

36. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2023. április 18-20.
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar

**Infokommunikációs technológiák térhódítása
nemzetbiztonsági szemmel egykor és ma**

Jelige: *Sauron szeme*

Pályamunka lezárásának időpontja: 2021.04.25.

2023.

I. Bevezetés

1) A témakör vizsgálatának főbb célja

A korszerű kommunikációs technológiák és az azokra épülő eszközök használata mindennapjaink részévé vált. Ezek alapvetően a nemzetközi üzleti szférában, nemzetközi szabványok mentén jönnek létre, mégis – a nemzetközi példákból jól látható – hogy a külföldi technológiák használata gyakran vet fel biztonsági, nemzetbiztonsági kérdéseket. Így volt ez akár a hidegháború időszakában, de mindez igaz napjainkban is. A kérdéskör mentén így egyik oldalról a nemzeti, illetve szövetségi rendszerhez kapcsolódó technikai eszközök előnybe részesítése (és így a nagyobb vélt biztonság), másrésről a megállíthatatlanul globalizálódó infokommunikációs környezet előnyeinek és lehetőségeinek kihasználása áll szembe.

A témakör rendkívül összetett, hiszen például amíg rendszerváltozást megelőző időszakban a COCOM lista fennállásának időszakában a saját/szövetségi szinten fejlesztett, gyártott kommunikációs eszközök preferálása mellett a technológiai hírszerzés fontos irányként jelent meg, addig napjaink multipoláris világában a fejlett technológiák a nemzetbiztonsági szempontokon túlmutatva, mindez már a nagypolitika színterére került.

2) Témaválasztás indoklása

Elsősorban az aktuális specializáció választásom végett szerettem volna a témát kifejteni, melyben az infokommunikációs technológiák és a biztonság összefüggéseit kívánom bemutatni, hiszen amellett, hogy a korszerű eszközök számos módon jobba teszik életünket, számos veszélyt is hordozhatnak. Gondoljunk csak az adataink védelmére, vagy akár például nem kellően biztonságos technológiák alkalmazására.

Populáris tekintetben is fontosnak tartottam kifejtését, a téma feldolgozását, mivel a dolgozatomban felhívhatom a figyelmet azokra a veszélyekre is, melyekre nem sokan gondolnának. Ezzel kiegészítve a kronologikusan a főbb nemzetbiztonságot is érintő technológiai botrányokat mutathatnám be, amelyek példával szolgálhatnak az olvasók számára. Ennek tárgyalása során a jelenleg körülöttünk lévő platformok/eszközök kockázata is szóba kerül.

3) A kérdéskör aktualitása

A dolgozatban ismertetett technológiai botrányok rávilágítják a figyelmet annak a veszélyére, hiszen a társadalmunk nem foglalkozik azokkal a közvetlenül nem látható „technológiai veszélyekkel, amelyek láthatatlanul léphetnek bele az életébe.

Egyre fontosabb vált a technológiák jelentősége, hiszen a nemzetközi hadszíntér körében megjelent a kibertér is, melyben a legújabb technológiai fejlesztések már meghatározóak. Ugyanakkor fontos megemlíteni azt is, amelyet a dolgozatom végén is kifejtettem, hogy az idő előrehaladtával a közösségi platformok jelentik az egyik legnagyobb fenyegetést. Ezzel összekapcsolva a múltbeli technológiai lehallgatások témakörét láthatjuk, hogy a mai már sokkal modernebb és észrevehetetlenebb hatásként van jelen.

4) Kutatási módszer megválasztása

Témaválasztásomhoz kapcsolódóan kutatási módszerként a szakirodalmak feldolgozását is alkalmaztam. A nyomtatott formában elérhető hazai szakirodalmak mellett, a témakör aktualitásának megfelelően elektronikus formában elérhető magyar és idegen nyelvű forrásokat is felhasználtam és a nemzetközi szintéren látható folyamatokat vázoltam.

II. Téma kifejtése

1) A hidegháború időszakának sajátosságai, jellemzői

A második világháború utáni időszakot nevezzük hidegháborúnak, 1947-től kezdődött és a 1980-90-es évek fordulójáig húzódott el. Kétpólusú világszemléletről beszélhetünk, a két nagyhatalom (USA és a Szovjetunió) szembenállásáról. Globális kiterjedésű ideológiai háború volt jelen. A szocialista blokk országaira jellemző volt a „szovjetizálás” és a szovjet típusú totális állam kiépítése (pl. államosítás, egypárti diktatúra, tervgazdálkodás), és ide tartozott hazánk is. A nyugati övezet pedig, jóval fejlettebb és liberális szemléletű volt demokratikus viszonyaival. Katonai szempontból nyugati oldalon az 1949-ben létrejött NATO (Észak Atlanti Szerződés Szervezete), a keleti blokk országaiban pedig a Varsói Szerződés (1955) katonai szövetsége volt jelen.

A szembenállás egyik fontos momentuma az űrverseny volt, melynek kifejlesztését és a szükséges technikai tudást, a technológiai fejlesztések egyik mérföldkövének, és az internet létrejöttének előzményeként is tekinthetjük.

A technikai-fejlesztési verseny is nagy szerepet játszott a szemben álló felek mögöttes titkosszolgálati küzdelmeiben. A fejlett fél mindig is nyugat volt, de a keleti blokk is felvette a lépést velük, felhasználta a rendelkezésre álló erőforrásokat, és a megfelelő ismeretsséggel rendelkező szakembereket is toborozta, alkalmazta.

Hazai tekintetben is érezhető volt a változás, hiszen az 1950-60-as évek felé haladva az állambiztonsági szféra a technikai-kutatási területekre szintén nagy hangsúlyt fektetett. A legnagyobb hatást az európai szociális országokkal kialakított állambiztonsági témájú

bilaterális és multilaterális együttműködések jelentették. Ez tartalmazta a kutatási-fejlesztési munkálatok összehangolását, a párhuzamosságok elkerülését, a tapasztalatok megosztását és az új, korszerű eszközök használatát. (Az innovatív eszközök használatát azért is érdemes kiemelni, hiszen az előzőleg említett COCOM-lista miatt a nyugati hatalmak találmányait nem alkalmazhatták, így saját fejlesztésekre volt szükség, és olyan együttműködésekre, ahol a keleti blokk tagjai megoszthatták új vívmányaikat.)¹

A második világháború alatt az amerikai hadsereg és a haditengerészet független külföldi SIGINT kapcsolatokat alakított ki a britekkel, valamint Kanada, Ausztrália és Új-Zéland együttműködésével. Ezek a kapcsolatok az évtizedek során tovább folytatódtak. A világháború hevében kovácsolt, évtizedes bizalom és csapatmunka által csillapított kötelékek továbbra is nélkülözhetetlenek voltak a jövőbeni hírszerzési sikerek szempontjából.

1946. március 5-én, a BRUSA (ma UKUSA néven ismert) megállapodás aláírása megerősítette az Egyesült Királyság és az Egyesült Államok közötti létfontosságú második világháborús együttműködést. A következő 10 évben elkészítették és átdolgozták a megállapodás függelégeit. Ezek a függelékek és mellékleteik részletesen bemutatják a két partner közötti munkakapcsolatot, és a többi felekkel (Ausztrália, Kanada és Új-Zéland) is megállapodnak.²

a) Echelon-botrány

Az Echelon nevezetű lehallgatási botrány az angol újságíró Duncan Campbell-től származik. Cheshire településén vett észre egy különös építményt, mely egy gabonasilóra asszociált, hiszen több méter magas betontornyokat foglalt magába. Ezzel az volt a probléma, hogy a tetőjükön antennák álltak.



1., 2., ábra: Cheshire településén látható lehallgató tornyok.; Forrás: A rádiótechnika évkönyve – 2002: Horváth Lajos: A világ legnagyobb fülei...

¹ Dobák Imre: Betekintés az állambiztonság 1960-70-es évei nemzetközi technikai kutatás-fejlesztési folyamatainak szerkezetébe

² <https://www.nsa.gov/news-features/declassified-documents/ukusa/>; letöltve: 2020.10.16.; fordította: szerző

Valamennyi hasonló feladattal: a legkorszerűbb berendezéseik segítségével, képesek voltak lehallgatni a rádió és telefonvonalakat, elolvasni a fax és e-mail forgalmazásokat. A vizsgálat során az is kiderült, hogy a globális NSA lehallgató rendszernek a létrehozója és üzemeltetője a CIA egyik legfontosabb részlege, a US National Security Agency (NSA) és kódneve Echelon. A rendszer segítségével folyamatosan és egyidejűleg több ezer összeköttetés megfigyelése volt lehetséges.³

Az 1997-es London Telegraph cikkjét találtam az akkori szemmel a legkézenfekvőnek ezzel a témakörrel kapcsolatban. Ezt a következőkben szeretném kifejtetni és ismertetni az ECHELON kapcsán.

Az Európai Bizottság jelentésében figyelmeztették először a polgárokat, hogy az Egyesült Államok kiterjedt hálózatot fejlesztett ki kémkedés céljából. A „Assessing the Technologies of Political Control” című jelentést az Európai Parlament Állampolgári Jogi Bizottsága készítette, amely részleteket tartalmaz egy amerikai irányítású hírszerző állomások hálózatáról, amelyek brit földön és szerte a világon rutinszerűen és válogatás nélkül számtalan telefon-, fax- és e-mail üzenetet figyelnek. Ez a jelentés megrázóan érintette a társadalmat, hiszen az ilyesfajta technológia bizonyítékai anekdotikusnak bizonyultak. Az ECHELON rendszer része az UKUSA rendszernek, de ellentétben a hidegháború alatt kifejlesztett elektronikus kémrendszerekkel, az ECHELON elsősorban nem katonai célpontok számára készült: kormányok, szervezetek és vállalkozások számára is a világ összes országában.

Az ECHELON rendszer úgy működik, hogy válogatás nélkül tárolja a nagy mennyiségű kommunikációt, majd a MEMEX-hez⁴ hasonló mesterséges intelligencia-segédeszközök segítségével kulcsszavak alapján szelektálja ki az értékeseket. Számos ország szótárait használja, melyek tartalmazzák a legfontosabb kulcsszavakat. A 1990-es évek végén az elektronikus hírközlés nyomon követése világszerte futótűzként terjedt a nemzetbiztonsági szolgálatok között, megjelent a kulcsszavas keresés automatikus alkalmazása különböző telekommunikációs hálózatokon, mely hatalmas áttörést jelentett a technológiában.

Néhány évvel korábban még az NSA létezése titok volt, alapokmánya és kötelességeinek említése titkos volt. Az egyik bázisa, a Menwith Hill, a világ legnagyobb kémállomásává vált.

