. Tagarev, “Countering Crime, Hate Speech, and Disinformation in Cyberspace,” *Connections: The Quarterly Journal,* vol. 20, no. 2, pp. 5-8, 2021.

[166] T. Kun, “Események a kibertérben a COVID-19 járvány idején,” *Biztonságtudományi Szemle,* vol. 2, no. 3, pp. 67-76, 2020.

[167] Cylance, “Cylance 2019 Threat Report.pdf,” 25 02 2019. [Online]. Available: https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Cylance-2019-Threat-Report.pdf?_ga=2.194100014.207560192.1557408928-1034628078.1557241850. [Accessed 23 05 2020].

[168] J. K. Cohen, “Ransomware targeting health systems in more 'sophisticated' ways,” 24 01 2020. [Online]. Available: https://www.modernhealthcare.com/cybersecurity/ransomware-targeting-health-systems-more-sophisticated-ways. [Accessed 20 05 2020].

[169] R. Garrett, “Lessons learned from a targeted ransomware attack,” 20 12 2019. [Online]. Available: https://www.modernhealthcare.com/opinion-editorial/lessons-learned-targeted-ransomware-attack. [Accessed 23 05 2020].

[170] Yoroi, “New Cyber Attack Campaign Leverages the COVID-19 Infodemic,” 25 02 2020. [Online]. Available: https://yoroi.company/research/new-cyber-attack-campaign-leverages-the-covid-19-infodemic/. [Accessed 08 04 2020].

[171] Cybersecurity and Infrastructure Security Agency, “CISA INSIGHTS Risk Management for Novel Coronavirus (COVID-19),” 06 03 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus.pdf. [Accessed 21 05 2020].

[172] Nemzeti Kibervédelmi Intézet, “VIGYÁZAT: ÚJABB KORONAVÍRUS MALSPAM KAMPÁNYOKAT FEDEZTEK FEL,” 03 2020. [Online]. Available: https://nki.gov.hu/it-biztonsag/hirek/vigyazat-ujabb-koronavirus-malspam-kampanyokat-fedeztek-fel/. [Accessed 23 05 2020].

[173] P. Paganini, “New Coronavirus-themed malspam campaign delivers FormBook Malware,” 08 03 2020. [Online]. Available: https://securityaffairs.co/wordpress/99156/cyber-crime/coronavirus-spam-campaign.html. [Accessed 14 05 2020].

[174] Reason Labs, “COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report,” 09 03 2020. [Online]. Available: https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/. [Accessed 13 03 2020].

[175] C. Cimpanu, “Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak,” 13 03 2020. [Online]. Available:

https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/?fbclid=IwAR3jE3mDkxTfKSL8UOeGlsqaXsgQ1wN_SekAn7t9EEMpYr5BW-fA9XX3p4M. [Accessed 20 03 2020].

[176] S. Stein and J. Jacobs, “Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak,” 16 03 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response. [Accessed 29 05 2020].

[177] J. Menn, C. Bing, R. Satter and J. Stubbs, “Exclusive: Hackers linked to Iran target WHO staff emails during coronavirus - sources,” 02 04 2020. [Online]. Available: https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC. [Accessed 29 05 2020].

[178] C. Ruhl, “Note to Nations: Stop Hacking Hospitals,” 06 04 2020. [Online]. Available: https://foreignpolicy.com/2020/04/06/coronavirus-cyberattack-stop-hacking-hospitals-cyber-norms/. [Accessed 23 05 2020].

[179] National Cyber Security Centre, “Final Joint Advisory COVID-19 exploited by malicious cyber actors v3.pdf,” 08 04 2020. [Online]. Available: https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf. [Accessed 23 05 2020].

[180] D. Walsh, “Data breach at Beaumont exposes information of 112,000 patients,” 17 04 2020. [Online]. Available: https://www.crainsdetroit.com/health-care/data-breach-beaumont-exposes-information-112000-patients. [Accessed 26 04 2020].

[181] Miniszterelnöki Kabinetiroda, “Orbán Viktor a Kossuth Rádió „Jó reggelt, Magyarország!”című műsorában,” kormany.hu, 17 04 2020. [Online]. Available: https://2015-2019.kormany.hu/hu/a-miniszterelnok/beszedek-publikaciok-interjuk/orban-viktor-a-kossuth-radio-jo-reggelt-magyarorszag-cimu-musoraban-20200417. [Accessed 07 04 2024].

