



Nemzeti Közszolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar
Intézményi Tudományos Diákköri Konferencia

A digitális analfabetizmus nemzetbiztonsági kockázatai

JELIGE: digitális analfabetizmus

2024.

TARTALOMJEGYZÉK

BEVEZETÉS	3
1. ANALFABETIZMUS.....	5
1.1 Az Alapoktól.....	5
1.2 Modern kori analfabetizmus	7
2. DIGITÁLIS ANALFABETIZMUS.....	10
2.1. Kitekintés	10
2.2. Digitális Analfabetizmusban rejlő Kockázatok	11
2.3. Többszereplős játék.....	13
2.4. Megoldás keresés	21
2.4.1 Az egyéni edukáció előnyei	21
2.4.2 Az állami szabályozás előnyei.....	21
2.4.3 Egyesített megközelítés előnyei	22
3. A DIGITÁLIS VAKSÁG VESZÉLYE EGY NEMZET BIZTONSÁGÁRA.....	23
1.1 A lelkek sebezhetősége.....	23
1.2 Az érzelmi csalások szerepe a titkosszolgálatok gyakorlatában.....	24
1.3 Az érzelmi csalások módszerei és eszközei	24
1.4 Az érzelmi csalások módszerének használata a titkosszolgálatok által.....	27
1.5 Másodlagos hatás.....	29
1.6 Védekezési lehetőségek az érzelmi csalásokkal szemben	30
1.7 Individuumban rejtőző kockázatok	31
KÖVETKEZTETÉSEK	33
FELHASZNÁLT IRODALOM.....	36
Jogszabályok.....	36
Szakirodalom	39
Egyéb forrás.....	41

BEVEZETÉS

A szerző figyelmét megragadó témát boncolgató minden tudományos értekezés, esszé bevezetőjében elvárt követelmény, hogy kifejtésre kerüljön, miért is aktuális, miért fontos az a terület, amivel foglalkozni érdemes és mire lehet majd használni az elkészített pályaművet. Felteszem hát én is a kérdést: miért is fontos a digitális analfabetizmussal foglalkozni manapság? Vagy szükséges-e feltennem a kérdést, miért is fontos a digitális analfabetizmussal foglalkozni manapság?

A XXI. században élünk. Mindennapi tevékenységeinket behálózzák az okos eszközök¹. Számolatlanul költjük a pénzt a legújabb elektronikai eszközökre, rendszerekre. Laptop, okostévé, okostelefon, okosóra – repkednek a tíz- sőt százvezrek. Vesszük őket úgy, mintha nem lenne holnap, mert társadalmi elismertséget, irigységet, vagy egyéb más interakciót akarunk vele kiváltani embertársaink körében. A [www.Statista.com](https://www.statista.com) mérőszámai² alapján a laptopok piacán világszerte generált bevétel az előrejelzések szerint 2024-ben eléri az 58,9 milliárd dollárt. Ez a piac várhatóan éves szinten 2,82% -kal növekszik (CAGR 2024-2029). Ami a jövőt illeti, a laptopok piacának volumene 2029-re várhatóan eléri a 89,8 millió darabot. Tabletek³ esetében ugyanezen számok a következők: 2024-ben a táblagépek piaca világszerte várhatóan 53,7 milliárd USD bevételt generál. Ez a piac várhatóan 2,79% -os éves növekedési ütemet fog tapasztalni (CAGR 2024-2029). Elemzések szerint 2029-re a táblagépek piacának volumene várhatóan eléri a 195,3 millió darabot. Végül szerepeljen itt az okostelefonok⁴ piaca is: 2024-ben ennek a termékkategória piacának bevétele világszerte várhatóan eléri a 0,5 milliárd dollárt. Becslések szerint ez a piaci szegmens várhatóan 3,57% -os éves növekedési ütemet fog tapasztalni (CAGR 2024-2029). A 2029-es előrejelzések szerint az okostelefonok piacának volumene várhatóan eléri az 1,7 milliárd darabot.

Döbbenetes számok ezek és a világ éhsége csak nő a fenti termékek iránt. De az átlagember ismeri egyáltalán a saját eszközét? Tényleg ismeri azokat az alkalmazásokat, amiket letölt? Tudja mi az a háromszintű autentikáció, mit jelentenek a cookie-k és az elfogadása? Vagy esetleg még azt sem tudjuk, hogyan lehet beállítani az időt az óraátállítások idején és zavartan, szemlesütve csendben kérdezzük meg kollégáinkat: Mi a TITOK?

¹ Digitális analfabetizmus a 21. században? - Neo Nomad

² Laptopok - világszerte | Statista piaci előrejelzés

³ Tablets - Worldwide | Statista Market Forecast

⁴ Okostelefonok - világszerte | Statista piaci előrejelzés

Ismét a [www.Statista.com](https://www.statista.com) mérőszámaait hívom segítségül⁵:

- 46%: Ez az arányszám azon ismert esetekben, ahol a szervezet ransomware támadás észlelését követően fizetett a titkosított adatok visszaszerzéséért.
- 9,22 milliárd USD: a kiberbűnözés költségei világ összesen
- 1,9 millió: a végfelhasználók által jelentett egyedi fenyegetések száma.

Véleményem szerint nem kell bátorság ahhoz, hogy kijelentsük, a mi világunkban ugyanúgy létezik az analfabetizmus, csak most már modernizálásra került, átalakult. A Mátrix itt van, megérkezett, dörömböl. Az ajtónkon. Belülről. Ez az, ami indokoltá teszi, hogy aktuális és fontos témaként beszéljünk a digitális-analfabetizmusról és az abban rejlő kockázatokról.

Aktuális és fontos téma, de milyen haszna van egy ilyen témában megírt értekezésnek? Céлом, hogy edukáljon és felébresszen. Céлом, hogy feltárjam azokat a társadalmunkban gyökerező problémákat, amik ahhoz vezetnek, hogy az egyén és rajta keresztül családok, szervezetek, cégek, kormányok, országok az áldozattá válásához vezetnek.

A katona a társadalom része. Önmagán és családján keresztül ezernyi szállal kötődik a környezetéhez és nem vonhatja ki magát a kibertér közvetítette kockázatok alól, még annak ellenére sem, hogy az állományba kerülésével és pályája során többszöri alkalommal esélyt kap arra, hogy tudatosuljon benne és ez által észlelje, elkerülje, eliminálja a veszélyt, vagy segítséget kérjen, ha mégis bajba kerül. A fenyegetés alatt álló katona hatékonysága csökken, ezáltal komoly kockázatokat is jelent az alkalmazhatósága, illetve a katonai nemzetbiztonság szempontjából.

A fenti kérdések megválaszolására az alábbi hipotéziseket állítottam fel.

H1: A technológiák fejlődését nem követi le a felhasználók tudásának és tájékozottságának gyarapodása.

H3: A társadalom egyes szereplői egyedül nem képesek tartós sikert elérni, ehhez együttműködés és koordináció szükséges.

H2: A digitális analfabetizmus egy bizonyos szint felett kihat egy ország nemzetbiztonságára.

Céлом tehát, hogy bemutassam, részletezzem, hogyan befolyásolja ez a jelenség a nemzetbiztonságot, valamint milyen megoldási javaslatok léteznek a probléma kezelésére.

⁵ <https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#overview>

1. ANALFABETIZMUS

1.1 Az Alapoktól

A kiber-analfabetizmus, a digitális-analfabetizmus, mind a jelenkor új kifejezései. Egyetemes tudásunk emlékeink között kutatva mind a két szó valaminek a hiányát, valamihez való hozzá nem értését jelentik. Egy produktum elkészítéséhez – legyen az festmény, épület, irodalmi mű, bármilyen ember alkotta forma – nem elégedhetünk meg homályos ismeretmorzsákkal. Az alkotást az alapoktól kell elkezdeni és tégláról, szóról, ecsetvonástól a következőkig kell felfejlődnie és kiteljesednie a végső kimenetnek. Jelen értekezés sem kivétel ez alól. Ahhoz, hogy téziseket állítsunk fel szükséges visszanyúlni a gyökerekhez, definiáljuk hát mit is jelent maga a fogalom, hogyan tudjuk, hogyan akarjuk értelmezni az emberi képesség, illetve annak hiányának fenti megfogalmazását.