³ https://www.thelivingmoon.com/45jack_files/03files/ECHELON_Menwith_Hill.html; 2020.10.17.; fordította: szerző

⁴ A DARPA (Defence Advanced Research Projects Agency) által kifejlesztett szoftver, a memória és az index kombinációja. Lehetővé teszi a felhasználók számára, hogy gyorsan és rugalmasan keressenek hatalmas mennyiségű információt, és hatékonyabban nyerhessenek belőle fontos adatokat. Az internet elődjének is nevezik; <https://www.darpa.mil/program/memex>; letöltve: 2021.03.10.; fordította szerző

Képesek voltak hallgatni a kommunikációs spektrum hatalmas darabjait egész Európában és a régi Szovjetunióban egyaránt.⁵

b) Five Eyes

„A FIORC a meglévő Five Eyes partnerség szellemében jött létre, az a hírszerző szövetség, amely Ausztráliát, Kanadát, Új-Zélandot, az Egyesült Királyságot és az Egyesült Államokat foglalja magába. A FIORC az Five Eyes országának következő, nem politikai hírszerzési felügyeleti, felülvizsgálati és biztonsági egységeiből áll:

- Ausztrália hírszerzési és biztonsági főfelügyelőjének hivatala
- Kanada Nemzetbiztonsági és Hírszerző Felülvizsgálati Ügynöksége
- Kanada hírszerzési biztosának irodája
- A hírszerzési biztos és az Új-Zéland hírszerzési és biztonsági főfelügyelőjének irodája
- Az Egyesült Királyság nyomozói hatáskörrel foglalkozó biztosának irodája
- Az Egyesült Államok hírszerzési közösségének főfelügyelőjének hivatala” forrás: <https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc>; fordította: szerző

A Tanács tagjai:

- Véleményt cserélnek a kölcsönös érdeklődésre számot tartó és aggályos kérdésekről;
- Összehasonlítják a felülvizsgálat és a felügyelet módszertanával kapcsolatos bevált gyakorlatokat;
- Feltárják azokat a területeket, ahol adott esetben megengedett az együttműködés a felülvizsgálatok és az eredmények megosztása terén;
- Fenntartják a kapcsolatot a politikai irodákkal, a felügyeleti és felülvizsgálati bizottságokkal, valamint adott esetben az Five Eyes-hoz nem tartozó országokkal.⁶

Összességében: az UKUSA-nak és a Five Eyes-nak is az volt a célja, hogy az embereket lehallgassák, mivel ez törvénytelen lett volna a saját országukra nézve, ezért gyakran látható együttműködés másik féllel, hogy egymás területeire hivatkozva biztosíthassák a lehallgatást.

⁵ London Telegraph, Tuesday 16 December 1997, Issue 936 (Spies like US): Duncan Campbell; fordította: szerző

⁶ <https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc>; letöltve: 2020.10.18.; fordította: szerző

c) COCOM-lista

A COCOM-listát azért is szerettem volna külön kiemelni, mivel nagyban befolyásolta a hidegháború időszaka alatt megalakuló innovatív technikákat és annak eszközeit. A COCOM-lista COCOM-nak (Coordinating Committee for Multilateral Export Controls) lényegében egy olyan együttműködés, amely tiltotta a csúcstechnológiák exportját a keleti tömb országaiban. A COCOM-listának 17 tagországa volt:

Ausztrália, Belgium, Dánia, az Egyesült Királyság, Franciaország, Görögország, Hollandia, Japán, Kanada, Luxemburg, a Német Szövetségi Köztársaság, Norvégia, Olaszország, Portugália, Spanyolország, Törökország és az USA.

Ez a fegyverkezési verseny lassítására szolgált a KGST országokban és Kínában, hiszen ezáltal a listán szereplő termékek nem juthattak el az adott országokba, így lemaradtak a nyugati fejlesztésektől.

A COCOM-lista például olyan termékek beáramlását tiltotta meg mint, az IBM PC, az Ethernet, az Apple Macintosh, a digitális telefonközpontok vagy akár a mobiltelefon-technológia.

Viszont a nyugati hatalmaknak is hatalmas gazdasági kárt okozott ennek a fenntartása, hiszen egy amerikai tanulmány szerint⁷ 9,3 milliárd dollárba került, ugyanakkor rengeteg ember veszítette el a munkáját 1985-ben.

Magyarországgal szemben a 1990-ben enyhítették, majd 1992-ben teljesen megszüntették. A szövetség 1994-ben oszlott fel, majd később a wassenaari egyezmény szolgálta a volt szövetség érdekeit, mely országai között hazánk is szerepelt.⁸

2) Kémbostrányok, technológiai incidensek/konfliktusok bemutatása a hidegháború időszakától napjainkig

a) U-2 incidens és néhány jelentősebb esemény

A Lockheed cég bázisa a kaliforniai Mojave-sivatagban adott helyet amerikai szupertitkos repülőgépeinek építésére és tesztelésére.

1954-ben CIA ügynökök érkeztek a telephelyre, egy titkos küldetés végett, melynek a neve; Wild Cherry küldetés volt. Ahhoz, hogy be tudjanak tekinteni a vasfüggöny mögé, a legjobb módszernek a fotografikus légifelderítést tekintették.

⁷ Hirsch, Steve. „Export Control Policy”, The Multinational Monitor; letöltve: 2021.03.19.

⁸ <https://www.origo.hu/gazdasag/20190125-penz-a-lelke-cocom-lista.html>; letöltve: 2020.09.10.

Műszaki hírszerzésre volt szükség, tehát nagy magasságok elérésére képes repülőgépekre, melyek a keleti blokk területe felé repülhettek és büntetlenül fényképezni tudtak a szovjet légvédelmi hatóságán kívül.

Az amerikai légierő úgy alakította át a gépeket, hogy bombázókat vásárolt kivették a bomba kamrát és helyükre kamerákat telepítettek.

A légierő átalakított bombázói azonban nem feleltek meg a CIA igényeinek, ezért a haditengerészethez fordultak a további megvalósításban. A legmegfelelőbb kivitelezést a Lockheed P-2 Neptune-ben találták meg, Mivel ezeket a gépeket mélyrepülése tervezték és akár 10 méter alatt is képesek voltak a megfelelő feladatot ellátni. 1958-ban jelent meg az első sikeres kísérlet, és a skyhook szerkezet a legújabb innovációt jelentette a kémkedés történetében. A repülőgép elején levő kampók segítségével az idegen területen lévő személyeket, jelen esetben kémeket fel tudták emelni a földről (vagy a vízből) a levegőbe. Az első éles gyakorlat a "Hidegláb hadművelet" során, két ügynököt dobtak le egy elhagyott szovjet állomásra, és onnan pár nap alatt tudtak szerezni dokumentumokat, rejtjelkulcsokat, felszereléseket.

A Neptune-nel való akciók nem voltak túl hosszú életűek, mert veszélybe sodorta volna a haditengerészet gépeit, az ellenséges területeken.

Így a későbbiekben radar gyakorló gépként kiadott repülőket bocsátott ki a CIA és az amerikai légierő, ez első kettőt a kelet-német Wiesbadenbe küldték, és ezzel kezdődtek meg a felderítő küldetések Kelet-Európában. Ezek az akciók 12-13 órát is igénybe vehettek. A Wild Cherry küldetések annyira kompromittálóak voltak azonban a későbbiekben, hogy 1963-ban leállították őket.

Az egyre jobban fejlődő kínai technológia is felkeltette az érdeklődését a nyugati hatalmaknak, ezért a következő célpontnak őket tűzték ki. 1958-64 között több mint 80 behatolás történt a kínai légtérbe.

1952-ben az amerikai hírszerzés tudomást szerzett egy titkos rakéta kilövő bázisról a Szovjetunióban.

A bázis elsődleges feladata az volt, hogy embert juttassanak az űrbe, továbbá ez volt a szovjetek fő ballisztikus rakéta kutatóbázisa. Valószínű ez volt a legfontosabb cél a katonai hírszerzés számára, elismerve, hogy a legnagyobb fenyegetést az orosz fejlesztés jelenti. Az Amerikai Egyesült Államok és a NATO megpróbált fotókat szerezni a létesítményről. A fotók értéke felbecsülhetetlen volt, mert csak általuk tudhatta meg a hírszerzés pontosan, milyen messzire jutottak a szovjetek a nagy hatótávolságú rakéták fejlesztésében. Mivel az amerikai légierőnek

nem volt megfelelő repülőgépe az akció végrehajtásához, így a brit légierő adott nekik, melynek neve, English Electric Canberra.

1953-ban kezdték el a kamerával felszerelt Canberra géppel a küldetést a szovjet rakétabázis ellen. Az ellenség észrevette a behatoló kémrepülőgépet és válaszul vadászgépeket küldtek rá. Ennek ellenére a Canberra több száz részletes fotóval tudott szolgálni, megsérült ugyan, de sikeresen le tudott szállni Iránban.

A sikeres akció után az amerikaiak is kifejlesztették a saját kémrepülőjüket, melynek a neve, RB-57.

Kelly Johnson tervezte meg a U-2 sugárhajtású repülőgépet.

Az U-2 mindent tudott, amire a küldetés végrehajtásához szükség volt. 21 000 méter felett repült és lefotózta a Szovjetunió számos területét. Az első kémrepülés a Szovjetunió felett 1956-ban történik. Ezzel egyidejűleg az RB-57-esek is folytattak a kémtevékenységet Kína, és a Szovjetunió felett egyaránt.

A kínai légvédelem az 1950-es évek elkezdte lelőni a légterében repülő RB-57-eseket és végül a U-2-kat is, valamint a szovjetek sem nézték tétlenül, hogy az amerikai és a NATO kémrepülőgépei fürkészik légterüket, ezért az oroszok elindították a saját felderítési programjukat. Példaként említhető, hogy pl. Európában a szovjet gépek letértek a kijelölt légifolyosókból, hogy Nyugat-Németországban NATO bázisokat keressenek. Még a szovjet kereskedelmi repülőjáratok is gyakran titkos kamerákat hordoztak.

1960. május 1-jén egy CIA U-2 gép tűnt el a Szovjetunió feletti akció közben. A pilóta Francise Gary Powers, akinek gépét 21 ezer méter magasságban egy szovjet SA-2-es rakéta találja el, mindössze hat hónappal azután, hogy a taiwani Wang százados RB-57 D gépét lelőtték. Powerst perbe fogták és kémkedés vádjával 10 évre elítélték. Viszont van egy váratlan fordulat a küldetésével kapcsolatban. Az U-2 gépmaradványai a rakétatalálat után több 100 km széles területen szóródtak szét, a szovjet felsővezetés hatalmas kutatást indít, hogy a lezuhant gép minden egyes darabját megtalálják és a titkait feltárják, szovjet katonák ezrei vesznek részt a kutatásban.