[182] Johns Hopkins University of Medicine, “COVID-19 Map - Johns Hopkins Coronavirus Resource Center,” coronavirus.jhu.edu, 03 10 2023. [Online]. Available: https://coronavirus.jhu.edu/map.html. [Accessed 08 10 2023].

[183] North Atlantic Treaty Organization (NATO), “North Macedonia joins NATO as 30th Ally,” 27 03 2020. [Online]. Available: https://www.nato.int/cps/en/natohq/news_174589.htm.

[184] N. Vlasyan, ““Apricot War” and Beyond: What Recent Events in Russia Tell Us About Armenian Communities,” 17 08 2020. [Online]. Available: https://evnreport.com/politics/apricot-war-and-beyond-what-recent-events-in-russia-tell-us-about-armenian-communities/.

[185] ERMES, “Media and disinformation in the Nagorno-Karabakh conflict and their role in conflict resolution and peacebuilding,” 17 12 2020. [Online]. Available: https://www2.coleurope.eu/system/tdf/uploads/news/event_report_-_media_and_disinformation_in_the_nagorno-karabakh_conflict.pdf?&file=1&type=node&id=draft&force=.

[186] RFE/RL's Azerbaijani Service, “'Know Who The Traitors Are': Azerbaijanis Speaking Out Against The Karabakh War Are Being Targeted On Social Media,” 23 09 2022. [Online]. Available: https://www.rferl.org/a/azerbaijan-traitors-nagorno-karabakh-social-media-campaign/32047849.html.

[187] J. E. Keating, “The AK-47 of the Cell-Phone World,” 03 01 2011. [Online]. Available: https://foreignpolicy.com/2011/01/03/the-ak-47-of-the-cell-phone-world/.

[188] R. E. Denton Jr and B. Voth , Social Fragmentation and the Decline of American Democracy: The End of the Social Contract, Cham: Palgrave Macmillan, 2016, pp. 151-167.

[189] S. Kemp, “Digital 2020: July Global Statshot - DataReportal – Global Digital Insights,” We Are Social & Hootsuite, 21 07 2020. [Online]. Available: https://datareportal.com/reports/digital-2020-july-global-statshot. [Accessed 18 10 2020].

[190] N. Nagy, “Ezek voltak 2021 legfontosabb eseményei a világon,” liner.hu, 31 12 2021. [Online]. Available: https://liner.hu/ezek-voltak-2021-legfontosabb-esemenyei/. [Accessed 07 01 2022].

[191] S. Khattak, “The dual role of social media in Taliban-controlled Afghanistan,” 24 08 2021. [Online]. Available: https://www.trtworld.com/opinion/the-dual-role-of-social-media-in-taliban-controlled-afghanistan-49431.

[192] Department of Defense, “The last American soldier to leave Afghanistan,” 31 08 2021. [Online]. Available: https://twitter.com/DeptofDefense/status/1432492782837501956.

[193] P. Snoj, “A magyar katonák senkit sem hagytak hátra,” 26 08 2021. [Online]. Available: https://honvedelem.hu/hirek/a-magyar-katonak-senkit-sem-hagytak-hatra.html.

[194] M. Seyler, “Single suicide bomber killed US troops and Afghans in ISIS-K attack at Kabul airport, Pentagon finds,” 05 02 2022. [Online]. Available: https://abcnews.go.com/Politics/single-suicide-bomber-killed-us-troops-afghans-isis/story?id=82676604.

[195] J. Besenyő és G. Sinkó, „The social media use of African terrorist organizations: a comparative study of Al-Qaeda in the Islamic Maghreb, Al-Shabaab and Boko Haram,” *Insights into Regional Development 3(3),* pp. 66-78, 2021.

[196] National Institute of Justice, “The Role of Social Media in the Evolution of Al-Qaeda-Inspired Terrorism,” 05 09 2017. [Online]. Available: https://nij.ojp.gov/topics/articles/role-social-media-evolution-al-qaeda-inspired-terrorism.

[197] J. Schroden, “Who is to blame for the collapse of Afghanistan's security forces?,” 24 05 2022. [Online]. Available: https://warontherocks.com/2022/05/who-is-to-blame-for-the-collapse-of-afghanistans-security-forces/.

[198] S. LaGrone, “UPDATED: Pentagon Declares Afghanistan Exodus a Non-Combatant Evacuation as U.S. Marines, Soldiers Mass in Kabul,” 16 08 2021.