Az analfabéta görög eredetű szóösszetétel, mára nemzetközileg ismert fogalommá nőtte ki magát: az *ana-* előtag ellentétet jelző kifejezés, az *alphabéta* ('ábécé') pedig a görög betűsor első két tagja⁶. A Magyar Etimológiai szótár értelmezése szerint „az analfabéta – 'írástudatlan (személy)'; 'valamihez nem is konyító': pl. *zenei analfabéta*. Az analfabetizmus: 'az írástudatlanság mint az adott népesség egy bizonyos hányadára jellemző állapot'.⁷” A Bakos Ferenc féle Idegen Szavak és Kifejezések Szótára szerint az analfabéta írástudatlan, írni-olvasni nem tudó személyt jelöl, pejoratív használatban műveletlen, tudatlan egyént.⁸

Az analfabetizmus létezéséért, mértékéért több felelős okot is fel lehet sorolni. Az OSINT kutatásaim alapján megállapítottam, hogy a szakmai források többnyire azonos csoportosításokat határoztak meg. Nem célom, nem feladatom és a keretek sem adottak az analfabetizmus újszerű osztályozásának megalkotására, de mégis egy sajátos fogalmi csoportosítást igyekeztem felvázolni:

- a) Oktatás (Ki): A világunk országai, régiói különböző fejlettségi fokon állnak. Nem mindegy, hogy kik, hányan, milyen körülmények között, mekkora idő ráfordítással tudják átadni az arra igényt formálóknak. A rendelkezésre álló szakemberekkel,

⁶ <https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-magyar-etimologiai-szotar-F14D3/a-a-F14E1/analfabeta-F1640/>

⁷ <https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-magyar-etimologiai-szotar-F14D3/a-a-F14E1/analfabeta-F1640/>

⁸ Bakos Ferenc: Idegen Szavak és Kifejezések Szótára, Akadémia Kiadó, 2004

képzettségükkel, az anyagi lehetőségekkel fordított arányban áll analfabetizmus társadalmi százaléka.

- b) Származás, társadalom (Kit): A szegénység gyakran megakadályozza a gyermekeket abban, hogy iskolába járjanak, mivel a családok nem engedhetik meg maguknak az oktatás költségeit, vagy a gyermekeknek dolgozniuk kell a család megélhetéséhez.
- c) Terület (Hely): Ebben az esetben nem a földrajzi, hanem a társadalmi, kulturális és politikai megközelítést használom. Világunk sokszínű közösségeiben eltérő szokások, vallási dogmák alakultak ki és az oktatás elérhetőségének szempontjából a hátrányos megkülönböztetésnek leginkább a nők az elszenvedői.

A nemi jellegű differenciálástól eltérő az autokrata berendezkedésű politikai erők gyakorlata, amelyek könnyebben tudják hatalmukat fenntartani egy olyan környezetben, ahol az ismeretek terjedésének gátja az írástudatlanság szélesebb körű fenntartásán alapul.

- d) Képesség (Az Egyén): Léteznek olyan egészségügyi problémák, amit egyesek genetikailag magukban hordoznak, mint például a diszlexia, diszgráfia, vagy más tanulási nehézségek. Ezek az egyének gyakran vagy nem kapják meg a szükséges támogatást és segítséget, vagy a betegségük jelenti gátját a fejlődésüknek ezzel hozzá járulva hozzá az analfabetizmushoz.
- e) Modern kori környezet (New Age): A technológiai fejlődés napjainkra odáig jutott, hogy az írástudatlanság, a ki nem alakult képességek felismerése és kezelése helyett egyes társadalmi csoportok magának a kézzel való írásnak is ódivatú jelleget tulajdonítanak és megkérdőjelezzik fontosságát. A képi megjelenések térhódítása sorvasztólag hat az olvasásunkra, a technológiai adatrögzítés pedig az írásunkra, mint képességre.

Az analfabetizmus törzsfejlődése alapján az alábbiak determinálhatók:

- a) **analfabetizmus:** Olyan az egyén képesség béli állapota, aki nem tanult meg se írni, se olvasni. Ennek a csoportnak egy alcsoportjába tartozik az az individuum, aki megtanult írni és olvasni, de elsorvadt nála a képesség. A kiváltó okai lehetnek az írás, olvasás

gyakorlásának elmaradása, esetleg külső erőhatás, vagy betegség okozta agyi trauma kialakulása.

- b) A szakirodalom bevezette és használja a **funkcionális analfabetizmus** fogalmát is. A keletkezésének pontos dátumára nem sikerült ráakadni, de az 1970-es években jelenik meg először a kifejezés, amikor a fiatal felnőttek képességsökkenését figyelték meg. A funkcionális analfabetizmus területén kutató Steklács János a következőképpen definiálja a fogalmat: „funkcionális analfabéta az, aki a szűkebb és tágabb értelemben vett környezete által a számára támasztott olyan követelményeknek, amelyhez az olvasás, illetve írás képességére van szükség, minimálisan sem tud eleget tenni” (Steklács 2005a: 172). Egyszerűsítve: olyan egyéneket illeltek ezzel a kijelentéssel, akik bár el tudták olvasni az adott szöveget, de nem tudták értelmezni azt.
- c) A **szakterületi analfabetizmus** fogalma kicsit kilóg a sorból, ugyanis nem általános képesség béli állapotról beszélhetünk. Ezzel a fogalommal lehet illelteni azokat az embereket, akik bizonyos területhez, eszközhöz egyáltalán nem értenek, vagy nincs érzékük hozzá. Ezek lehetnek képesség hiányára visszavezethetők (pl. zenei, képzőművészeti), érdeklődés hiányán alapuló (pl. műszaki, digitális), vagy tanulás hiánya miatt kialakult (pl. pénzügyi).

1.2 Modern kori analfabetizmus

Az okfejtés láncolatában meg is érkeztünk a digitális-analfabetizmus fogalmához. Hogyan határozhatjuk meg az ókori kifejezés alapján mit is értünk ezen fogalom alatt? Hiányt jelent, de már nem a klasszikus formában vett írás, olvasás hiányát, hanem inkább valamilyen képesség béli fogyatékoságot. A digitális-analfabetizmus olyan kompetenciák hiányának együttesét jelenti, amelyek megléte mellett az egyén magabiztosan, hatékonyan, a kockázatok minimalizálása mellett tudja használni, felhasználni és kihasználni a digitális támogató eszközök nyújtotta lehetőségeket. A digitális technológiák és eszközök életünk szerves részévé váltak. Azok, akik nem rendelkeznek alapvető digitális készségekkel, jelentős hátrányba kerülhetnek. Az elvárások ott vannak a

- a) **Munkaerőpiacon megfogalmazott követelményekben:** A modern munkahelyi környezet kiemelt hangsúlyt fektet a digitális készségekre. Mindazok, akik nem

rendelkeznek megfelelő szintű digitális ismeretekkel, hátrányba kerülhetnek a munkaerőpiacon a versenytársaikkal szemben, nehezen találnak munkát, és kisebb eséllyel haladnak előre karrierjükben.

- b) **Társadalmi kommunikációban:** A kormányok egyre szélesebb spektrumban kommunikálnak az állampolgárokkal digitális formában, ügyfélkapukon keresztül. Azok, akik nem tudják használni a digitális eszközöket, nehezebben férnek hozzá információkhoz, szolgáltatásokhoz, lehetőségekhez, befolyásolja a tájékozottságukat és döntéshozatali képességüket, ezzel tovább nyitják a társadalmi egyenlőtlenség ollóját.
- c) **Oktatás és tanulás területén:** 2020-ban hirtelen egyik napról a másikra kellett átállni a digitális oktatásra (COVID hatás). A digitális készségek hiányoztak mind a pedagógusok, mind a diákok esetében, mind a környezetben. Számos megoldandó helyzetet alakult ki: legyen elegendő darabszámú és műszaki paraméterekkel (kamera, mikrofon) rendelkező eszköz elő, megfelelő internetkapcsolat biztosítása technikailag és a háztartások részéről anyagilag. És ha minden adott volt, akkor léptek elő a készségeken alapuló problémák: oktató szoftverek használata, csoportképzések, tananyagok továbbításának kérdése, a kamerák és mikrofonok szenzitív használata (gondoljunk bele hány alsóneműben rohangáló családtagot ismerhettek meg az osztályközösségek tagjai). Az eltelt négy esztendő sokat hozzáadott a fentiek kezeléséhez és szélesebb teret kaptak az oktatásban a digitális eszközök és platformok. Ugyanakkor a hátrányos helyzetben lévőkre még intenzívebb nyomás nehezedik, mert azok a diákok, akik nem rendelkeznek megfelelő digitális ismeretekkel, az hátrányba kerülhetnek a tanulásban és ennél fogva az életben.
- d) **Társadalmi életben:** Ez a kategória, ahol nem lehet eleget írni a felsorolásban, hol, az életünk mely területén használjuk a digitális eszközöket. Valószínűleg a komplementer halmazzal gyorsabban lehetne végezni. Egy digitális világban a digitális analfabetizmus megnehezítheti az emberek mindennapjait, illetve már lehetetlenné tesz bizonyos területen való eligazodást, társadalmi elszigeteltséghez vezethet, mivel az online platformok egyre fontosabb szerepet játszanak a kapcsolattartásban. Azok, akik nem képesek használni ezeket az eszközöket, kimaradhatnak a közösségi életből és a fontos információk áramlásából.