Az U-2 darabjait összegyűjtötték, és alapos tanulmányozásnak vetették alá, Hruscsov elrendelte, hogy az orosz légiipar gyártson másolatot az amerikai kémrepülőgépről. 1961-ben a gép törzse készen is állt. 1962-ben azonban az U-2 “másolását” a szovjetek beszüntetették.⁹

⁹ History TV: A szuperhatalmak titkos repülőgépe: Kémrepülőgépek

b) Profumo-ügy

Az ügy első kiindulópontja, 1961. július 8-ára tehető, amikor John Profumo, brit államtitkár, egy partin vett részt Lord Astor vidéki birtokán. Ekkor ismerkedett meg a 19 éves Christine Keeler táncosnővel, aki több társadalmi osztályban is megfordult. A partin jelen volt továbbá Eugene (Jevgenyij) Ivanov, orosz katonai attasé, aki szintén szoros kapcsolatot tartott Christine-nel. Pletykák kezdtek el terjedni Profumo és Keeler között, amik a Parlamentig is eljutottak. Később ellenkező bizonyítékok kerültek napvilágra, amely lebuktatta a hadügyminisztert, így későbbi mély megbánással beismerte, hogy megtévesztette az alsóházat. A botrány döntő jelentőségű volt a választásokban, így az ellenzéki Munkáspárt legyőzte a konzervatívokat. John Profumo 1963. június 4-én lemondott posztjáról.¹⁰

A botrány elszenvedője Stephen Ward volt. Híres oszteopata, akinek fontos barátai voltak, köztük John Profumo, Lord Astor és Jevgenyij Ivanov. Az MI5 és az MI6 használta ki a kapcsolatait arra, hogy információkat szolgáltasson a társadalmi összeköttetéseiről, és tudott arról is, hogy megpróbálták rávenni Ivanovot arra, hogy kettős ügynök legyen. Ezen információk birtokában keresztűzbe került, és mentálisan nem bírta ezt elviselni, így 1963-ban öngyilkosságot követett el.

Jevgenyij, Christine-nel való kapcsolatát kihasználva megpróbált a brit államtitkok közelébe férkőzni.¹¹

A botrány lekötötte a brit közvélemény figyelmét és hiteltelenné tette a kormányt. Jonathan Haslam professzor is megerősítette a BBC History magazinnak adott nyilatkozatában, kiemelve, hogy *„az újonnan feltárt bizonyítékok szerint a botrány nyomán, a hidegháború tetőpontján az Egyesült Államok bizalma megrendült Nagy-Britannia biztonságpolitikai képességeiben. Washingtonban nagyon dühösek lettek, hogy úgymond a britek inkompetenciája miatt az Egyesült Államok jelentős nemzetbiztonsági kockázatnak lett kitéve.”*¹²

c) Watergate-botrány

Az incidens kezdeti időpontja 1972. június 17-re tehető, amikor több betörőt is letartoztattak. Az elkövetők Richard Nixon újraválasztási kampánya alatt hallgatták le a telefonokat és

¹⁰ <https://www.britannica.com/event/Profumo-affair>; Profumo affair British political scandal: Robert W. Pringle letöltve: 2021.03.10.; fordította: szerző

¹¹ <https://www.historyextra.com/period/20th-century/real-history-profumo-affair-christine-keeler-who-what-happened/>; Sex, lies and spies: the real history of the Profumo Affair: Anna Harris; letöltve: 2020.03.12.; fordította: szerző.

¹² https://index.hu/tudomany/tortenelem/2015/10/28/oriasi_karokat_okozott_a_hideghaborus_szexbotrany/; letöltve: 2021.03.12.

dokumentumokat is loptak. Carl Bernstein és Bob Woodward újságírók, a betörés után kezdték el a nyomozást, majd felfedték Nixon, volt amerikai elnök, szerepét is a bűntettben.

A botrány előzménye volt, hogy az Egyesült Államok a vietnámi háborúba keveredett, így az ország mélyen megosztott volt. Az elnöki kampány részeként került sor arra, hogy illegális információkat gyűjtsenek. Amikor betörték a Fehér Házba, már megvolt a gyanúja, hogy Nixon emberei lehettek, de ezt felvetést a szőnyeg alá söpörték. A nagyobb bűncselekménye Nixonnak az volt, mikor ezt a CIA-nak is felvetette, hogy kapják el a tetteseket, így ez visszaéléssel bizonyult az igazságszolgáltatással szemben. Ekkor már egyre több ember gyanakodott az elnökre, köztük Bob Woodward és Carl Bernstein, a Washington Post újságírói. Úgynevezett „Deep Throat” névtelen bejelentő segítette őket a munkájukban. (Aki 30 évvel később, 2005-ben fedte fel valódi énjét, az FBI volt igazgatóhelyettese, William Mark Felt állt az álnév mögött.¹³) A Fehér Ház tanácsosa, John Dean tanúskodott az elnök bűncselekményeiről, köztük a rögzített beszélgetésekről is, amelyeket az Ovális Irodában vettek fel, ezek a szalagok az ügyészség szerint, elegek lettek volna az elnök lebuktatására. Ebből az ügyből kiinduló lavinát „A szombat esti mézszárlásnak” is nevezik. Archibald Cox, különleges ügyész tovább követelte a kazettákat, ezt Nixon megelégedve elbocsátotta, így az Igazságügyi Minisztérium több képviselője is lemondott tiltakozásképpen, ezután az elnök a kazetták egy részét átadta az ügyészségnek. 1974 elején kezdett el kibontakozni a botrány, az esküdtszék vádat emelt Nixon segédje ellen, hiszen az elnök gyanúsítását nem lehetett egyelőre megtenni. A Legfelsőbb Bíróság kötelezte Nixont a kazetták kiadására (ezt augusztus 5-én tette meg), ezután felelősségre vonták, az igazságszolgáltatás akadályozásáért, a hatalommal való visszaélés és az Alkotmány megsértéséért. A kiadás után tagadhatatlan bizonyítékot szolgáltatott a Watergate-bűncselekményben való részvételben, így augusztus 8-án lemondott elnöki posztjáról. A posztját betöltő, Gerald Ford, megkegyelmezett Nixonnak, így nem került börtönbe.¹⁴

d) Toshiba botrány

A Szovjetunió a COCOM-lista rendszerének kijátszására és kiépülő szerve a KGB „X-vonala” volt. Az említett szovjet titkosszolgálat volt felelős a technológiai és tudományos hírszerzésért, feladataihoz sorolható, a COCOM-listán szereplő tiltott termékek megrendelése, majd leszállítása, és fedőcégek alapítása a nyugati területeken. Viszont ennek a hátránya az volt, hogy egy egész országot ellátó megrendelést nem biztosíthattak.

¹³ <https://www.history.com/news/watergate-deep-throat-fbi-informant-nixon>; How ‘Deep Throat’ Took Down Nixon From Inside the FBI: Annette McDermott; letöltve: 2021.03.09.; fordította: szerző

¹⁴ <https://www.history.com/topics/1970s/watergate>; Watergate Scandal; letöltve: 2021.03.09.; fordította: szerző

A Toshiba 1982 és 1984 között a Kongsberg cég által tudott CNC szerszámgépeket eladni az akkori Szovjetunióknak, amelyek számítógép-vezérlésűek voltak, így a szovjeteknek lehetőségük volt tengeralattjáró-hajócsavarok gyártását. Ennek köszönhetően az 1980-as években a propellerzaj jelentősen lecsökkent, így a nyugati államok jóval kevesebb jelentést kaphattak az ellenség mivoltáról, és nem tudták őket követni.

A jogalkotók szerint a Toshiba mindent megtett, hogy eltitkolja az érzékeny berendezések értékesítését a hatóságok előtt. Megváltoztatta a gép nevét, további változtatásokat hajtott végre, és egy új gépet adott be exportengedélyekre.

Ennek következményeképp az amerikai szenátus kettőtől öt évig terjedően megtiltotta a Toshiba termékek behozatalát az USA-ba. A katonai tisztviselők szerint ez az eset az exportellenőrzések egyik legsúlyosabb megsértése volt a háború utáni időszakban.¹⁵

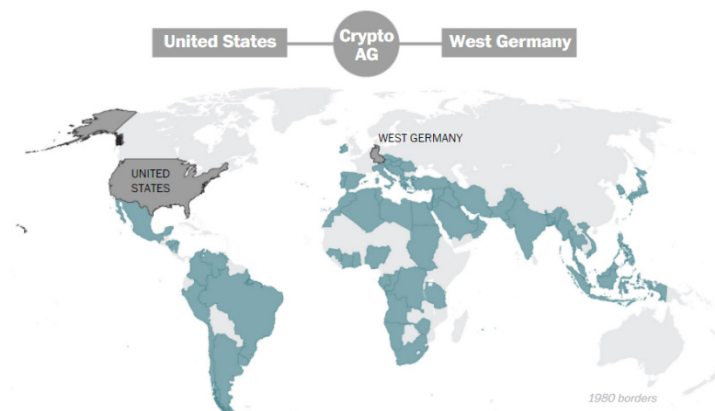
e) Crypto AG-botrány

Svájcot nem túlzás, hogy nagy mértékben megrendítette a Crypto AG-botrány.

A Crypto AG vállalat a második világháború alatt az amerikai csapatok számára készített rejtjelző gépeket. Majd évtizedekig a titkosító eszközök meghatározó gyártója lett, és a technológiai fejlődés során megoldásai a mechanikus váltóktól az elektronikus áramkörökig, végül a szilícium chipelig és szoftverekig terjedt. A svájci cég dollármilliókat keresett a 21. századig berendezései eladásával több mint 120 országban. Ügyfelei között volt Irán, Latin-Amerika, India, Pakisztán és a Vatikán is. Viszont, amit soha egyikük sem tudott, az az volt, hogy a Crypto AG titokban a CIA tulajdonában állt, és együttműködött a nyugatnémet hírszerzéssel. Ezek a kémügynökségek úgy szerelték fel a vállalat eszközeit, hogy könnyen feltudják törni azokat a kódokat, amelyekkel az országok titkosított üzeneteket küldtek. A „Thesaurus”, később a „Rubicon” néven ismert művelet a CIA történelmének legmerészebbjei közé tartozik. 1970-től a CIA és kódtörő testvére, az NSA irányította a Crypto működésének szinte minden aspektusát, a technológia megtervezésében, az algoritmusok szabotálásában és az értékesítési célok irányításában. Figyelték Irán molláit az 1979-es túszválság idején, Argentína hadseregével kapcsolatos hírszerzési adatokat adtak Nagy-Britanniának a falklandi

¹⁵ Farnsworth, Clyde. „Toshiba, Norway Concern Assailed in Soviet Sale”, The New York Times, 1987. május

háború alatt, nyomon követték a dél-amerikai diktátorok merényleteit és elkapták a líbiai tisztviselőket, akik gratuláltak maguknak egy berlini diszkó 1986-os bombázása miatt.



3. ábra: A dokumentumok szerint több mint 120 ország használta a Crypto AG eszközeit az 1950-es évektől egészen a 2000-es évekig. Forrás: The Washington Post

A programnak voltak korlátai. Amerika fő ellenfelei, köztük a Szovjetunió és Kína, soha nem voltak Crypto-ügyfelek. A német kémügynökség, a BND úgy vélte, hogy a leleplezés kockázata túl nagy, és az 1990-es évek elején kiszállt. A CIA megvásárolta a németek részesedését, és tovább folytatta a kémkedést, egészen 2018-ig.