[Online]. Available: https://news.usni.org/2021/08/16/pentagon-declares-afghanistan-exodus-a-non-combatant-evacuation-as-u-s-marines-soldiers-mass-in-kabul.

[199] E. Guo and A. W. Ohlheiser, “Afghans are being evacuated via WhatsApp, Google Forms, or by any means possible,” 17 08 2021. [Online]. Available: https://www.technologyreview.com/2021/08/17/1032127/afghanistan-kabul-evacuation-whatsapp-google-forms-security/.

[200] M. M. Balmaceda, “Gas, Oil and the linkages between domestic and foreign policies: The case of Ukraine,” *Europe-Asia Studies*, vol. 50, no. 2, pp. 257-286, 1998.

[201] I. Fülöp, “Ukrajna biztonság- és védelmi politikájáról,” *Új Honvédségi Szemle,* vol. 8, no. 1, pp. 31-38, 1998.

[202] BBC, “Ukraine takes extra Russian gas,” 24 01 2006. [Online]. Available: http://news.bbc.co.uk/2/hi/europe/4642684.stm. [Accessed 28 05 2022].

[203] Reuters, “FACTBOX - 18 countries affected by Russia-Ukraine gas row,” 07 01 2009. [Online]. Available: https://www.reuters.com/article/topNews/idUKTRE5062Q520090107?sp=true. [Accessed 28 05 2022].

[204] L. Cendrowicz, "Russia-Europe Gas Spat Ends — For Now," Time, 09 01 2009. [Online]. Available: https://web.archive.org/web/20090117132153/http://www.time.com/time/world/article/0,8599,1870597,00.html. [Accessed 28 05 2022].

[205] P. Belkin, “The European Union's Energy Security Challenges,” *Connections,* vol. 7, no. 1, pp. 76-102, 2008.

[206] U.S. Energy Information Administration, “16% of natural gas consumed in Europe flows through Ukraine,” 14 03 2014. [Online]. Available: https://www.eia.gov/todayinenergy/detail.php?id=15411. [Accessed 01 06 2022].

[207] T. Kun, “The European Migration Crisis and the aspects of Security Politics,” in *Keleti Károly Faculty of Business and Management*, Budapest, 2018.

[208] T. Kun, “Social Engineering in Europe’s Energy Crisis?,” *Sodobni vojaški izzivi/Contemporary Military Challenges*, vol. 25, no. 1, pp. 73-88, 2023.

[209] North Atlantic Treaty Organization (NATO), „Relations with Ukraine,” nato.int, 07 03 2024. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_37750.htm. [Hozzáférés dátuma: 14 04 2024].

[210] J. Henley, “Finland and Sweden confirm intention to join Nato,” theguardian.com, 15 05 2022. [Online]. Available: https://www.theguardian.com/world/2022/may/15/finland-formally-confirms-intention-to-join-nato-russia. [Accessed 14 04 2024].

[211] Finnish Government, “Finland and Nato,” valtioneuvosto.fi, 27 03 2023. [Online]. Available: https://valtioneuvosto.fi/en/finland-and-nato. [Accessed 14 04 2024].

[212] North Atlantic Treaty Organization (NATO), “Press statement following the meeting between Türkiye, Sweden, and the NATO Secretary General,” nato.int, 10 07 2023. [Online]. Available: https://www.nato.int/cps/en/natohq/news_217147.htm. [Accessed 14 04 2024].

[213] Georgetown University, “What’s Behind Turkey’s Reversal on Sweden’s NATO Bid? A Foreign Policy Professor Answers,” georgetown.edu, 12 07 2023. [Online]. Available: https://www.georgetown.edu/news/whats-behind-turkeys-reversal-on-swedens-nato-bid-a-foreign-policy-professor-answers/. [Accessed 14 04 2024].

[214] Reuters, “Hungary's Orban invites Swedish PM for NATO talks,” reuters.com, 23 01 2024. [Online]. Available: https://www.reuters.com/world/hungarys-orban-invites-swedish-pm-nato-talks-2024-01-23/. [Accessed 14 04 2024].

[215] Atlantic Council, “Experts react: How close is Sweden to joining NATO after the Turkish parliament’s approval?,” atlanticcouncil.org, 23 01 2024. [Online].