Összességében a bitek és byteok rohanó sztrádáján világunk hihetetlen mértékű digitális transzformáción megy át, amely azt eredményezi, hogy a gazdaságok és a társadalmak átalakulnak. Azok, akik nem tudnak lépést tartani ezzel a változással, kimaradhatnak a fejlődésből és perifériára szorulnak. Megvonhatnánk a vállunkat és azt mondhatnánk: mindig is voltak szegények, elmaradottak, most is lesznek, csak más fogalmat találunk ki rájuk. Ha ezt tennénk nem lennénk felelős szakemberek, akik felismerve a digitális-analfabetizmusban rejlő kockázatokat azt is látják; cselekedni kell. Mert mit is okozhatnak a kibertérben járatlan, vakon mozgó természetes és nem természetes személyek:

- a) **Gazdasági hátrányokat:** Az alacsony digitális készségekkel rendelkező, vagy erre kevésbé fogékony egyének hatékonysága alacsonyabb, ami a vállalkozásokra kivetítve csökkentheti a termelékenységet, növelheti a költségeket, csökkenti a profitot. Az egyén lemarad, elszegényedik, hátrányos helyzete egyre jobban mélyül.
- b) **Társadalmi elszigeteltséget:** Azok, akik nem tudják használni a digitális eszközöket, könnyen magányossá válhatnak, kirekesztődnek a társadalomból. Ez legjobban az idősebb generációkra igaz, akik nehezebben alkalmazkodnak az új technológiákhoz, gyermekeinek, rokonaik a kitágult világban fizikailag távolabb kerültek tőlük, perszonális interakciók száma lecsökken.
- c) **A demokratikus integritás eróziója⁹:** A digitális írástudás hiányában lévő lakosság nagyobb valószínűséggel válik áldozatává a félretájékoztatásnak és propagandának, ami destabilizálhatja a demokratikus folyamatokat és a nemzeti kohéziót. A közvélemény manipulálása digitális platformokon keresztül társadalmi megosztottsághoz vezethet, tovább bonyolítva a nemzetbiztonsági erőfeszítéseket (Riantodi, 2022).
- d) **Biztonsági kockázatokat:** A digitális-analfabéták nagyobb eséllyel válnak a kiberbűnözők, ellenérdekelt szervezetek áldozatává, adott esetben magukkal rántva a közösségi médiában lévő ismerőseiket, a munkaadójukat, vagy - ha csak az orosz-ukrán háború mobileszközök használatának példáit említem – saját és társaik halálát okozva.

⁹ <https://typeset.io/papers/digital-literacy-as-an-effort-to-build-national-resilience-3vb63131>

2. DIGITÁLIS ANALFABETIZMUS

2.1. Kitekintés

Az információs rendszerek robbanásszerű növekedése és növekvő függősége elképesztő. Hazánk kormányzati stratégiája, hogy olyan globális információs adatbázist alkosson meg, amely magában foglalja az elektronikus kereskedelmet (bevételek és adók), az egészségügyet, a kereskedelmi vendéglátást, a kutatási közösségeket, az oktatási rendszereket, az állampolgárok személyes adatait, azaz egy virtuális elektronikus kormányzatot. Ha ezt a hatalmas információs labirintust megzavarják, vagy behatolnak az nemzeti bénuláshoz vezet.

A civil információs infrastruktúra a nemzetbiztonság legsebezhetőbb pontja. Az ellenfelek teljes mértékben képesek kihasználni egy ország és - egy esetleges szövetségi rendszerbe tagozódása esetén – szövetségesei információs infrastruktúráját és a hozzá kapcsolódó technológiákat, hogy tönkre tegyék gazdasági-, demokratikus- és nemzetbiztonságunkat. Az gazdasági, ipari, katonai és kommunikációs technológiákra való függőség egy nemzet számára veszélyes keveréke az lehetőségeknek és kockázatoknak¹⁰.

A kibertérből érkező támadóknak előnyeik vannak az anonimitás, a jogi kétértelműség, a könnyen elérhető fegyverrendszerek, a támadási sebesség és az erőfeszítéseik nemlineáris nyereségei révén. A támadások számos forrásból és különféle módokon érkezhetnek. Az amerikai szakirodalom kedvenc szava a várható tragédiára Pearl Harbor, nekünk magyaroknak Mohács¹¹ jutott (Kovács-Krasznay 2017.).

A fenyegetés valós, veszélyes és reneszánszát élve habzsolja a jutalmát. A katonai, kereskedelmi, társadalmi, kormányzati és gazdasági szektorok technológiailag elválaszthatatlanok, a nemzetet képviselő és mindent átszövő civil információs kultúra (vagy kulturálatlanság) a nemzetvédelem érzékeny pontja.

¹⁰ <https://typeset.io/papers/national-information-systems-the-achilles-heel-of-national-821iyg3mup>

¹¹ http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_1_03_kovacs_laszlo-krasznay_csaba_-_digitalis_mohacs_2.0_kibertamadasok_es_kibervelem_a_szakertok_szerint.pdf

2.2. Digitális Analfabetizmusban rejlő Kockázatok

A digitális analfabetizmus komoly fenyegetést jelent a nemzetbiztonságra, mivel gyengíti az egyének és intézmények képességét a digitális kihívások kezelésére és reagálására. Manapság, amikor a társadalmak egyre inkább a digitális technológiákra támaszkodnak, a digitális írástudás hiánya sebezhetőségeket eredményezhet, amelyeket a potenciális ellenfelek könnyen kihasználhatnak. Ez a helyzet különösen aggasztó, mivel a digitális tájékozottság hiánya nemcsak a személyes biztonságot érinti, hanem a közszolgáltatások és infrastruktúrák védelmét is. Az alábbiakban bemutatjuk a digitális analfabetizmusnak a nemzetbiztonságra gyakorolt legfontosabb hatásait¹²:

- a) **Kiberveszélyekkel szembeni sebezhetőség¹³**: A digitális analfabetizmus gátolja a kiberbiztonsági protokollok megértését, így egyének és szervezetek könnyebben válhatnak kibertámadások áldozataivá. A tudás hiányosságai lehetőséget adnak a támadók számára, hogy kémkedjenek, vagy szabotálják az érintett rendszereket. A hibrid fenyegetések, melyek digitális nyomkövetést és adatmanipulációt alkalmaznak, tovább növelik a sebezhetőséget. Ez a jelenség különösen veszélyes, mivel a kibertámadások célja nemcsak az információk ellopása, hanem az infrastruktúrák destabilizálása is. A digitális készségek fejlesztése ezért elengedhetetlen a biztonságos online környezet fenntartásához (Wilhelmsen, 2022).
- b) **A demokratikus folyamatok eróziója¹⁴**: Azok az emberek, akik nem rendelkeznek megfelelő digitális írástudással, sokkal könnyebben esnek áldozatul a félretájékoztatásnak és a propagandának. A digitális világban való tájékozódás képessége elengedhetetlen ahhoz, hogy a felhasználók kritikusan értékelhessék az információkat. A digitális tudás hiánya miatt hajlamosabbak lehetnek elhinni a hamis híreket és manipuláló üzeneteket, így a közvélemény formálásának eszközeivé válnak. A médiát és az online tartalmakat nem képesek megfelelően elemezni, ami súlyos következményekkel járhat a társadalmi diskurzusban és a demokratikus folyamatokban. A digitális írástudás fejlesztése tehát kulcsfontosságú.

¹² <https://typeset.io/papers/digital-literacy-as-an-effort-to-build-national-resilience-3vb6313l>

¹³ <https://typeset.io/papers/kommersiell-sporing-nasjonal-risiko-12jespyd>

¹⁴ <https://typeset.io/papers/digital-literacy-as-an-effort-to-build-national-resilience-3vb6313l>

- c) **Függőség a sebezhető információs rendszerektől**¹⁵: A civil információs infrastruktúra, amelyet gyakran a digitális analfabetizmus kompromittál, kritikus sebezhetőséget jelent a nemzetbiztonság szempontjából. Az infrastruktúra zavarai nemzeti bénuláshoz vezethetnek. Ahogy a digitalizáció növekszik, a rosszul informált állampolgársággal járó kockázatok is nőnek, ami potenciálisan katasztrofális kudarcokhoz vezethet a nemzeti védelmi rendszerekben (Ross, 1997).
- d) Megoldási javaslatként egyes véleménycsoportok felvetik a **kormányzati megfigyelés** és a **digitális terek szigorúbb szabályozásának** lehetőségét. Szerintük a megoldás csökkentheti a kiberfenyegetéseket. Ez a megközelítés ugyanakkor komoly aggályokat vet fel a magánélet védelme és a demokratikus értékek megőrzése terén. A biztonság növelése érdekében tett intézkedések könnyen veszélyeztethetik a polgári szabadságjogokat, ami arra utal, hogy megfelelő egyensúlyt kell találni a védelem és az egyéni jogok között. A kihívás tehát az, hogy biztosítsuk a társadalom biztonságát anélkül, hogy sérülnének a demokratikus alapelvek (Wilhelmsen, 2022). A fenti gondolatok lényegi elemei jelen nevén Vivi Ringnes Berrefjordtól, a Védelmi Tanulmányok Intézetének Kiberprogramjának vezetőjétől és az Oslói Egyetem kutatójától származnak. A megfogalmazásából élesen kitűnik, hogy mennyire eltrének ugyanazon szövetségi rendszer (megj. NATO) tagországainak megoldási javaslatai ugyanazon problémának a kezelésére.
- e) Az USA PATRIOT Act nevű törvényt 2001. október 26-án írták alá, és célja az volt, hogy a szeptember 11-i terrortámadások után megerősítse az Egyesült Államok kormányának képességét a terrorizmus elleni harcban. A PATRIOT Act pozitív hatásai és kritikai pontjai a mai napig éles viták tárgyát képezik a világ jelenleg vezető államának társadalmában, mivel sokan úgy vélik, hogy a törvény korlátozza az állampolgárok szabadságát és sérti az alapvető jogokat, ugyanis
- Megdőntötte a magánszféra egyensúlyát:* A törvény jelentősen bővítette a kormányzati szervek jogkörét, például a telefonos és internetes megfigyelésekre, a banki tranzakciók és pénzmozgások nyomon követésére, valamint a gyanúsítottak adataihoz való hozzáférésre.