A Crypto termékeit továbbra is a világ több mint egy tucat országában használják. Két vállalat vásárolta meg a Crypto eszközeinek nagy részét. Az első, a CyOne Security a menedzsment kivásárlásának részeként jött létre, és ma már kizárólag a svájci kormánynak értékesíti a biztonsági rendszereket. A másik, a Crypto International, ami átvette az egykori cég márkáját és nemzetközi üzletágát.^{16 17}

¹⁶ <https://www.bbc.com/news/world-europe-51487856:szervő>; Swiss Crypto AG spying scandal shakes reputation for neutrality: Imogen Foulkes; letöltve: 2020.10.20.; fordította: szerző

¹⁷ 'The intelligence coup of the century' For decades, the CIA read the encrypted communications of allies and adversaries, by Greg Miller – The Washington Post, Feb. 11, 2020



4.ábra: Hagelin M-209; Forrás: The Washington Post

Példaként a fent látható eszköz Boris Hagelinhez köthető. Egy zenedoboznak kinéző titkosítógépet fejlesztett ki, amely kevésbé volt olyan bonyolult, mint a németek Enigma-gépei. Tökéletes volt a mozgó csapatok részére, mérete és használata miatt. A használója betűről betűre forgathatja a tárcsát, és lenyomhatja a hajtókart. Az elrejtett fogaskerek megfordultak, és egy titkosított üzenetet nyomtak egy papírsíkra. Ezután a kódolt üzenetet kellett Morse-kóddal továbbítani a címzettnek, aki megfordította a sorrendet.

f) Wiki-Leaks

A Wiki-Leaks-et 2006-ban alapította Julian Assange, ún. nonprofit szervezetként, azzal a céllal, hogy kormányok és nagyvállalatok titkos ügyleteire világítson rá, ezzel csökkentse az országokon belüli korrupciót. Névtelen források információi és kiszivárogtatókból származó eredeti dokumentumok tartják fent a kapcsolódó internetes oldalt. Ennek egyik pozitívuma, hogy nem pletykákat, véleményeket vagy máshol is nyilvánosan elérhető anyagokat, hanem politikai ügyiratokat, történelmi és diplomatikus információkat tesz közé.

Wiki-Leaks botrányként ismert, amikor 251 287 diplomáciai táviratot szerzett meg a weboldal 2010 november végén. Mindezek előtt egy bizonyos „Collateral Murder” videó került nyilvánosságra 2010 áprilisában, ezzel együtt még közel 466 743 háborús napló, amelyek az afgán és az iraki háborúból származtak. Összességében körülbelül 718 030 dokumentum gyűlt össze, amit egyetlen kiszivárogtatóhoz, Bradley Manning közkatonához tudtak kötni. Manning 2009-ben volt Irakban, ahol hírszerzési elemzőként férhetett hozzá a titkos adatbázishoz.

A Wiki-Leaks első szakaszában, 2008-ban, több jelentős Kenyával kapcsolatos dokumentumot tett közé, ezzel párhuzamosan próbálták fejleszteni az ún. „Wiki-modell” -t, a nyilvános olvasóközönség aktívan posztolhat és szerkeszthet anyagokat.

A második szakaszában az előbb említett, „Collateral Murder” keltette fel a világi hatalmak figyelmét, amely nem csupán tájékoztatásul szolgált, hanem politikai szempontokra is alkalmas volt. „2010. április 5., 10:44 (EST) A WikiLeaks nyilvánosságra hozott egy minősített amerikai katonai videót, amely több mint egy tucat ember válogatás nélküli meggyilkolását ábrázolja Új-Bagdad iraki külvárosában - köztük a Reuters két tagját.

A Reuters az információs szabadságról szóló törvényen keresztül próbálta megszerezni a videót, a támadás óta sikertelenül. Az Apache helikopter lövegéből készített videó egyértelműen mutatja a megsebesített Reuters alkalmazottnak és megmentőinek nem provokált meggyilkolását. Két, a mentésben részt vevő kisgyermek is súlyosan megsebesült.”¹⁸

A harmadik szakasza pedig, a szintén előbb is említett diplomáciai táviratok kiadása. A WikiLeaks négy hírszervezetnek adta ki először ezeket (Le Monde, El Pais, The Guardian és Der Spiegel), mielőtt bármi nyilvánosságra került volna. Majd a The Guardian megosztotta a New York Times-szal is, így egyszerre adták ki a táviratokat, szeparáltan.¹⁹

Az oldal még most is működik és szivárogtat ki információkat, ezzel több politikai és területi vitát és összefüggést felfedve. Hivatalos weboldala: <https://wikileaks.org/>.

g) Edward Snowden

Edward Snowden 1983. június 21.-én született Észak-Karolina államban, az Egyesült Államokban. „Az én nemzedékem volt az utolsó Amerika, sőt talán a világ történelmében is, amelyre ez igaz – az utolsó nem digitalizált nemzedék, amelynek a gyerekkora nincs fent a felhőben, hanem jobbra analóg formában került rögzítésre, például kézzel írott naplók, polaroid felvételek és VHS-kazetták révén.”²⁰ Edward egy teljesen átlagos amerikai kisgyerek volt a '90-es években. Ez a kisgyerek, mint akkoriban megannyi társa, nagyon nagy érdeklődést mutat a videojátékok, a számítógép iránt. Akkoriban az internet még sokkal kevésbé volt szabályozott és mederbe terelt, ugyanakkor sokkal szabadabb, hozzáférhetőbb is volt, egyenlőbb és igazságosabb feltételeket biztosítva bárkinek, aki csatlakozott.

A Snowden-botrány a CIA és az USA egyik legmeghatározóbb és legnagyobb afférja volt. Edward Snowden, Booz Allen Hamiltonnak dolgozott infrastruktúra elemzőként az NSA-nél, Hawaiiiban. Azelőtt a CIA rendszertervező mérnöke, rendszergazdája és vezető tanácsadója volt.

¹⁸ <https://collateralmurder.wikileaks.org/>; letöltve: 2021.03.15.; fordította: szerző

¹⁹ <https://www.technologyreview.com/2010/12/09/120156/everything-you-need-to-know-about-wikileaks/>; Everything You Need to Know About Wikileaks, Two experts lay out the facts surrounding the controversy: Jonathan Zittrain, Molly Sauter, december 9, 2010; letöltve: 2021.03.15.; fordította: szerző

²⁰ Edward Snowden – Rendszerhiba (2019)

Ezeket látva érezhető, hogy az USA bizalmat fektetett Snowdenbe és a munkájába, akinek 2013 júniusi interjúja robbantotta ki az egész botrányt. Elmondása szerint, kezdetben abban hitt, hogy nemes szándékkal fogják felszabadítani a tengerentúli elnyomott népet, idővel azonban a hírek figyelése mellett rádöbbsent, hogy a valóság annál sokkal több, mint amit a sajtó feltár és minden népet félrevezetnek, nem csak az amerikaiakat. Ennek célja a befolyásolás volt. Edward indoka az volt, hogy nem akart egy olyan világban élni, melyben bármit mond és tesz, vagy a családja, barátai csinálnak, nyilvántartásba kerüljön és bármikor visszakövethető legyen. Arra várt, hogy korrigálják a jogtalanságokat, de megfigyelése szerint ez nem történt meg és csak az előző kormányok túlkapásait még rosszabbá és erőszakosabbá tették. A legnagyobb félelemnek azt tulajdonította, hogy a leleplezések eredményeként az USA számára semmi sem változik meg. A sajtó tájékoztatása után a társadalom tudni fogja, hogy meddig megy el az amerikai kormány, hogy hatalmat biztosítson saját magának azzal a céllal, hogy még nagyobb befolyást szerezzen az amerikai társadalom és a globális társadalom fölött. Az említett, The Guardian interjúja alapján, a vita két szálon mozgott. Az egyik szál a washingtoni törvényhozásban folyt arról, hogy milyen demokratikus jogi kontroll szükséges az NSA által folytatott kémkedés bírói korlátozására, amely figyelembe veszi a jogi és alkotmányos normákat is. A másik szál sokkal inkább érdekli a technológiai cégeket, és azon embereket, akik biztonsági problémákkal foglalkoznak. Ezen belül például, hogy miért gyengítette tudatosan az NSA a mindenki által használt és elterjedt titkosítási szabványokat. Miért tört be a telekommunikációs cégek rendszereibe, hogy ellopja a felhasználók adatait, és miért készített olyan sebezhetőségeket, amik hátsó bejáratot nyitnak azokba a telekommunikációs rendszerekbe, amikben mindannyian bízunk. Edward Snowden leleplezése után fontos kérdés merült fel, amely mindennapjainkban is számottevő problémák forrása. Létezik-e magánszféra? A mai digitalizált világban ez egy olyan kérdés, ami szinte mindenkit érint. Ez az eset súlyos következményekkel járt, hiszen köztudottá vált, hogy az USA lényegében mindenkit megfigyel és mindenkiről begyűjti az információkat, lehallgatja az embereket válogatás nélkül és ebben nagy szerepet játszanak az óriáscégek is a titkosszolgálatok mellett. A Facebook, a Google, Instagram és sok más közösségi oldal már teljesen részesévé vált az életünknek és ezek uralják már az online piacot is.

Európában ennek ellenére a magánszféra védelme alapvető jog és egy egységes európai szabályozás igénye merült fel. A megoldást abban is láttak, hogy a titkosszolgálatok munkáját még pontosabban a jogállami szabályok közé kell szorítani. Összességben a következmény tehát, hogy a botrány bebizonyította, hogy az internetfelhasználók adatai nincsenek biztonságban és széles körű vita indult a nemzetbiztonsági érdekek és a magánélethez való jog

közötti egyensúly témakörében. A hírszerző informatikus jelenleg Oroszország területén tartózkodik és szándékában áll orosz állampolgárságot szerezni, ezzel kettős állampolgárrá válna. Többszöri hosszabbítások után, 2020. október 22-én kapott örökérvényű lakhatási jogot. Ezeket az információkat Anatolij Kucserena, Snowden ügyvédje közölte. *"Miután több éve élünk a szüleinktől elválasztva, a feleségemmel nem akarjuk, hogy a fiunktól is elválasszanak minket. Ezért a világjárvány és a határok lezárása idején orosz-amerikai kettős állampolgárságért folyamodunk"*²¹ osztotta meg Snowden egy Twitter bejegyzésben.

h) A Cambridge Analytica cég botránya

*„Több mint 270 000 felhasználó adatát kezelte nem megfelelően korrekt módon az a vállalat, amelynek szolgáltatásait az amerikai sajtójelentések szerint Donald Trump és más republikánus politikusok is igénybe vették. Szakértői becslések szerint az adatok jellege miatt végül közel 50 millió ember adatai kerülhettek illetéktelenekhez.”*²² -írja a hvg.hu. Összefoglalva talán így lehet bemutatni korunk egyik legfrissebb botrányát, ami 2018-ban robbant ki, és a *thisisyourdigitallife* app segítségével gyűjtötte be az adatokat. A Facebook adatkezelési hibája miatt az applikáció nem csak a közvetlen felhasználók adataihoz férhetett hozzá, hanem az ismerőseikéhez is. Az említett alkalmazás a Cambridge-i Egyetem egyik tanárhoz, Aleksandr Kogan-hoz fűződik, aki 2014-ben fejlesztette ki a szoftvert. Az appot használók a letöltéssel engedélyt adtak a tartózkodási helyük hozzáféréséhez és hogy milyen tartalmakat néztek, kedveltek a Facebookon. Egyes források szerint a Cambridge Analytica cég 50 millió Facebook-oldal segítségével alkotott képet egyes emberek politikai felfogásáról, hogy személy szerint tudja őket irányítani a különböző reklámokkal, ezzel az elnökválasztást is befolyásolva.²³

Az ügy egyre komolyodott, hiszen az Európai Parlament és a londoni alsóház is kérdőre vonta Mark Zuckerberget, a Facebook vezérigazgatóját, miszerint az adatlopás által, nincs-e szándéka a világ kormányai ellen fordulni. (Donald Trump neve is felhangzik a botrány kapcsán, hiszen Robert Mueller különleges ügyész szerint, Trump kért be információkat az Analytica-tól.) Damian Collins, a londoni alsóház digitális, kulturális, média- és sportügyekért felelős bizottságának elnöke, levelet intézett Zuckerberghoz, melyben felszólította, hogy jelenjen meg a bizottság előtt. Ugyanakkor az EP is megtette ezt a lépést. *„A Facebooknak egyértelművé kell tennie az 500 millió uniós polgár képviselői előtt, hogy a személyes adataikat nem használják*

²¹ <https://twitter.com/Snowden/status/1323024457645105153>; 2020.12.01.; fordította: szerző

²² https://hvg.hu/tudomany/20180317_cambridge_analytica_adatgyujtes_facebook; 2021.03.15.