Available: https://www.atlanticcouncil.org/blogs/new-atlanticist/experts-react/experts-react-how-close-is-sweden-to-joining-nato-after-the-turkish-parliaments-approval/. [Accessed 14 04 2024].

[216] Government Offices of Sweden, “Sweden in NATO,” government.se, 07 03 2024. [Online]. Available: https://www.government.se/government-policy/sweden-in-nato/. [Accessed 14 04 2024].

[217] Deutsche Welle, “Germany commits €100 billion to defense spending,” 27 02 2022. [Online]. Available: https://www.dw.com/en/germany-commits-100-billion-to-defense-spending/a-60933724.

[218] European Commission, “REPowerEU: Joint European action for more affordable, secure and sustainable energy,” 08 03 2022. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1511.

[219] European Commission, “EU-US LNG TRADE,” 02 02 2022. [Online]. Available: https://energy.ec.europa.eu/system/files/2022-02/EU-US_LNG_2022_2.pdf. [Accessed 01 06 2022].

[220] B. Sieniawski, “Former minister’s Nord Stream sabotage tweet causes uproar in Poland,” 30 09 2022. [Online]. Available: https://www.euractiv.com/section/energy-environment/news/former-ministers-nord-stream-sabotage-tweet-causes-uproar-in-poland/.

[221] J. Pennington, S. Jeong and H. Ritchie, “Kremlin claims Nord Stream sabotage reports are part of a “misinformation campaign”,” 08 03 2023. [Online]. Available: https://egyptindependent.com/kremlin-claims-nord-stream-sabotage-reports-are-part-of-a-misinformation-campaign/.

[222] UN Security Council, “Security Council Rejects Draft Resolution Establishing Commission to Investigate Sabotage of Nord Stream Pipeline,” 27 03 2023. [Online]. Available: https://press.un.org/en/2023/sc15243.doc.htm.

[223] Infostart, “Dánia segített Amerikának kémkedni: Angela Merkelt is lehallgatták,” 31 05 2021. [Online]. Available:

https://infostart.hu/kulfold/2021/05/31/dania-segitett-amerikanak-kemkedni-angela-merkelt-is-lehallgattak.

[224] J. E. Barnes, H. Cooper, T. Gibbons-Neff, M. Schwirtz and E. Schmitt, “Leaked Documents Reveal Depth of U.S. Spy Efforts and Russia’s Military Struggles,” 08 04 2023. [Online]. Available: https://www.nytimes.com/2023/04/08/us/politics/leaked-documents-russia-ukraine-war.html.

[225] B. Ellis, S. Glover, J. Winter and M. Hicken, “Man arrested in connection with intel leak: ‘Actions speak louder than words’,” 14 04 2023. [Online]. Available: https://edition.cnn.com/2023/04/14/politics/jack-teixeira-profile/index.html.

[226] Portfolio, “Kibertámadás tette elérhetetlenné az OTP netbankját,” portfolio.hu, 13 05 2023. [Online]. Available: https://www.portfolio.hu/bank/20230513/kibertamadas-tette-elerhetetlenne-az-otp-netbankjat-614956. [Accessed 16 10 2023].

[227] UN OCHA, “Joint Coordination Centre opens in Istanbul to facilitate safe export of commercial foodstuffs and fertilizers from Ukrainian ports,” 27 07 2022. [Online]. Available: https://reliefweb.int/report/turkiye/joint-coordination-centre-opens-istanbul-facilitate-safe-export-commercial-foodstuffs-and-fertilizers-ukrainian-ports. [Accessed 09 11 2023].

[228] United Nations, “Black Sea Grain Initiative,” 2023. [Online]. Available: https://www.un.org/en/black-sea-grain-initiative. [Accessed 26 11 2023].

[229] Aljazeera, “Russia-Ukraine Black Sea grain deal: All you need to know,” 17 07 2023. [Online]. Available: https://www.aljazeera.com/news/2023/7/17/russia-ukraine-black-sea-grain-deal-all-you-need-to-know. [Accessed 26 11 2023].

[230] N. Camut, “African Union calls on Russia to reinstate Ukrainian grain deal,” 23 07 2023. [Online]. Available: https://www.politico.eu/article/african-union-calls-to-reinstate-the-ukrainian-grain-deal/. [Accessed 09 11 2023].

[231] European Council, “Infographic - Ukrainian grain exports explained,” 11 10 2023. [Online]. Available:

https://www.consilium.europa.eu/en/infographics/ukrainian-grain-exports-explained/. [Accessed 26 11 2023].