¹⁵ <https://typeset.io/papers/national-information-systems-the-achilles-heel-of-national-821iyg3mup>

Nemzetbiztonsági ok: levelek és titkos megfigyelés: A törvény lehetővé tette az FBI számára, hogy nemzetbiztonsági okokra hivatkozva a magánlevelezésbe betekinthessen és ennek segítségével titokban adatokat gyűjtsön.

Szólásszabadság és szabadságjogok: Számos jogvédő szervezet és polgári szabadságjogi aktivista szerint a PATRIOT Act túlzott megfigyelési jogokat adott a kormánynak, veszélyeztetve az állampolgárok magánszféráját és szabadságjogait, beleértve a szabad, kritikus hangvételű véleménynyilvánítást.

2.3. Többszereplős játék

Ahogy az előző idézetekből is kitűnik az állami szerepvállalás erősítése, valamint az egyén szerepe már tetten érhető a kibertér veszélyeit csökkentő tényezők között. Már ennél a két szereplőnél is felsejlik, hogy egyetlen tényező nem képes a teljes megoldás megalkotására. A kibertér folyamatosan fejlődik és egyre inkább életünk szerves részévé válik, a fenyegetések is egyre kifinomultabbak. A kiberbiztonság megteremtése többszereplős komplex feladat, amelyben az aktorok együttműködése szükséges, elengedhetetlen, hogy minden érintett fél közösen dolgozzon a védelem kialakításán. Mielőtt rátérek a munkám célcsoportjára, a globális kitekintés céljából összegyűjtöttem milyen más szereplők játszhatnak szerepet és felelősséget.

a) Nemzetközi szervezetek:

Számos szervezet játszik kulcsszerepet a globális kiberfenyegetések elleni harcban és a kiberbiztonsági szabályozások kialakításában:

- **Egyesült Nemzetek Szervezete (ENSZ):** Az ENSZ különböző bizottságai, mint például az ENSZ Közgyűlés Első Bizottsága a Leszerelés és Nemzetközi Biztonság területén, aktívan foglalkoznak a kiberbiztonsági kérdésekkel. Az ENSZ Kiberbűnözés Elleni Egyezmény kidolgozása folyamatban van, amely célja a nemzetközi együttműködés erősítése a kiberbűnözés elleni küzdelemben. Ugyanakkor a nem megfelelő előkészítés vádja és az ebből adódó tartalmi kifogások már évekkel ez előtt megszülettek¹⁶. Idén, 2024. augusztusában, amikor ez ENSZ számítógépes bűnözéssel foglalkozó ad hoc bizottsága jóváhagyta a számítógépes bűnözés elleni küzdelmet célzó első egyezményt, annak szövegével sem a digitális jogvédő szervezetek, sem a nagy technológiai cégek nem értettek egyet. Deborah Brown, a Human Rights Watch

¹⁶ <https://m.sg.hu/#gsc.tab=0>

igazgatóhelyettese és Nick Ashton-Hart, a Cybersecurity Tech Accord vezetője – utóbbi több mint 100 technológiai vállalatot, köztük a HP-t, a Metát és a Microsoftot is képviseli – arra figyelmeztettek, hogy „a küldöttek az Emberi Jogi Főbiztosság által azonosított hiányosságok közül egyikkel sem foglalkoztak”.

- **Európai Unió (EU):** Az EU számos kezdeményezést indított a kiberbiztonság területén, beleértve az Európai Unió Kiberbiztonsági Ügynökséget (ENISA), amely támogatja a tagállamokat a kiberbiztonsági stratégiák kidolgozásában és végrehajtásában. Bár az ENISA alapvetően az EU tagállamait segíti, az ügynökség nemzetközi szinten is aktívan együttműködik különböző nemzetközi és regionális szervezetekkel, mint például az EUROPOL, az INTERPOL, és az OECD, valamint a magánszektor kiberbiztonsági szereplőivel.
- **NATO:** A NATO kiberbiztonsági politikája a tagállamok védelmét szolgálja a kibertámadásokkal szemben. A szervezet 2016-ban hivatalosan is kibővítette a kollektív védelmet (azaz az 5. cikkely alkalmazását) a kibertámadásokkal szembeni védelemmel. A NATO Kibervédelmi Kiválósági Központja (Cooperative Cyber Defence Centre of Excellence - CCDCOE) Tallinnban található. A központ célja a kiberbiztonsággal kapcsolatos képzés, kutatás és gyakorlatok szervezése, valamint a tagállamok közötti információmegosztás elősegítése.
A Kibervédelmi Képességfejlesztési Program (Cyber Defence Pledge) keretében a tagállamok vállalják, hogy fejlesztik saját kiberbiztonsági képességeiket és amennyiben szükséges támogatást, segítséget nyújtanak a partneri országoknak.
- **G20:** Tagjai az elmúlt években egyre inkább felismerik a kibervédelem és a kiberbiztonság fontosságát a globális gazdaság és nemzetközi stabilitás fenntartásában. A G20 országok is foglalkoznak a kiberbiztonsági kérdésekkel, bár a szervezet nem rendelkezik kifejezetten jogi, vagy szabályozási hatáskörrel a kibervédelem területén. A G20 Kiberbiztonsági Munkacsoportja ajánlásokat dolgoz ki a pénzügyi rendszerek védelmére, feladata a közös kiberbiztonsági

szabványok kialakítása, valamint a kiberfenyegetések és támadások kezelésére irányuló globális válaszok kidolgozása.

- **ASEAN:** Délkelet-ázsiai Nemzetek Szövetsége (Association of Southeast Asian Nations) egy regionális szervezet, amely 10 délkelet-ázsiai országot tömörít: Brunei, Kambodzsa, Indonézia, Laosz, Malajzia, Mianmar, Fülöp-szigetek, Szingapúr, Thaiföld és Vietnam. Tagállamai közötti együttműködés célja többek között a régió kiberbiztonsági kapacitásainak növelése és a közös fenyegetések elleni védekezés erősítése, ennek érdekében alkották meg az ASEAN Cybersecurity Cooperation Strategy dokumentumát.
- **SAC:** Dél-Amerikai Kibervédelmi Szövetség (South American Cybersecurity Alliance) alapítása hivatalosan még nem történt meg, de az ötlet és a szükségesség már évek óta felmerült a dél-amerikai régióban. A szervezet létrehozásának mozgatórugója a regionális célok elérése, regionális együttműködés keretében.

b) Kormányok:

A regnáló politikai hatalom feladata és felelőssége a nemzeti kiberbiztonsági stratégiák kidolgozása és végrehajtása, az országok digitális védelmének a biztosítása. Az erőforrások és eszközök felhasználásának célja, hogy olyan védelmi mechanizmust, eszközparkot, tudásbázist hozzon létre és támogasson, amely képes az állam létének, működésének megvédésére, a központi rendszerek és infrastruktúrák, valamint a polgárok megóvására a kibertámadásoktól. A kiberbiztonsági stratégiák alapvetően a kiberfenyegetések megelőzésére és kezelésére kell összpontosítsanak. Az Európai Unió az ENISA (Európai Unió Kiberbiztonsági Ügynökség) révén ösztönzi a tagállamok közötti együttműködést és a közös biztonsági szabványok kialakítását.

A kormányok felelősek továbbá

- A nemzeti **kiberbiztonsági stratégiák** kidolgozásáért és végrehajtásáért. Előbbi meghatározza az ország kiberbiztonsági politikáját, szabályozását és célkitűzéseit.