²³ https://hvg.hu/tudomany/20180317_cambridge_analytica_adatgyujtes_facebook1; 2021.04.20.

fel a demokrácia manipulálására” – írta Antonio Tajani, az uniós képviselő-testület elnöke a Twitteren.”²⁴

Zuckerberg válaszul felelősséget vállalt a cég nevében is biztonsági baklövéséért és szigorításokat vezetett be a közösségi platformon az adataink védelmét tekintve. *„Ezután a Facebook minden egyes applikáció fejlesztőjét felülvizsgálta és minden alkalmazás hozzáférését elemezte, hogy egyik se tudjon visszaélni és adatokat gyűjteni. Ha találtak olyan alkalmazást, amely mégis hozzáféréssel rendelkezett ezekhez, akkor azokat törölték a felületükről.*”²⁵ Továbbá után kirobbant egy ún. #DeleteFacebook kezdeményezés is, amely az oldaltól való megszabadulást hirdette.²⁶ A végkifejlett jelentős milliárd dolláros büntetések tömkelege lett, amely a Facebook nyakába zúdult. Több mint 1 milliárd embert érintett az eset világszerte.

Politikai hatása:

Ez a jelenség teljesen átalakította továbbá a választási kampányokat, hiszen a Facebook és a Twitter által, sokkal irányíthatóbbá változtatta az embereket. Nem csak az amerikai elnökválasztásnál jelenik meg, hanem a Brexit-kampányt is befolyásolta. Trump-választási kampányánál, a „Big Data”²⁷ adatelemzését, így személyre szabhatták a bizonyos politikai kampányokat az olvasók számára, továbbá jelentős adatmennyiséget gyűjtöttek össze a felhasználókról.²⁸

3) A nemzetközi szintén látható esetek

a) USA-Kína technológiai konfliktusa (Huawei, 5G kommunikáció):

A Huawei cég hallatán nagyon sok aggályt vet fel a jelenlegi nemzetbiztonsági szféra felé. A kínai technológia vállalat egyesek szerint kapcsolatban állhat a kommunista kormánnyal, és a készülékei segítségével információkat szivárogtathat a felhasználóikról. Ennek első konfliktusa 2018 augusztusában indult ki Donald Trump-tól, megtiltva az állami szféráknak, hogy olyan

²⁴https://hvg.hu/tudomany/20180320_Zuckerberg_bajban_Az_EP_es_a_brit_parlament_is_magyarazatot_var_az_adatgyujtesi_ugyben; letöltve: 2021.04.20.

²⁵ Papp Kristóf Csaba: A Cambridge Analytica-botárny tanulságai; KNBSZ: Szakmai Szemle, XVIII. évfolyam 1. szám 2020. március; 148. oldal; letöltve: 2021.04.22.

²⁶https://hvg.hu/tudomany/20180323_mark_zuckerberg_facebook_cambridge_analytica_adatgyujtesi_botrany_d_eletefacebook; letöltve: 2021.04.20.

²⁷ „A cégek, magányszemélyek, intelligens hálózatok által napi szinten előállított nagy mennyiségű adatot nevezzük BD-nek, ami azonban strukturált és strukturálatlan adathalmaz is egyben.” -forrás: Bányász Péter: A közösségi média szerepe a választásokban, 99. oldal; Nemzetbiztonsági Szemle, 7. évfolyam (2019) 1. szám letöltve: 2021.04.22.

²⁸ Papp Kristóf Csaba: A Cambridge Analytica-botárny tanulságai; KNBSZ: Szakmai Szemle, XVIII. évfolyam 1. szám 2020. március; 145.-158. oldal; letöltve: 2021.04.22.

cégekkel szerződjenek le, akik együttműködtek a Huawei-el.²⁹ A kínai cég 2019 március elején bejelentette, hogy beperli az amerikai kormányt annak döntése miatt. Ezek a döntések mind az amerikai, mind a kínai kormány gazdaságát is veszélyeztették, hiszen a nyugati kisvállalatok 25 %-a használja a cég eszközeit, Kína szempontjából pedig evidens a csökkenő eladásainak a káros gazdasági hatása. Mr.Song Liuping, a vállalat jogi vezetője szerint az USA nem adott bizonyítékot arra, hogy a Huawei bármiféle biztonsági fenyegetést jelent.

A világ két legnagyobb gazdasága az elmúlt években zűrzavaros kereskedelmi csatába keveredett, amelynek során egymilliárd dollár értékű árukra vetettek ki vámokat. 2019 május elején, Washington több mint kétszeresére, tehát 200 milliárd dollárra emelte a kínai áruk vámját, ami arra készítette Pekinget is, hogy megtorolja az amerikai termékek saját vámemeléseit.³⁰

A Google is felfüggesztett több együttműködést is a Huawei-el, az amerikai kereskedelmi minisztérium rendelete miatt. A Qualcomm és az Intel is csatlakozott ehhez a szankcióhoz, és megszüntették a kereskedést a céggel.

Mit is foglalt magában az elrendelés? - A Fehér Ház közleménye szerint Trumpnak az volt a célja, hogy megvédje USA-t olyan külföldi ellenfelektől, akik ki akarják használni az információs és kommunikációs technológiai infrastruktúra és a szolgáltatások sérülékenységét. Az Egyesült Államok szövetségeseit is ösztönözte, hogy kerüljék el az érintett technológiákat, és Ausztrália, valamint Új-Zéland egyaránt letiltotta a Huawei eszközök használatát az 5G hálózatokban.

A Huawei válasza: továbbra is állítja, hogy nem fenyeget veszélyt és teljesen független a kínai államtól. Vallja, hogy az USA-ban kiépíthető alternatív technológia, csak drágább és gyengébb minőségű lesz, mint az általuk kínált. Így ezzel az amerikai fogyasztók érdekeit is károsítani fogja az 5G hiánya. A vállalat ésszerűtlen korlátozásnak tartja, és a Huawei elnöke Liang Hua ki is jelentette, hogy aláírja a kormánnyal a „no-spy” megállapodást.³¹

A rendelet utáni állapot:

Az elemzők szerint nem fogja csődbe vinni a céget az amerikai embargó, megoldásnak tekinthetik a saját fejlesztések felgyorsítását, ezzel pedig megkezdődik a külső forrásoktól

²⁹ https://hvg.hu/tudomany/20190515_donald_trump_huawei_amerika_kina_gazdasagi_haboru; letöltve: 2020.09.30.

³⁰ <https://www.bbc.com/news/business-48441814>; Huawei: US blacklist will harm billions of consumers, 29 May 2019 letöltve: 2020.10.01.; fordította: szerző

³¹ <https://www.bbc.com/news/world-us-canada-48289550>; Trump declares national emergency over IT threats, 16 May 2019; letöltve: 2020.10.05.; fordította: szerző

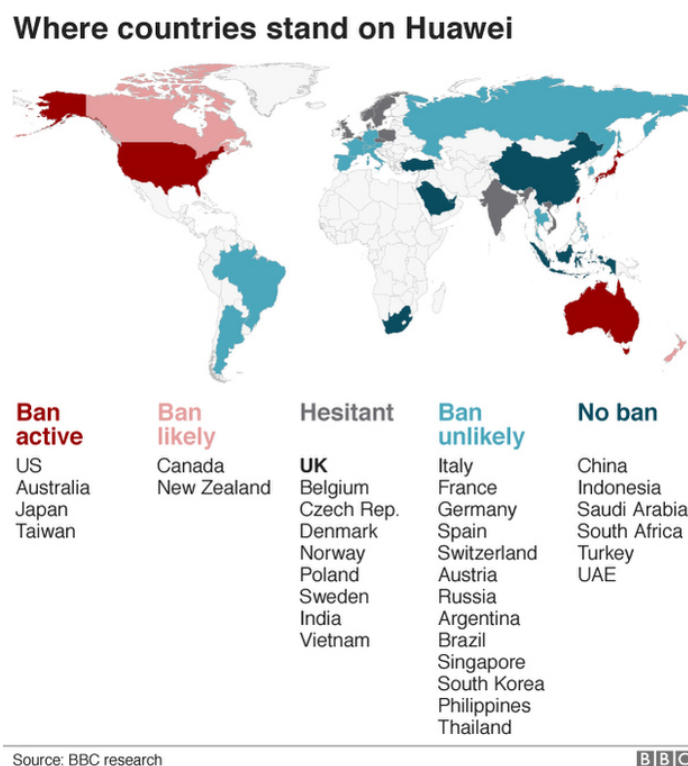
kevésbé függő alkatrészgyártás és elsősorban egy saját operációs rendszer elindítása is lehetséges.

Bár a Huawei esetében is, Trump a nemzetbiztonsági kockázatok végett indokolja az intézkedéseket, a valódi okok között ott lehet a kínai társaság kirobbanó, az amerikai cégeknek is komoly versenyt állító sikere.

A cég bevétele is érezheti az amerikai döntéseket, hiszen jelentős veszteség érheti őket, az előző évi hozamokhoz képest. A 2018-as adatokhoz mérten a 2019-es évben mintegy 40-60 millióval kevesebb okostelefont értékesíthet a Huawei és alapítója szerint, 30 milliárd dollárral lesz kevesebb a bevétele, a 2018. évi 100 milliárdhoz képest.

Zsen Cseng-fej nyilatkozatába arra is kitért, hogy „...cége a bevétel vártnál gyengébb alakulása ellenére sem fogja visszafogni kutatási-fejlesztési beruházásait. Az amerikai szankciókról szólva elmondta, hogy azt "mindkét fél meg fogja szenvedni" és a konfliktusnak "nem lesz győztese". Megjegyezte ugyanakkor, hogy a Huawei "nem lehet elpusztítani" és cége "kutatási és fejlesztési erőfeszítéseivel folytatja hozzájárulását az emberi társadalom fejlődéséhez".³²

A következő ábrán látható, hogyan ítélik meg egyes országok a Huaweiit.



5. ábra: Huawei helyzete szerte a világon. Forrás: BBC³³

³²https://hvg.hu/tudomany/20190617_huawei_bevetel_amerikai_szankciok_donald_trump_gyartok_piaci_reszes_eke_mobiltelefon_piac; letöltve: 2020.10.12.