[232] J. Heintz, E. M. Lederer, C. Megerian and R. Santana, “Putin promises no-cost Russian grain shipments to 6 African countries,” 27 07 2023. [Online]. Available: https://apnews.com/article/russia-putin-africa-summit-food-crisis-de317f5075d4b1719ade457f4eabbf82. [Accessed 29 11 2023].

[233] Reuters, “Russia says first free grain shipments to Africa are on their way,” 17 11 2023. [Online]. Available: https://www.reuters.com/markets/commodities/russia-begins-supplying-free-grain-african-countries-agriculture-minister-2023-11-17/. [Accessed 29 11 2023].

[234] CGTN, “Russia to donate more wheat to Africa by year-end,” 03 11 2023. [Online]. Available: https://newsaf.cgtn.com/news/2023-11-03/Russia-to-donate-more-wheat-to-Africa-by-year-end-1opD4tc93Wg/index.html. [Accessed 29 11 2023].

# RÖVIDÍTÉSJEGYZÉK

| Idegen nyelvi (angol) megnevezés | Magyar nyelvi meghatározás |
|---|---|
| NATO – North Atlantic Treaty Organization | Észak-atlanti Szerződés Szervezete |
| PFP – Partnership for Peace | Partnerség a békéért, Békepartnerség |
| INFO OPS – Information Operations | információs műveletek |
| OPSEC – Operational Security | műveleti biztonság |
| MILDEC – Military Deception | katonai megtévesztés |
| PSYOPS – Psychological Operations | pszichológiai műveletek |
| PD – Physical Destruction | fizikai pusztítás |
| EW – Electronic Warfare | elektronikai hadviselés |
| CNO - Computer Network Operations | számítógép-hálózati műveletek |
| PSYWAR - Psychological Warfare | lélektani hadviselés |
| PA – Public Affairs | közügyek |
| IO – Information Objectives | információs célok |
| OPLAN – operation plan | operációs terv |
| USIA – United States Information Agency | az Egyesült Államok Információs Ügynöksége |
| CIA – Central Intelligence Agency | Központi Hírszerző Ügynökség |
| ENISA – the European Union's Agency for Cybersecurity | Az Európai Unió Kiberbiztonsági Ügynöksége |
| ICT – Information and Communications Technology | Információ- és Kommunikációtechnológia |
| UN – United Nations | ENSZ - Egyesült Nemzetek Szervezete |
| NIS – Network and Information Security | Hálózati- és információbiztonság |
| CyCLONE - European Cyber Crises Liaison Organisation Network | Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata |
| GDPR – General Data Protection Regulation | Általános Adatvédelmi Rendelet |

| | |
|---|---|
| AI – Artificial Intelligence | mesterséges intelligencia |
| DoS – Denial-of-service | szolgáltatás megtagadás |
| DDoS – Distributed denial-of-service | elosztott szolgáltatás-megtagadás |
| MitM – Man-in-the-middle | beékelődéses támadás |
| IP – Internet Protocol | internetprotokoll |
| DNS – Domain Name System | tartománynévrendszer |
| TLD – top-level domain | Legfelső szintű tartomány |
| HTTP – HyperText Transfer Protocol | hiperszöveg átviteli protokoll |
| Wi-Fi – Wireless Fidelity | vezeték nélküli megbízhatóság |
| SSL – Secure Sockets Layers | SSL protokoll |
| VoIP – Voice over Internet Protocol | internetprotokoll feletti hangátvitel |
| BEC – Business Email Compromise | üzleti elektronikus levelezés kompromittálása |
| MFA – Multi-Factor Authentication | többtényezős azonosítás |
| SQLi – Standard Query Language injection | SQL befecskendezés |
| XSS – Cross Site Scripting | weboldalak közötti szkriptelés |
| TTP – Tactics Techniques and Procedures | taktikák, technikák és eljárások |
| MaaS – Malware as a Service | Kártevő szoftver, mint szolgáltatás |
| SIS – Safety Instrumented System | biztonsági műszeres rendszer |
| HUMINT – Human Intelligence | emberi intelligencia |
| UGC – User Generated Content | felhasználók által generált tartalom |
| DLL – Dynamic Link Library | dinamikus csatolású könyvtár |
| MAU – Monthly Active Users | Havi aktív felhasználók száma |

# ÁBRAJEGYZÉK