- Törvények és szabályozások megalkotása útján *jogi és szabályozási kereteket* hoznak létre, előírják a biztonsági intézkedéseket, továbbá megalkotja a kiberbűnözés elleni törvényeket, adatvédelmi szabályokat.
- Nemzeti Kiberbiztonsági Központok működtetésén keresztül kezelik a kiberfenyegetésekkel kapcsolatos figyelmeztetéseket és az incidensekre adott válaszreakciókat.
- Támogatják a kiberbiztonsági kutatásokat, fejlesztéseket, valamint a kiberfenyegetések felismerésében, azok hatékony kezelésében és a digitális környezet védelme érdekében nemzeti oktatási rendszert hoznak létre és üzemeltetnek.
- Nemzetközi együttműködéseket kezdeményezésében és az abban való aktív részvételben, mindezt a globális kiberfenyegetések elleni védekezés érdekében.
- A kiberincidensekre, illetve az általuk okozott károk helyreállítása érdekében **válságkezelési terveket** hoz létre, amelyek tartalmazzák a kiberbiztonsági incidensekre adott válaszokat, kulcsszerepet játszanak a gyors és koordinált reagálásban.
- A folyamatos fejlesztésért és adaptációért, amely magában foglalja a jogi keretek megalkotásától kezdve a technikai válaszingintézkedésekig terjedő széles spektrumú intézkedési skálát.

c) Vállalatok:

A kiberbiztonsági stratégiák kidolgozásában a vállalatok felelőssége megkerülhetetlen. A digitális világ biztonságának megőrzésében, védelmének erősítésében ők azok, akik napi szinten ki vannak téve a fenyegetéseknek. A kibertámadások, mint például adatszivárgások, ransomware támadások, a vállalati rendszerek meghekkélése, súlyos pénzügyi és reputációs károkat okozhatnak a cégeknek. A vállalatoknak felelősségük, hogy megfelelő intézkedéseket hozzanak a kiberfenyegetések megelőzésére, kezelésére, utókövetésére az üzleti működésük

folyamatosságának biztosítására és az adatok védelmének érdekében. Feladatainak csoportosítása az alábbiak szerint néz ki:

- A vállalatoknak átfogó **kiberbiztonsági politikát** kell kidolgozniuk, amely meghatározza a vállalat kiberbiztonságra vonatkozó céljait, elveit és elvárásait. Ez a politika irányt mutat a vállalat minden szintjén dolgozóknak és szabályozza, hogyan kell kezelni az érzékeny adatokat, miként kell reagálni a potenciális kibertámadásokra, valamint hogyan kell végrehajtani a biztonsági protokollokat és vészhelyzeti terveket. Az ilyen politika egyértelműen meghatározza az elvárt magatartást a munkavállalók és a partnerek számára is.
- A vállalatok felelőssége az, hogy **rendszeresen értékeljék** a kiberbiztonsági **kockázatokat**, és **azonosítsák** az esetleges **sebezhetőségeket**. Az értékelés során fel kell tárniuk a gyenge pontokat, de nem csak az informatikai infrastruktúrában, amelyek potenciálisan kibertámadások célpontjaivá válhatnak, hanem a rendszert alkotó humán és fizikai tényezők esetében is. Az eredmények alapján a vállalatoknak megfelelő intézkedéseket kell hozniuk a kockázatok csökkentésére, például a hálózati védelem megerősítésére, titkosítási eljárások alkalmazására, vagy a hozzáférés-ellenőrzési mechanizmusok szigorítására, jogosultsági szintek meghatározására, elhelyezési protokollokra.
- A vállalatoknak biztosítaniuk kell, hogy minden érzékeny adat — például személyes adatok, pénzügyi adatok, szellemi tulajdon, ügyfélinformációk — megfelelő védelmet kapjon a titkosítás és a biztonságos tárolás révén. A kiberbiztonsági stratégiáknak tartalmazniuk kell az adatkezelési szabályokat és az adatbiztonság megvalósítását is.
- A **hozzáférési jogok** szigorú szabályozása segítségével **azonosítási és hitelesítési folyamatokat** kell kidolgozniuk, amivel a jogosulatlan hozzáféréseket tudják korlátok közé szorítani, ezzel csökkentve az adatszivárgás és a belső fenyegetések kockázatát.
- A kibertér fenyegetései egyenes arányban állnak a vállalatok online kapcsolódási pontjai, védelmi mechanizmusai és a csatlakozás időtartamának

szorzatával. A cégeknek állandó készenléti helyzetet kell kialakítaniuk arra az esetre, ha kibertámadás célpontjaivá válnának. A vállalatoknak rendelkezniük kell egy **incidenskezelési tervvel**, amely meghatározza a válaszlépéseket és a károk minimalizálásának módját. A tervnek tartalmaznia kell a támadás észlelését, az információk gyors megosztását az érintettekkel, az incidens kezelését, a hiba elhárításának lépéseit és a nyomozás megkezdését. Ezen kívül a vállalatoknak fel kell készülniük a **kríziskommunikációra** is, hogy kezeljék a külső személyeket (ügyfeleket, médiát, állami intézményeket). Együtt kell működniük a kormányzati szervekkel és más iparági szereplőkkel a legjobb gyakorlatok megosztása és a fenyegetések elleni közös védekezés érdekében¹⁷. Az EU az ENISA-n keresztül ösztönzi a tagállamok közötti együttműködést és a közös biztonsági szabványok kialakítását.

- A fenti rendszerre organikus és folyamatosan változó entitásra kell gondolni, ami szóhasználatomban annyit jelent, hogy a vállalatoknak folyamatosan felül kell vizsgálniuk és fejleszteniük kell a biztonsági intézkedéseiket: a rendszeres **biztonsági auditokat, sebezhetőségi teszteket, kockázatkezelési gyakorlatok frissítését**, de a kiberbiztonság egyik legfontosabb aspektusa a **felhasználói tudatosság** növelése is.

A témaválasztásom legfőbb indoka pont az volt, hogy értékelésem szerint a legnagyobb kockázatokat gyakran az alkalmazottak nem megfelelő kiberbiztonsági ismeretei okozzák. Ehhez folyamatos **képzéseket** kell tartani a munkavállalók részére, amelyben nem kizárólag a régi gyakorlatokra kell ismétlődő módon felhívni az operátorok figyelmét, de be kell építeni a külső környezetből és belső tapasztalatból származó ismereteket is.

d) Oktatási intézmények:

A szemléletmódomból adódóan a proaktív intézkedések eredményességében hiszek. Ahhoz, hogy a kríziseket megelőző lépések megtörténhessenek edukációs folyamatnak kell elindulni. A digitális jelen megkövetelné, hogy a gyermekneveléssel együtt már a szülők megtegyék az első edukációs lépéseket.

¹⁷ EU Cybersecurity Strategy: The Cybersecurity Strategy | Shaping Europe's digital future

A digitális korszak elérkezésével az információk áramlása, tárolása és kezelése soha nem látott mértékben vált globális és dinamikus folyamatokká. Az oktatási intézmények – mint a tudás központjai és a jövő generációjának nevelőhelyei – különösen fontos szereplői ennek a digitális forradalomnak. Az iskolák, egyetemek és kutatóintézetek napjainkban nemcsak tudományos kutatásokat végeznek, hanem a tanulók digitális kompetenciáinak fejlesztését is célul tűzik ki; illetve kellene kitűzniük.

Az oktatási intézmények önmagukban is hatalmas mennyiségű személyes és érzékeny adatot kezelnek, amelyek védelme és biztonságos kezelése kulcsfontosságú a biztonságos és hatékony oktatási környezet fenntartásához. Ezen adatok védelme nemcsak a digitális támadásokkal szembeni védekezést jelenti, hanem az etikai normák, jogszabályok betartását is.

A kiberbiztonság tehát nem csupán technikai kérdés, hanem alapvető etikai, jogi és társadalmi felelősségvállalás is, amelyet az oktatási intézményeknek minden szinten figyelembe kell venniük.

Az oktatási intézményeknek egyben kell megfelelniük:

- a rendszereik védelmét tekintve (megfelelő kiberbiztonsági intézkedések kidolgozása és alkalmazása);
- ki kell alakítaniuk és végre kell hajtaniuk átfogó kiberbiztonsági oktatási programokat, tudatosítani kell az alanyokban (tanulók és dolgozók), hogy tisztában legyenek a digitális környezet biztonságának fontosságával;
- együtt kell működniük az iparági szereplőkkel és a kormányzati szervekkel a kiberbiztonsági kutatások és fejlesztések terén. A kiberbiztonsági stratégiák kidolgozása az oktatásban nem csupán egy technikai kihívás, hanem szoros összefonódik az oktatás jövőjével és minőségével. Az oktatási intézményeknek képeseknek kell lenniük arra, hogy alkalmazkodjanak az új technológiai trendekhez, mint a mesterséges intelligencia, a felhőalapú szolgáltatások vagy az IoT (Internet of Things).

e) **Egyének:**

Legvégül pedig elemzés alá veszem az individuumot, magát a homo sapienst. Az egyének szerepe nemcsak a saját eszközeik és adataik védelmére korlátozódik, hanem hozzájárul a szélesebb közösség biztonságához is.

- Az **alapok elsajátítása** révén az egyén tudásával kiegészíti azokat a technikai szintű megoldásokat, amelyek együttesen eredményezhetnek sikeres küzdelmet a kibertámadások ellen. Tehát ebben az esetben nem elégséges kifejezés a *használat*, hanem helyette a *tudatos használat* jelenti a fontos láncszemet. Mit is jelent ez: biztonságos navigálást, a személyes információk védelmét, az erős jelszavak alkalmazását, a kártékony programok (malware) és a csalások időben történő felismerését.
- Az **egyén biztonsága, a személy adatvédelmének keresztül** valósul meg. Az interneten való jelenlét mindenképpen adatokat, nyomokat generál – akár közösségi média használata, online vásárlás, vásárlói véleményalkotás, éttermi, turisztikai ajánlásokról legyen szó. A személyes információk illetéktelen kezekbe kerülése súlyos következményekkel járhat, mint például identitáslopás, pénzügyi csalások, magánéleti visszaélések, tippadás bűnelkövetők részére. Az önmagunk, családunk és munkahelyünk védelme érdekében több megoldás is létezik az egyén szintjén:
 - erős jelszavak használata és azok hozzáférhetőségének megakadályozása;
 - legalább kétfaktoros autentikáció használata;
 - személyes vonatkozású információk és azok hozzáférhetőségének tudatos körbe határolása.
- A tematikus rendőrségi hírek és közérdekű reklámok nagyban elősegítik az egyén önképzését, figyelemfelhívását. Az aktuális fenyegetési trendek, az ellenük való védekezés legjobban a médián keresztül jut el az állampolgárhoz. Ez a fajta tájékoztatás segít például a phishing, mint a legelterjedtebb kibertámadási forma – amely hamis e-mailek, weboldalak, üzenetek formájában próbálja meg az áldozatokat személyes információit megszerezni – elleni védekezésben. Szintén az egyén akcióján múlik az operációs rendszerek és alkalmazások rendszeres frissítése, amelyek nemcsak új funkciókat, hanem biztonsági javításokat is jelentenek.