³³ <https://www.bbc.com/news/business-48441814>; Huawei: US blacklist will harm billions of consumers, 29 May 2019 letöltve: 2020.10.01.; fordította: szerző

Kiegészítő rész: Az 5G technológia

„Az 5G sokkal nagyobb sebességgel és kapacitással rendelkezik, mint a korábbi mobilrendszerek, a jelentősen megrövidült várakozási idő miatt pedig jóval gyorsabb betöltési sebességet biztosít a felhasználók számára.”³⁴ A régi bázisállomások elavultak lesznek az 5G technológia befogadásához, hiszen elavultak lesznek, így a nagyobb frekvenciához, amit az 5G produkál kénytelenek lecserélni őket. Ez a technológiai haladás azért is szükséges, mert egyre jobban gyarapodik a technológiai, ún. okoseszközöknek a száma, amely képes internetkapcsolatot létrehozni.³⁵ Példa erre, hogy az Apple cég a 2021-es tavaszi eseményén, már olyan eszközöket mutatott be, amelyek képesek az 5G hálózat feldolgozására.

b) Google, Apple; high-tech cégek konfliktusa a nagyhatalmakkal

A négy legnagyobb high-tech cég: Apple, Amazon, Facebook és a Google ellen tárgyalás zajlott 2020 második felében az USA-ban. A BBC 2020. július 30-ai cikke szerint: „A világ legnagyobb technológiai vállalatainak vezetői megjelentek a washingtoni törvényhozók előtt, hogy megvédjék cégeiket azok ellen az állításokkal szemben, amelyek visszaélnék a versenytársak megsemmisítésére irányuló hatalmukkal.”³⁶ David Cicilline kongresszusi képviselő szerint; romboló, káros módszerekkel gyakorolták hatalmukat a terjeszkedés érdekében, ezt egy éven tartó vizsgálat mutatta ki. *„Néhány céget fel kellene bontani, továbbá mindegyiket megfelelően szabályozni kellene”* - mondta a több mint öt órás tanúvallomás végén. A Facebook-tól Mark Zuckerberg, az Amazon-tól Jeff Bezos, a Google-től Sundar Pichai és az Apple-től Tim Cook ragaszkodtak ahhoz, hogy semmi törvénytelen cselekedetet nem követtek el, és hangsúlyozták cégeik amerikai gyökereit és értékeit. Dan Ives, a Wedbush Securities technikai elemzője szerint nagy port kavarhatott Washingtonban az ügy, de szerinte valószínűtlen, hogy a kongresszus olyan új jogszabályok alapján álljon össze, amelyek változtatásra kényszerítik a technológiai vállalatokat. *„Jogalkotási hiányosság hiányában nem látunk érdemi változást a szabályozásban, bár a jövőbeni akvizíciókat minden bizonnyal megvizsgálják, és nehezebb lesz lezárni.”*³⁷ Hogy mi igaz a vállalatok vallomásából, biztosra nem tudhatjuk, rengeteg aggály merül fel a tech-

³⁴ <https://www.pannonantenna.hu/mit-jelent-az-5g-es-milyen-pozitiv-hatas-a-lesz-az-on-eletere/>; Mit jelent az 5G, és milyen hatása lesz az Ön életére?; letöltve: 2021.04.20.

³⁵ <https://www.pannonantenna.hu/mit-jelent-az-5g-es-milyen-pozitiv-hatas-a-lesz-az-on-eletere/>; Mit jelent az 5G, és milyen hatása lesz az Ön életére?; letöltve: 2021.04.20.

³⁶ <https://www.bbc.com/news/business-53583941>; Apple, Amazon, Facebook, Google face claims of 'harmful' power, 30 July 2020 letöltve: 2021.04.15.; fordította: szerző

³⁷ <https://www.bbc.com/news/business-53583941>; Apple, Amazon, Facebook, Google face claims of 'harmful' power, 30 July 2020 letöltve: 2021.04.15.; fordította: szerző

cégekkel kapcsolatban. A következőekben pedig az általam összegyűjtött fenyegetéseket gyűjtöttem össze, mely alátámaszt néhány aggodalmat, mind a cégek, mind a személyes életünk felé.

4) A közösségi hálók jelentős veszélye a 21 századi társadalomban; kiszolgáltatottság az internetnek

Ez a témakör az egyik legaktuálisabbnak tekinthető szerte a világon. „The Social Dilemma”³⁸ kutatását veszem a témakörhöz alapul. Ez a program vizsgálja, hogy miért esünk annyira a közösségi hálók csapdájába, az algoritmusok miért befolyásolnak mind, minket, mind a környezetünket.

„Csupán két iparág nevezi az ügyfeleit 'felhasználónak': a drogbiznisz és a szoftver” -Edward Tufte.³⁹ Miért van az, hogy egy push értesítés⁴⁰ következtében az agyunk egyből ráakar minket venni, hogy nézzük meg azt? Szinte ugyanazt a hatást váltja ki a drogok elvonása a fogyasztójától, mintha nem néznénk meg az értesítéseket napokig. A meggyőző tervezési technikák, például az előzőleg említett push értesítések és a hírcsatorna végtelen görgetése olyan visszacsatolási hurkot hoztak létre, amely ragaszkodik az eszközeinkhez. Rengeteg kérdést felvet ennek az új technológiának a hatása, és bárkit képesek ennek a segítségével lenyomozni, hiszen szinte minden fent van a világhálón.

A következőkben, amit a kutatás is említ, háromféle problémát szeretnék felvetni, bővebben kifejtteni.

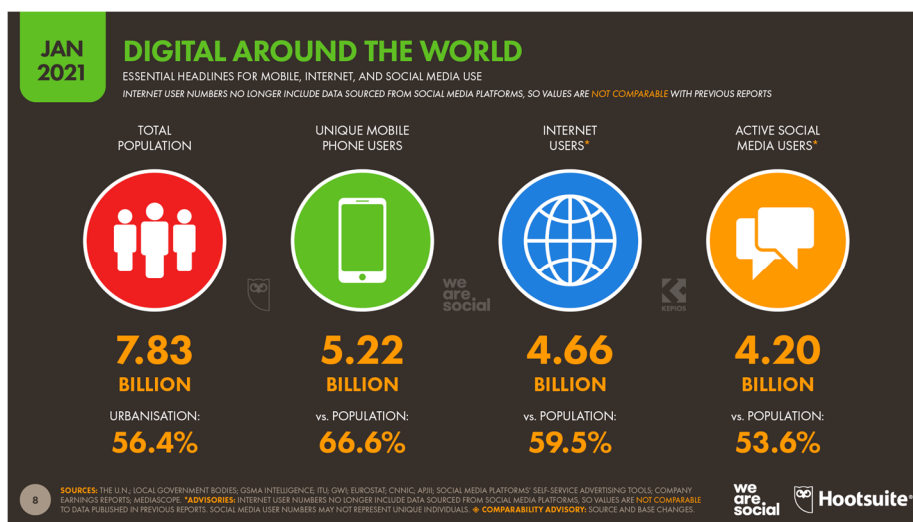
³⁸ <https://www.thesocialdilemma.com/the-dilemma/>; letöltve: 2021.03.10.; fordította: szerző

³⁹ <https://sundial.csun.edu/161195/arts-entertainment/review-netflixs-the-social-dilemma-is-a-great-conversation-starter-but-not-enough-to-create-change/>; Review: Netflix's "The Social Dilemma" is a great conversation starter, but not enough to create change: Preston Vanderslice; letöltve: 2021.04.20; fordította: szerző

⁴⁰ „Angolul „push notification”, az üzenetünk, amit a telefonra kapunk. Ezeket az értesítéseket, a különböző alkalmazások küldik nekünk. Az üzeneteket, a nap bármely szakában megkaphatjuk, függetlenül attól, hogy használjuk az alkalmazást vagy sem. Sőt még attól is függetlenül is, hogy használjuk-e a telefonunkat. Természetesen ehhez szükségünk van internetre, a telepített alkalmazásra és az engedélyünkre.” -forrás: <https://hwellkft.hu/marketing-szotar/push-ertesites>; letöltve: 2021.04.22.

a) Mentális és fizikai egészség károsodása

Tegyünk fel egy mindennapi példát, elmegyünk a városba, mi az első dolog, amit biztosan megpillant az ember, akár tömegközlekedésen, akár az utcán vagy bárhol? A mobiltelefon, vagy bármilyen más telekommunikációs eszköz, főképp igaz ez a nagyvárosokban. A körülöttünk való világot szinte észre se veszi az adott személy, nem foglalkozik a környezetével, az előbb említett push értesítések vagy az információk folyamatos bevitele, „görgetése” végett.



6. ábra: Globális digitális áttekintés 2021. január; Forrás: DataReportal

A Föld teljes népessége majdnem eléri a 8 milliárd főt, és ez a 2021-es kutatás bemutatja, hogy a világ közel 60%-a használja az internetet (2021. januárjában, ez a szám értelemszerűen egyre jobban növekszik). Mellékes tájékoztatásul szolgál az a tény, hogy az afrikai országokban, ahol több millió ember a civilizációtól távol él, még lehet nem is találkozott ezzel a technikával.

Az ábrán látható, hogy majdnem az összes internetező a közösségi médiát is rendszeresen használja, és egy évvel korábbi kutatás szerint ez a szám 13%-kal kevesebb volt, tehát egy év alatt majdan 490 millió felhasználót jelentett.⁴¹

Ezek ugyan számok, de nagyban tükrözik a társadalmi élet átalakulását, és hogy a mobil- és internethasználat előtérbe került.

b) Dezinformáció

A dezinformáció, másnéven félretájékoztatás, olyan információtartalommal rendelkezik, amely nem valós tényeken alapul és nyereségszerzés céljából kreálják. A mai társadalomban egy nagyon fontos és kiemelendő probléma, főképpen a jelenlegi koronavírusos időszak kapcsán, amit mindannyian tapasztalhattunk az interneten.

⁴¹ <https://datareportal.com/global-digital-overview>; letöltve: 2021.03.25.; fordította: szerző

Ezzel a problémával az EU is erőteljesen küzd, és igyekszik mindent elérni annak érdekében, hogy a mostani kritikus szintet minimálisra csökkentse. A következő ábrán látható az EU dezinformáció elleni közös és koordinált fellépésének áttekintése. Az érintett területeken egy akciótervet állított fel és 4 részre bontotta a programot.

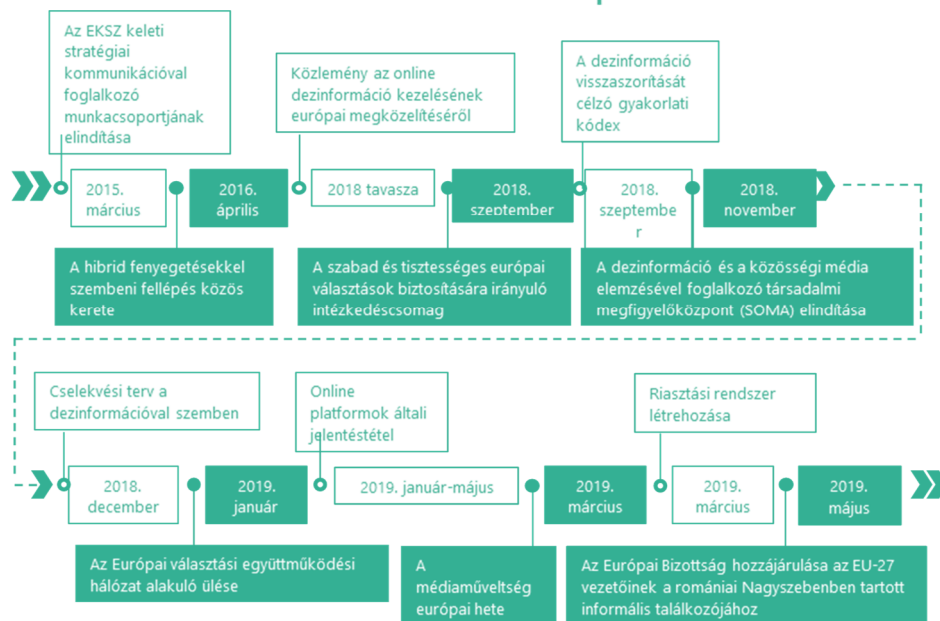
„1. Az EU megerősítette képességeit a dezinformáció azonosítása és a dezinformáció elleni fellépés terén az Európai Külügyi Szolgálaton belüli stratégiai kommunikációs munkacsoportok és a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport segítségével. Javította továbbá a koordinált válaszadást a riasztási rendszer létrehozásával, melynek célja a tagállamok és az uniós intézmények közötti információcsere megkönnyítése.

2. Az EU együttműködött az online platformokkal és az iparral az önkéntességen alapuló, dezinformáció visszaszorítását célzó gyakorlati kódex keretében a politikai kommunikáció átláthatóbbá tétele és a szolgáltatásaik manipulatív igénybevételének megakadályozása érdekében. Ezáltal a felhasználók megérthetik, hogy miért látják az adott politikai tartalmakat és hirdetéseket, továbbá információt kapnak azok eredetéről.

3. A Bizottság és a főképviselő, az Európai Parlament együttműködésével, segítette növelni a tudatosságot és a dezinformációval szembeni rezilienciát a társadalomban, nevezetesen tényalapú üzenetekkel és a médiaműveltség előmozdítására irányuló erőfeszítések fokozásával.

4. A Bizottság együttműködés, iránymutatás és támogatás, valamint jogalkotási intézkedések révén támogatta a tagállamok erőfeszítéseit a választások integritásának biztosításában és az Unió demokratikus rendszerei ellenálló képességének erősítésében.”

Az EU dezinformáció elleni közös és koordinált fellépésének áttekintése



42

7. ábra: az EU dezinformáció elleni közös és koordinált fellépésének áttekintése; Forrás: Közös közlemény az EP-nek; 2019.6.14.

De mik is azok a dolgok, amik segítik a dezinformációt?

A lakosság egyre nagyobb rétege figyelmen kívül hagyja a tényeket, sőt készségesen elfogadja a nyilvánvaló hazugságokat. Azt az igazságot gondolják helyénvalónak, amit ők is gondolnak, ezért a biztos tények megtekintésétől eltávolodnak. A kommunikatív bőség és a „post-truth” terjedésének legmeglepőbb hosszú távú hatása vitathatatlanul az, hogy megerősítik az arrogáns igazsághit modern megkérdőjelezését és elutasítását.⁴³

Erre még külön egy konkrét kutatást emelnék ki, melyben Sinan Aral és szerzőtársai 2006-2017 között a Twitteren terjedő híreket vizsgálták, és kutatásuk bebizonyította, hogy az álhírek sokkal több társadalmi réteget érnek el, kevés idő alatt és mélyebben terjedtek el a megfigyelt kategóriákban. Egyes esetekben jelentős mértékben akadályozták meg a hiteles hírek terjedését. A politikai hírek emelkednek ki a legjobban ezek közül.⁴⁴

A dezinformációnak még a további segítő tényezőihez tartozik az átalakult hírfogyasztási szokások, a túlzott információmennyiség a közösségi platformokon és a titkos, algoritmusok,

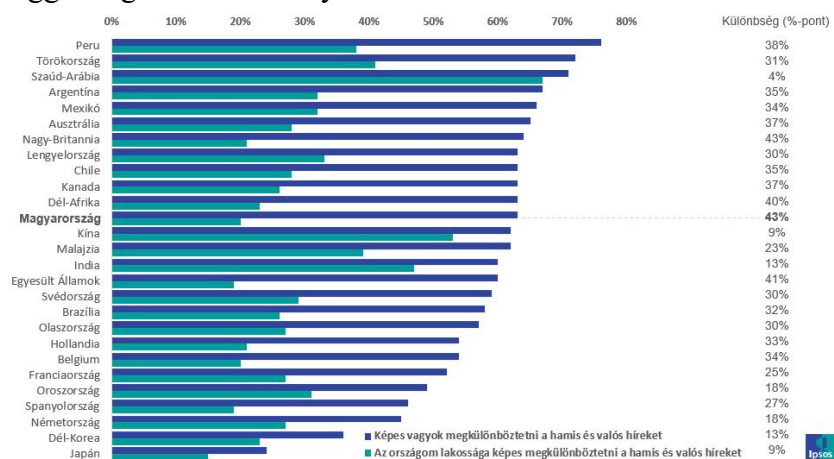
⁴² Európai Bizottság: Közös közlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságának és a Régiók Bizottságának; Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról; Brüsszel, 2019.6.14.

⁴³ <https://theconversation.com/post-truth-politics-and-why-the-antidote-isnt-simply-fact-checking-and-truth-87364>; Post-truth politics and why the antidote isn't simply 'fact-checking' and truth: John Keane letöltve: 2021.04.10.; fordította: szerző

⁴⁴ <https://science.sciencemag.org/content/359/6380/1146>; The spread of true and false news online: Soroush Vosoughi, Deb Roy, Sinan Aral; letöltve: 2020.04.20.; fordította: szerző

és a trollhadseregek⁴⁵, amelyek Oroszországban a legelterjedtebbek, és amit utolsóként megemlítenék azok a botnetek⁴⁶.⁴⁷

Az Ipsos általi kutatásba történő betekintéssel zárnam ezt a fejezetet, melyben leírja, hogy a világon a felnőtt emberek 82%-a bizonyosodik meg a hírek hiteles forrásából, ugyanakkor a lakosság csupán 30%-a képes megkülönböztetni a valódi híreket a hamisaktól. A magyar lakoságnál ez a szám jóval kisebb. A következő diagramon látható országokra lebontva ez az arány, mely eléggé megosztó véleményem szerint.



8. ábra: Az Ipsos 2020-as kutatása; Forrás: Ipsos

„Egytizednyi tömeg egyáltalán nem bizonyosodik meg a hírek igazságtartalmáról, ezzel Magyarország lakossága – a törökökkel egyetemben – a legnagyobb felületet adja a fake news terjedésének.”⁴⁸

⁴⁵ „A Szentpéterváron található Internet Research Agency nevű, online kutatással foglalkozó cégnél például váltott műszakban, hármas csoportokban, eltérő bérkategóriába sorolva dolgoznak becslések szerint ezen, hogy Nyugat-ellenes, Kreml-barát híreket osszanak meg hazai és külföldi portálokon. A témákat az adott nap elején jelölik ki, és meghatározott számú kommentet kell meghatározott számú profillal elhelyezni. Ezeket nagyban meghatározzák az aktuális kül- és belpolitikai történések.” -forrás: Lélektani műveletek a közösségi médiában: Bányász Péter, Dobos László, Palla Gergely, Polner Péter, (14. oldal); Dialóg Campus, Budapest, 2019

⁴⁶ „A robóhálózat (továbbiakban botnet) egy fertőzött informatikai eszközökből álló hálózat, amelyet a botnet gazdája többféle károkozásra is alkalmazhat. A fertőzött munkaállomások felhasználásának célja főképp kényszerű levelek kiküldése, szolgáltatás megtagadást okozó támadások (Denial-of-Service – DoS) indítása, vagy éppen szenszitiv (például banki) adatok eltulajdonítása.

A támadónak elsőként hozzáférést kell szereznie az áldozat eszközéhez, ami sokféleképpen történhet. Egyik szokványos mód az ún. exploit kitek segítségével történő fertőzés, amelynek során a támadó egy weboldalon keresztül – valamilyen sérülékenység kihasználásával – automatikusan telepíti a káros kódot (bot) a site-ot meglátogatók gépére. Másik, szintén gyakori módszer a káros kódot tartalmazó kényszerű levelek útján történő fertőzés is. A célpontok klasszikusan asztali számítógépek, de egyre gyakrabban kerülnek a célkeresztbe IP kamerák, mobiltelefonok, vagy akár routerek is.” -forrás: <https://nki.gov.hu/it-biztonsag/tudastar/robotohalozat-botnet-2/>

⁴⁷ Lélektani műveletek a közösségi médiában: Bányász Péter, Dobos László, Palla Gergely, Polner Péter, (14. oldal); Dialóg Campus, Budapest, 2019

⁴⁸ <https://www.ipsos.com/hu-hu/magyarok-tizede-egyaltalan-nem-ellenorzi-hirek-megbizhatosagat>; A magyarok tizede egyáltalán nem ellenőrzi a hírek megbízhatóságát, 21 október 2020; letöltve: 2021.04.20.

c) Algoritmusok hatása a gondolkodásunkra, tetteinkre

Először az algoritmusokról; mik is azok, mi alapján működik? A különböző információs eszközök és rendszerek algoritmusokat létrehozni, amikben beépített mikroprocesszor található, ez reprodukálható és hordozható digitális formában integrálja a szövegeket, hangokat és képeket.

Erre a legjobb példa a bizonyos „filter bubble”⁴⁹, magyarosítva szűrőbuborék. A webhelyek az előzőleg is használt böngészési szokásainkat használják fel és alkalmazzák az algoritmusok létrehozásához. Ez egy ún. intellektuális elkülönítés a felhasználó által kedvelt és nem kedvelt tartalmi között, a különböző közösségi platformok használják ezt, mint az Instagram, YouTube, TikTok, Twitter, Facebook és a Google is. A Google beállításokban, mellesleg mi is megtudjuk nézni, hogyan „rangsorolt” be minket, ha rendelkezünk fiókkal, ezzel a módszerrel tekinthetjük ezt meg: beelépünk a szinkronizálás fül alatti „Beállíthatja, hogy a rendszer hogyan szabja személyre a Keresést, a hirdetéseket és egyebeket a böngészési előzmények alapján”-ra, majd a tevékenységvezérlőknél találjuk magunkat, ott pedig az összes tevékenységvezérlő megtekintése menüpontra kattintunk, ezután a következő ablak szinte legalján a hirdetések személyre szabásánál, ugrás a hirdetésbeállításokhoz menüpont és meg is találhatjuk az említett keresőmotorokat⁵⁰, mely nagy vonalakban meghatározza személyünket és cselekedeteinket. Ezt nem csak mi tehetjük meg, hanem bármelyik szerver és a tudunk nélkül gyűjthet be rólunk mindenféle információkat.