2.4. Megoldás keresés

Az egyén kiberbiztonsággal kapcsolatos edukációjának növelése és az állami szabályozás előtérbe helyezése két különböző, de egymást kiegészítő megközelítést jelent a kiberfenyegetések kezelésére. Mindkét megoldásnak megvannak a maga előnyei, és fontos, hogy azokat nem egymás ellen, hanem együtt alkalmazzuk a biztonságos digitális környezet kialakítása érdekében. Az egyéni edukáció előnyei több szempontból is kiemelkednek, különösen akkor, ha az állami szabályozást nemcsak kiegészítő, hanem integrált elemként kezeljük.

2.4.1 Az egyéni edukáció előnyei

Az egyéni edukáció növelése elsősorban abban rejlik, hogy az egyének közvetlen és aktív szerepet vállalhatnak saját digitális biztonságuk fenntartásában. A személyes tudatosság és ismeretek növelése lehetővé teszi, hogy az emberek ne csupán passzívan várják az állami szabályozásokat vagy intézkedéseket, hanem önállóan is hozzájáruljanak a kiberfenyegetések elleni védekezéshez. A digitális analfabetizmus csökkentése és a kiberbiztonsági alapelvek oktatása a társadalom egészére hatással lehet, javítva az egyének képességét arra, hogy felismerjék a kockázatokat, és megfelelő döntéseket hozzanak a személyes adataik védelme érdekében.

Elméleti síkon az egyéni edukáció előnye abban is rejlik, hogy a tudatos és informált állampolgárok hozzájárulhatnak egy olyan kulturális normához, amely értékeli a digitális biztonságot. Ha az egyének tisztában vannak a kiberfenyegetések mértékével és következményeivel, azzal nemcsak a saját védelmüket biztosítják, hanem hozzájárulnak a társadalom kollektív biztonságához is. Ez a szemléletváltás segíthet a digitális térben való felelősségteljesebb viselkedés kialakításában, és a társadalom egészére kiterjedő, biztonságosabb környezet megteremtésében.

2.4.2 Az állami szabályozás előnyei

Az állami szabályozás erőteljes intézkedéseket jelent, amelyek biztosítják a kiberbiztonság egységes védelmét az egész társadalomban. Az államok rendelkeznek a szükséges erőforrásokkal és jogi háttérrel ahhoz, hogy átfogó, rendszerszintű megoldásokat dolgozzanak ki, amelyek nemcsak az egyéni, hanem a vállalati és kormányzati szintű biztonságot is garantálják. Az állami szabályozás és a jogi előírások, például a személyes adatok

védelméről szóló rendeletek, közvetlenül befolyásolják a kiberbiztonsági normákat és az ipari szabványokat, amelyek irányt adnak a technológiai fejlődésnek és biztosítják a felhasználók védelmét.

Elvi szinten az állami szabályozás előnye, hogy a szabályozók képesek az egész társadalomra kiterjedő, átfogó intézkedéseket hozni, amelyek biztosítják a szabványok betartását. A kormányzati intézkedések, mint például a kibertámadások elleni védelmi stratégiák, nemcsak egyéni védelmet biztosítanak, hanem hozzájárulnak az állami és vállalati szintű kockázatok kezeléséhez is. Az államok olyan kötelező erejű előírásokat alkothatnak, amelyek egyesítik a különböző szektorokat, így az iparági szereplőknek és magánszemélyeknek is egy közös keretrendszeren belül kell működniük.

2.4.3 Egyesített megközelítés előnyei

Bár mind az egyéni edukáció, mind az állami szabályozás önállóan is hasznos, a legjobb eredményeket akkor érhetjük el, ha ezeket kombináljuk. A tudatos és jól informált egyének jobban tudják alkalmazni az állami szabályozások adta keretet, míg az állami intézkedések biztosítják, hogy a szélesebb társadalmi csoportok számára egy egységes és hatékony szabályozási környezet álljon rendelkezésre.

Az egyén szerepe abban áll, hogy a szabályozásokat saját életükben és döntéseikben alkalmazzák, míg az állami intézkedések a digitális világ komplexitását kezelik és rendszerszintű védelmet biztosítanak. Ezáltal a két megközelítés egymást erősítve járulhat hozzá egy biztonságosabb digitális környezethez.

Bár az állami szabályozás jelentős szerepet játszik a kiberbiztonságban, az egyéni edukáció kulcsfontosságú ahhoz, hogy a társadalom minden tagja felelősen és tudatosan vegyen részt a digitális világban. A legjobb megoldás az, ha az állami szabályozás és az egyéni felelősségvállalás egymást kiegészítve működik, biztosítva, hogy minden szinten hatékony védelmet nyújtsunk a kibertámadásokkal szemben.

3. A DIGITÁLIS VAKSÁG VESZÉLYE EGY NEMZET BIZTONSÁGÁRA

3.1 A lelkek sebezhetősége

A kiberbűnözés a 21. század egyik legnagyobb kihívása, amely nem csupán egyéni vagy vállalati szinten jelent problémát, hanem nemzetbiztonsági kockázatokat is rejt magában. A titkosszolgálatok és más állami szervezetek egyre inkább támaszkodnak a kibertérben végrehajtott műveletekre, legyen szó hírszerzésről, dezinformációs kampányokról, vagy kiberhadviselésről. Ezen műveletek között az érzelmi csalás, angolul „social engineering”, illetve a romantikus csalások a két legjellemzőbben használt eszköz. Az érzelmi csalások különösen veszélyesek a titkosszolgálati gyakorlatban, mivel az áldozatok, legyenek akár hétköznapi emberek, vállalati alkalmazottak vagy állami tisztségviselők, gyakran nem ismerik fel az ilyen manipulációk jeleit, ezért önként osztanak meg olyan információkat, amelyeket egyébként védenének.

Az érzelmi csalások során az elkövetők pszichológiai manipulációval és megtévesztéssel igyekeznek befolyásolni az áldozatok érzelmeit és döntéseit, hogy bizalmas információkhoz jussanak, vagy olyan cselekedeteket kényszerítsék őket, amelyek egyébként ellenállást váltanának ki belőlük. Az ilyen jellegű támadások célja, hogy egyéneket befolyásolva olyan érzékeny vagy titkos információkhoz jussanak, amelyek alapvetően nem lennének hozzáférhetők számukra.

A romantikus csalások, melyek során az elkövető a szerelem illúziójával manipulálja az áldozatot, kihasználva az áldozatok érzelmi sebezhetőségét. Az elmagányosodó modern társadalmainkban egyre gyakrabban előforduló jelenség. A digitális világ elterjedésével a távolsági kapcsolatok könnyebben kialakíthatók, ami egyben új támadási felületet is nyújt a csalóknak.

A témaválasztásom fő mozgatórugója, hogy elemezzem azokat az emberi lelki folyamatokat, amelyek biztonsági kockázatot okoznak. Azon emberi magatartásokról beszélek, amelyek az ésszel felfogható nyilvánvaló tények ellenére, arra serkentik az emberi hozzáállást, hogy higgyen a hihetetlenben. A jelenség mélyebb megértéséhez érdemes megvizsgálni a mögöttes pszichológiai mechanizmusokat.

3.2 Az érzelmi csalások szerepe a titkosszolgálatok gyakorlatában

Az érzelmi világra gyakorolt hatások, csalások alkalmazása a titkosszolgálatok számára nem új keletű, azonban a digitális kor lehetőséget biztosít arra, hogy ezek a módszerek nagyobb hatékonysággal és szélesebb körben legyenek alkalmazhatók. A gyakran alkalmazott módszerek közé tartozik a „phishing” (adathalászat), az álprofilok létrehozása, hamis információk terjesztése, vagy éppen manipulációs pszichológiai technikák alkalmazása.

A titkosszolgálatok célja az érzelmi manipulációk alkalmazásakor elsősorban információszerzés, ami lehet hírszerzési adat, ipari titok, vagy politikai döntéshozók információinak megszerzése. Továbbá, az érzelmi manipuláció alkalmas arra is, hogy befolyásolja egy-egy társadalmi csoport vagy egyén viselkedését, például választási időszakban, ahol álhírek, célzott propaganda, vagy dezinformációk terjesztésével lehet manipulálni az emberek politikai döntéseit.