Ezek az algoritmusok is többféle hirdetést, webhelyt fognak megjeleníteni számunkra, melynek lehetnek negatív és pozitív oldalai is. Egy belső Facebook jelentés szerint a közösségi platformon, az emberek 64%-a azért csatlakozott szélsőséges csoportokhoz, mert az algoritmusok oda terelték őket.⁵¹

III. Összegzés

A dolgozatom elején szót ejtettem a hidegháború jellemzőiről, azoknak a vívmányairól és botrányairól. Ezek a botrányok és kezdetleges kommunikációs eszközök voltak az alappillérei a jelen társadalmunknak és technológiai eszközeinknek. Ezért is volt fontos ennek bemutatása, hogy megismerjük az alapot, ahonnan indult ez a tömérdek információ- és adathalmaz. Az első

⁴⁹ „A „filter bubble” (filter/szűrőbuborék) egy olyan intellektuális elkülönítés, ami a webhelyek algoritmusai alapján történik. Az ilyen algoritmusok feladata a felhasználók korábbi böngészési szokásai alapján feltételezni, hogy mit szeretnének látni, és ilyen információkat kínálni nekik.” -forrás:

<https://matebalazs.hu/szurobuborek.html>

⁵⁰ 2021.04.20.

⁵¹ <https://www.thesocialdilemma.com/the-dilemma/>; letöltve: 2021.03.10.; fordította: szerző

kommunikációs afférokból is látszott, hogy minden, aminek látható nyoma van, előbb-utóbb nem marad titok az emberiség számára, nevezzük ezt „technológiai lábnyomnak”. Kezdetben inkább nagyobb tehetősebb körökben jelent meg, majd folyamatosan fejlődött és ért el a mindennapi emberhez.

Hogy miért is került kapcsolatba a jelenkori internet veszélyei az infokommunikációs technológiához? Ez a mai korban véleményem szerint teljesen összemosódik, az 1970-es, 1980-as években bemutatott botrányok kapcsán még nem terjedt el olyan szinten, hogy az átlagemberhez is eljusson és veszélyt jelentsen rá, és ez a tanulmány is azt mutatja, hogy a technológia fejlődéséhez igazodni kell ezáltal. A kiszolgáltatottság veszélye ezzel folyamatosan nő, és a személyes, vagy akár a nagyobb cégek és szervezetek adatai rossz kezekbe kerüljenek, vagy nagyobb gazdasági veszély is kialakuljon ezáltal. Különböző szempontok és biztonsági előírások alapján tudjuk ezeket szabályozni és figyelni rá, ez a dolgozat is erre hívja fel a figyelmet, milyen hátrányokkal vagy problémákkal kell szembenézni a technológiák fejlődése során.

A jelenben, ha egy képet megosztunk, ha egy posztot kiírunk, vagy elfogadjuk azokat a bizonyos „cookie” beállításokat, minden mozdulatunk és érdeklődési körünk lekövethető. Bizonyos szabályzók már léteznek erre, de mindig figyelniünk kell adatink biztonságára és arra is, hogy ne szippantson be minket a közösségi média világa. Ez a dolgozat is egy ilyen célt szolgál, hogy aki olvassa realizálja azt a tényt, hogy „sose lehet egyedül”, hiszen a technológia fejlődése megteremtette azt a szituációt, hogy bárhol és bárki lekövethető és lehallgatható legyen, legyenek példák erre a munkában bemutatott esetek.

IV. Felhasznált irodalmak, folyóiratok:

- A rádiótechnika évkönyve – 2002: Horváth Lajos: A világ legnagyobb fülei...
- Bányász Péter: A közösségi média szerepe a választásokban, 99. oldal; Nemzetbiztonsági Szemle, 7. évfolyam (2019) 1. szám letöltve: 2021.04.22.
- Dobák Imre: Betekintés az állambiztonság 1960-70-es évei nemzetközi technikai kutatás-fejlesztési folyamatainak szerkezetébe
- Edward Snowden – Rendszerhiba (2019)
- Európai Bizottság: Közös közlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságának és a Régiók Bizottságának; Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról; Brüsszel, 2019.6.14.
- Farnsworth, Clyde. „Toshiba, Norway Concern Assailed in Soviet Sale”, The New York Times, 1987. május
- Hirsch, Steve. „Export Control Policy”, The Multinational Monitor; letöltve: 2021.03.19.
- History TV: A szuperhatalmak titkos repülőgépe: Kémrepülőgépek
- Lélektani műveletek a közösségi médiában: Bányász Péter, Dobos László, Palla Gergely, Polner Péter, (14. oldal); Dialóg Campus, Budapest, 2019
- London Telegraph, Tuesday 16 December 1997, Issue 936 (Spies like US): Duncan Campbell; fordította: szerző
- Magyar Közlöny, 1999. december (126. szám, 2. kötet)
- Papp Kristóf Csaba: A Cambridge Analytica-botárny tanulságai; KNBSZ: Szakmai Szemle, XVIII. évfolyam 1. szám 2020. március; 145.-158. oldal; letöltve: 2021.04.22.
- Pászka Tibor mk. dandártábornok – Haza, tudás, becsület – A jubileum kötelez! Felderítő szemle, 2007. július VI. évf. Emlékszám, MK KFH, Budapest, pp. 8.
- ‘The intelligence coup of the century’ For decades, the CIA read the encrypted communications of allies and adversaries, by Greg Miller – The Washington Post, Feb. 11, 2020

Internetes források:

- <https://collateralmurder.wikileaks.org/>; letöltve: 2021.03.15.; fordította: szerző
- <https://datareportal.com/global-digital-overview>; letöltve: 2021.03.25.; fordította: szerző

- https://hvg.hu/tudomany/20180317_cambridge_analytica_adatgyujtes_facebook; letöltve: 2021.03.15.
- https://hvg.hu/tudomany/20180320_Zuckerberg_bajban_Az_EP_es_a_brit_parlament_is_magyarazatot_var_az_adatgyujtesi_ugyben; letöltve: 2021.04.20.
- https://hvg.hu/tudomany/20180323_mark_zuckerberg_facebook_cambridge_analytica_adatgyujtesi_botrany_deletfacebook; letöltve: 2021.04.20.
- https://hvg.hu/tudomany/20190515_donald_trump_huawei_amerika_kina_gazdasagi_haboru; letöltve: 2020.09.30.
- https://hvg.hu/tudomany/20190529_huawei_google_android_egyesult_allamok_szankciok_birosag; letöltve: 2020.10.05.
- https://hvg.hu/tudomany/20190617_huawei_bevetel_amerikai_szankciok_donald_trump_gyartok_piaci_reszesede_mobiltelefon_piac; letöltve: 2020.10.12.
- https://hvg.hu/tudomany/20191014_huawei_5g_halozat_fejlesztes; letöltve: 2020.10.09.
- <https://hwellkft.hu/marketing-szotar/push-ertesites>; letöltve: 2021.04.22.
- https://index.hu/tudomany/tortenelem/2015/10/28/oriasi_karokat_okozott_a_hideghaborus_szexbotrany/; letöltve: 2020.10.10.
- <https://matebalazs.hu/szurobuborek.html>; letöltve: 2021.04.20.
- <https://nki.gov.hu/it-biztonsag/tudastar/robothalozat-botnet-2/>; 2021.04.15.
- <https://science.sciencemag.org/content/359/6380/1146>; The spread of true and false news online: Soroush Vosoughi, Deb Roy, Sinan Aral; letöltve: 2020.04.20; fordította: szerző
- <https://sundial.csun.edu/161195/arts-entertainment/review-netflixs-the-social-dilemma-is-a-great-conversation-starter-but-not-enough-to-create-change/>; Review: Netflix's "The Social Dilemma" is a great conversation starter, but not enough to create change: Preston Vanderslice; letöltve: 2021.04.20; fordította: szerző
- <https://theconversation.com/post-truth-politics-and-why-the-antidote-isnt-simply-fact-checking-and-truth-87364>; Post-truth politics and why the antidote isn't simply 'fact-checking' and truth: John Keane letöltve: 2021.04.10.; fordította: szerző
- <https://twitter.com/Snowden/status/1323024457645105153>; letöltve: 2021.12.01.; fordította: szerző
- <https://www.bbc.com/news/business-48441814>; Huawei: US blacklist will harm billions of consumers, 29 May 2019 letöltve: 2020.10.01.; fordította: szerző

- <https://www.bbc.com/news/business-53583941>; Apple, Amazon, Facebook, Google face claims of 'harmful' power, 30 July 2020 letöltve: 2021.04.15.; fordította: szerző
- <https://www.bbc.com/news/world-europe-51487856>; Swiss Crypto AG spying scandal shakes reputation for neutrality: Imogen Foulkes; letöltve: 2020.10.20.; fordította: szerző
- <https://www.bbc.com/news/world-us-canada-48289550>; Trump declares national emergency over IT threats, 16 May 2019; letöltve: 2020.10.05.; fordította: szerző
- <https://www.britannica.com/event/Profumo-affair>; Profumo affair British political scandal: Robert W. Pringle letöltve: 2021.03.10.; fordította: szerző
- <https://www.darpa.mil/program/memex>; letöltve: 2021.03.10.; fordította: szerző
- <https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiore>; letöltve: 2020.10.18.; fordította: szerző
- <https://www.history.com/news/watergate-deep-throat-fbi-informant-nixon>; How 'Deep Throat' Took Down Nixon From Inside the FBI: Annette McDermott; letöltve: 2021.03.09.; fordította: szerző
- <https://www.history.com/topics/1970s/watergate>; Watergate Scandal; letöltve: 2021.03.09.; fordította: szerző
- <https://www.historyextra.com/period/20th-century/real-history-profumo-affair-christine-keeler-who-what-happened/>; Sex, lies and spies: the real history of the Profumo Affair: Anna Harris; letöltve: 2020.03.12.; fordította: szerző
- <https://www.ipsos.com/hu-hu/magyarok-tizede-egyaltalan-nem-ellenorzi-hirek-megbizhatosagat>; A magyarok tizede egyáltalán nem ellenőrzi a hírek megbízhatóságát, 21 október 2020; letöltve: 2021.04.20.
- <https://www.nsa.gov/news-features/declassified-documents/ukusa/>; letöltve: 2020.10.16.; fordította: szerző
- <https://www.origo.hu/gazdasag/20190125-penz-a-lelke-cocom-lista.html>; letöltve: 2020.09.10.
- <https://www.pannonantenna.hu/mit-jelent-az-5g-es-milyen-pozitiv-hatas-a-lesz-az-on-eletere/>; Mit jelent az 5G, és milyen hatása lesz az Ön életére?; letöltve: 2021.04.20.
- <https://www.szeretlekmagyarorszag.hu/osszeomolhat-a-svajci-semlegesseg-mitosza-az-evszazad-kembotranya-miatt/>; letöltve: 2020.10.20.
- <https://www.technologyreview.com/2010/12/09/120156/everything-you-need-to-know-about-wikileaks/>; Everything You Need to Know About Wikileaks, Two experts

lay out the facts surrounding the controversy: Jonathan Zittrain, Molly Sauter, december 9, 2010; letöltve: 2021.03.15.; fordította: szerző

- https://www.thelivingmoon.com/45jack_files/03files/ECHELON_Menwith_Hill.html; 2020.10.17.; fordította: szerző
- <https://www.thesocialdilemma.com/the-dilemma/>; letöltve: 2021.03.10.; fordította: szerző