3.3 Az érzelmi csalások módszerei és eszközei

Az érzelmi csalások alatt olyan pszichológiai manipulációs technikák összességét értjük, amelyek célja, hogy az áldozatokat rábírják bizalmas információik kiadására, hozzáférés biztosítására, vagy olyan cselekvések végrehajtására, amelyeket normális körülmények között nem tennének meg. Az elkövetők célja, hogy megtévesszék az áldozatokat, és kihasználják emberi gyengeségeiket, például a bizalmat, a félelmet vagy a kapzsiságot.

A romantikus csalások pszichológiai hátterének megértéséhez elengedhetetlen a csalók motivációinak feltárása. Az elkövetők gyakran nárcisztikus személyiségjegyekkel rendelkeznek, azaz túlzott önimádatra, manipulációs készségre és mások kihasználására törekednek. A hatalom és a kontroll iránti vágy szintén jelentős motiváló erőként jelenhet meg. Kevésbé jellemző mozgató rugó a társas kapcsolatok hiánya, vagy a magánytól való félelem, de ritkán ez is szerepet játszhat.

Az áldozatok szempontjából a szerelemhez és a kötődéshez való alapvető emberi igények kihasználása áll a középpontban. A csalók gyakran az áldozat sebezhetőségeit, magányát vagy önbizalomhiányát célozzák meg. A manipuláció különböző formáit alkalmazzák, mint például a szeretetbombázás, vagy az idealizálás és devalválás ciklusának ismételtetése.

Az érzelmi csalások során használt eszközök és módszerek rendkívül sokfélék, ezek közül a leggyakoribbak:

- a) **Phishing (adathalászat):** Az adathalászat célja, hogy az áldozatokat bizalmas információik önkéntes kiadására vegyék rá, például banki azonosítók, jelszavak, személyes adatok megszerzésére.
- b) **Baiting (csali):** A bűnözők vonzó ajánlatokat, vagy csaliként megjelenített fájlokat használnak, amelyek megnyitása során az áldozat gépe kompromittálódik, és hozzáférést biztosít a támadóknak.
- c) **Pretexting (álcázás):** Az elkövető egy hivatalos, hiteles szerepbe bújik – például banki alkalmazottat, rendőrt, egyéb megbízható személyt színlel -, hogy megszerezze az áldozat bizalmát és információit.
- d) **Scareware:** Félelemkeltő üzeneteket küldenek az áldozatoknak, például azt állítva, hogy rendszerük fertőzött, és azonnali lépéseket kell tenniük. Ilyenkor az áldozat gyakran magától adja át a szükséges információkat, vagy telepít káros szoftvert.

Ezek az eszközök és technikák az emberi természet gyengeségeire – a kíváncsiságra, a félelemre és a bizalomra – építenek. A mesterséges intelligencia (MI) fejlődésével újabb módszerek, például a „deepfake” videók és hangfelvételek is megjelentek, amelyek képesek tökéletesen utánozni egy valódi személyt, így rendkívül megtévesztő hatást keltve. A „deepfake” technológia lehetővé teszi, hogy például egy politikai vezető hamisított beszédek, vagy nyilatkozatokat tegyen közzé, ami zavart és félreértéseket okozhat.

A titkosszolgálatok ezeket az eszközöket többféle célra is alkalmazhatják:

- a) **Hírszerzésre és kémkedésre:** A titkosszolgálatok hagyományos célja az információszerzés, és ennek során gyakran alkalmaznak érzelmi csalásokat. A modern világban a titkos információk jelentős része elektronikus úton tárolódik és mozog, így a digitális manipulációk az információszerzés egyik leghatékonyabb módjává váltak. Az érzelmi csalások során az ügynökök sokszor olyan pszichológiai eszközöket alkalmaznak, amelyekkel beférkőznek az áldozatok bizalmába, és így hozzáférést nyernek a kívánt információkhoz. Például egy külföldi titkosszolgálat ügynökei adathalászat segítségével férhetnek hozzá egy állami hivatal érzékeny adatbázisához. Egy másik módszer lehet, hogy

az ügynök egy hiteles álprofilt hoz létre valamelyik közösségi média platformon, és célzott kapcsolatfelvétellel eléri, hogy az áldozat fokozatosan megosszon olyan részleteket, amelyek érzékeny információkat tartalmazhatnak. Az ilyen módszerek kiválóan alkalmasak arra, hogy belső információkat szerezzenek például védelmi stratégiákról, politikai döntéshozatalról, vagy éppen diplomáciai titkokról.

A titkosszolgálatok célja gyakran az, hogy érzékeny, vagy titkos információkhoz jussanak, például katonai tervekhez, diplomáciai értesülésekhez, ipari titkokhoz vagy politikai döntéshozók szándékaihoz.

- b) **Politikai befolyásolásra:** Az érzelmi csalások szintén gyakori eszközei a dezinformációs kampányoknak, amelyeket a titkosszolgálatok más országok közvéleményének vagy politikai döntéshozatalának befolyásolására használnak. A social engineering technikákat sokszor álhírek terjesztésére használják, amelyek célja, hogy zavart keltsenek egy adott közösségben vagy politikai pártban, és ezzel gyengítsék a közvélemény bizalmát.

Például egy külföldi titkosszolgálat álhíreket terjeszthet egy ország politikai vezetőiről vagy választási folyamatairól, amelyekkel célja lehet a politikai instabilitás kiváltása. Ilyen esetekben a social engineering technikákat – például hamis profillal való kommentálást, „deepfake” videók és manipulatív üzenetek terjesztését – alkalmazzák, hogy megosszák a közvéleményt, és feszültséget keltsenek. Az érzelmi csalások célzott használata egy választási kampány során például úgy irányíthatja a közvéleményt, hogy az egy adott politikai pártot vagy jelöltet részesítsen előnyben.

- c) **Dezinformáció terjesztésére:** Az érzelmi csalás a dezinformációs kampányok egyik alapvető eszköze. A titkosszolgálatok célja gyakran az, hogy megbízhatatlanná tegyenek egy kormányt, politikai vezetőt, intézményt a közvélemény szemében, így destabilizálva az adott ország politikai, vagy gazdasági helyzetét. Az érzelmi manipulációs kampányok könnyen célt érhetnek a közösségi médián keresztül, ahol hamis hírek és összeesküvés-elméletek széles körben terjedhetnek.

- d) **Kritikus infrastruktúra elleni támadás:** Az ellenérdekelt titkosszolgálatok fenti terület elleni támadásainak előfordulása legjellemzőbben egy, a célország

valamilyen cél elérésének ellehetetlenítése érdekében érhető tetten. A módszerek ebben az esetben is szinte ugyanazon alaptechnikákon nyugsznak, de a személyre szabott támadás miatt nem nélkülözhetik az egyediséget sem.

- e) **Gazdasági kémkedésre:** A titkosszolgálatok által elérendő lényeges cél a gazdasági titkok elérése. A cégek kutatási és fejlesztési eredményei, üzleti stratégiái, vagy egyéb kritikus információk fontos célpontjai lehetnek. A gazdasági kémkedés a titkosszolgálatok egyik olyan területe, ahol az érzelmi manipulációk különösen nagy jelentőséggel bírnak. Az állami titkosszolgálatok gyakran a nemzeti érdekeket védelmezve, vagy versenyelőny szerzése céljából hajtának végre ipari kémkedést. A gazdasági hírszerzés során a titkosszolgálatok gyakran alkalmazzák a „phishing”, vagy más social engineering módszereket, hogy érzékeny információkhoz, például szabadalmakhoz, kutatási eredményekhez vagy gyártási eljárásokhoz jussanak.

Egy gyakori példa, hogy egy titkosszolgálat álprofillal közelít meg egy nagyvállalat kulcsfontosságú alkalmazottját, például egy fejlesztési vagy kutatási osztály vezetőjét, és fokozatosan bizalmat épít ki vele. Az érzelmi manipuláció révén az ügynök akár munkahelyi bizalmasként is felléphet, és ráveheti a célpontot arra, hogy fontos információkat osszon meg vele. Az ilyen adatok megszerzése nagy versenyelőnyt jelenthet a származási ország számára, például a technológiai fejlesztések vagy gazdasági stratégiai tervek terén.

3.4 Az érzelmi csalások módszerének használata a titkosszolgálatok által

A titkosszolgálatok érzelmi csalásokon alapuló műveletei általában több lépcsőben zajlanak, és ezek során kifinomult módszerekkel manipulálják a célpontokat. A social engineering technikák alkalmazása lehetővé teszi a titkosszolgálatok számára, hogy célzott és hatékony információszerzési módszereket alkalmazzanak. Az érzelmi manipulációk sokszor gyorsabbak és egyszerűbbek, mint a hagyományos, technikai alapú hackelési módszerek, és az emberi gyengeségekre építve nehezebben is védhetők ki. Ráadásul ezek a módszerek nemcsak az információszerzés, hanem a politikai befolyásolás és a társadalmi feszültségek kiélezése terén is hasznosnak bizonyulnak, különösen, ha nagyszabású dezinformációs kampányokkal párosulnak.

- a) **Célpont kiválasztása és információgyűjtés:** A social engineering műveletek egyik legfontosabb lépése a célpont alapos tanulmányozása és az elérhető információk összegyűjtése. Ez magában foglalhatja az OSINT kutatás révén elérhető a közösségi médián, a nyilvános adatbázisokban és egyéb online forrásokban elérhető információk összegyűjtését. A titkosszolgálatok célzottan keresik azokat a gyengeségeket, vagy körülményeket, amelyek révén a célpontok manipulálhatók, kompromittálhatók lehetnek. Ezekre nehéz bármilyen példát is felhozni, mert a zsarolhatósági faktor mindig az egyén magatartásvonalától függ.
- b) **Kapcsolatfelvétel:** Miután a titkosszolgálat megfelelő mennyiségű információt szerzett a célpontról, megpróbál közvetlen, vagy közvetett módon kapcsolatba lépni velük. Ez történhet e-mailen keresztül, telefonon, vagy akár közösségi média platformokon keresztül. Az elkövetők sokszor álcázzák magukat, például hivatalos szervezet képviselőjeként, vagy egy megbízható barátként lépnek fel.
- c) **Tévesztés és manipuláció:** Miután a kapcsolat létrejött, a titkosszolgálat megpróbálja a célpontot érzelmi nyomás alá helyezni. Például fenyegetésekkel, jutalmakkal, vagy érzelmi manipulációval arra kényszerítik őket, hogy cselekedjenek. Ez lehet akár érzékeny adatok kiadása, egy rendszerbe való belépés vagy más, a titkosszolgálat számára hasznos cselekvés.
- d) **Bizalmas információk megszerzése:** Ha a manipuláció sikeres, a titkosszolgálat hozzájut a kívánt információkhoz. Ezek az adatok sok esetben azonnali előnyhöz juttatják a szervezetet, például politikai döntések befolyásolása, vagy kémkedési célok elérése révén. A social engineering módszerekkel megszerzett információk gyakran kritikus fontosságúak lehetnek egy ország, vagy szervezet biztonsága szempontjából.
- Ezek a sikeres műveletek alapot adhatnak további „együttműködés” kikényszerítésére is, hiszen az elkövetés igazolására minden bizonyíték a kikényszerítő nemzetbiztonsági szerv birtokában van. A minősített információ tiltott módon való átadását minden ország a legsúlyosabb büntetésekkel honorálja. Vesztenivalója ebben az esetben legtöbbször csak az elkövetőnek van...

Kutatásaim alkalmával pár példát is találtam a titkosszolgálatok által a közelmúltban alkalmazott érzelmi manipulációs technikákra:

- **APT 29 (Cozy Bear) – Orosz állami támogatású hackercsoport:** Az orosz hírszerzéshez kötődő APT 29 csoport az érzelmi csalások több formáját is alkalmazta, például a 2016-os amerikai elnökválasztás során végrehajtott phishing támadásokkal. A célpontok – politikusok, kampánystábok és hivatalos szervezetek – e-mailjein keresztül sikerült érzékeny adatokat megszerezni, amelyeket aztán politikai befolyásolásra és dezinformációs kampányokra használtak fel.
- **A kínai titkosszolgálatok kibertevékenysége:** A kínai hírszerzés az érzelmi manipulációra és a social engineering technikákra épülő módszereket alkalmaz, különösen az ipari kémkedés terén. Kínai kiberbűnözői csoportok gyakran célzott adathalászati kampányokat folytatnak nyugati cégek ellen, ahol a vállalati alkalmazottakat megfélemszik, hogy ipari titkokhoz jussanak, különösen technológiai és biotechnológiai területeken.
- **Irán és a social engineering kampányok:** Az iráni kormányhoz köthető kibertevékenységek során több esetben használták az érzelmi manipulációt politikai célok elérésére. Például iráni állami támadók olyan diplomáciai és katonai célpontokat vettek célba adathalászati támadásokkal, amelyek segítségével érzékeny adatokat próbáltak megszerezni a Közel-Kelet politikai helyzetének befolyásolására.

3.5 Másodlagos hatás

Létezik a romantikus csalásoknak olyan hatása is, amely nem közvetlenül hat a nemzetbiztonságra és első látásra kevésbé nyilvánvaló, mégis több szinten is érintik a kérdéskört.

- a) **Információbiztonság:** A csalók gyakran bizalmas információkat próbálnak megszerezni az áldozatoktól, amelyeket akár zsarolásra, akár kémiszolgálati célokra is felhasználhatnak. Különösen veszélyes lehet, ha az áldozat állami vagy vállalati titkok birtokában van.
- b) **Társadalmi kohézió:** A romantikus csalások aláássák az emberek közötti bizalmat, és negatívan befolyásolják a társadalmi kapcsolatokat. A széles körben elterjedt

csalások a társadalmi kohézió gyengüléséhez vezethetnek, ami hosszú távon a nemzetbiztonságot is veszélyezteti.

- c) **Gazdasági hatások:** A jelentős anyagi veszteségek, amelyeket az áldozatok elszenvednek, a gazdaság egészére is negatív hatással lehetnek. A csalások a fogyasztói bizalom csökkenéséhez és a befektetések visszaeséséhez vezethetnek.
- d) **Radikalizáció:** Egyes esetekben a romantikus csalások az áldozatok radikalizálódásához is vezethetnek. Ha az áldozat úgy érzi, hogy teljesen megtévesztették, és a bizalma megrendült, hajlamosabb lehet szélsőséges ideológiákhoz vagy csoportokhoz kötődni.

3.6 Védekezési lehetőségek az érzelmi csalásokkal szemben

Az érzelmi csalások elleni védekezés elsősorban a megelőzésen és a felismerésen alapul, de leegyszerűsítése elfedné a feladat komplexitását, amely magában kell foglalja a tájékoztatást, az oktatást és a jogszabályi környezet fejlesztését. Fontos, hogy az emberek tisztában legyenek a csalók által alkalmazott módszerekkel, óvatosan járjanak el az online ismerkedés során és ismétlődő jelleggel oktatáson és belső teszteken kell átesniük. Az állami szervezeteknek és a civil szervezeteknek együtt kell működniük annak érdekében, hogy felhívják a figyelmet a veszélyekre és segítséget nyújtsanak az áldozatoknak. A védekezés rétegei a következők:

- a) **Oktatás és tudatosság növelése:** Az egyének és szervezetek számára nélkülözhetetlen a kiberhigiéna oktatása, amely magában foglalja a biztonságos jelszavak használatát, a gyanús e-mailek felismerését és a bizalmas információk megfelelő védelmét.
- b) **Technológiai védekezés:** Különféle szoftverek és rendszerek léteznek, amelyek segíthetnek a gyanús tevékenységek felismerésében. Ilyenek például az adathalászati kísérletek ellen védő e-mail szűrők, az antivírus szoftverek és a tűzfalak.
- c) **Ellenőrzési rendszerek bevezetése:** Többfaktoros hitelesítés (2FA) és más biztonsági intézkedések bevezetése csökkenti annak kockázatát, hogy egy egyszerű jelszólopás révén egy támadó hozzáférést nyerjen érzékeny adatokhoz.

- d) **Pszichológiai ellenálló képesség növelése:** Az embereknek fontos tudniuk, hogy az érzelmi manipulációra alapuló támadások ellen legjobban tudatosság és óvatosság révén védekezhetnek.

3.7 Individuumban rejtőző kockázatok

A vizsgált kockázati terület eddig abból a szempontból került vizsgálat alá, amikor a kezdeményező valamilyen nemzetbiztonsági szerv és a támadást szándékos cselekvés mozgatja. Számolni kell azzal a lehetőséggel is, amikor az egyén maga kreálja a kockázatot, a magatartása sodorja önmagát és a képviselt területet támadható helyzetbe.

Az érzelmi csalások komoly veszélyt jelentenek a nemzetbiztonságra. Néhány főbb kockázati terület:

- a) **Titkos információk kiszivárgása:** Amennyiben egy állami szervezet alkalmazottai manipuláció áldozatává válnak, például phishing támadások révén, könnyen hozzáférhetnek olyan titkos információkhoz, amelyek veszélybe sodorhatják az ország belső biztonságát. Például egy védelmi minisztériumi alkalmazott hitelesnek tűnő üzenetre válaszolva kiszolgáltathatja az intézmény hozzáférési adatait.
- b) **Kritikus infrastruktúra támadása:** Az érzelmi manipulációval elért támadások a kritikus infrastruktúrák ellen is irányulhatnak, például energiahálózatok, vízművek vagy egészségügyi rendszerek ellen. Egy jól szervezett, social engineering módszereken alapuló támadás lehetővé teszi, hogy az ilyen rendszerekbe behatolva leállításokat, vagy károkat okozzanak, komoly nemzetbiztonsági problémákat generálva.
- c) **Gazdasági kémkedés és ipari titkok megszerzése:** Az érzelmi csalások révén a titkosszolgálatok vállalatokból és kutatóintézetekből is ki tudják nyerni a titkos kutatási adatokat, új technológiai megoldásokat, amelyek stratégiai előnyt biztosíthatnak egy másik ország számára.
- d) **Nemzetközi politikai kapcsolatok destabilizálása:** A social engineering eszközeivel könnyen kialakíthatók konfliktusok nemzetek között, ha sikerül olyan álhíreket, vagy információkat terjeszteni, amelyek gyanút keltenek a felek között. Ez akár diplomáciai válságot, vagy háborús feszültséget is kiválthat.

- e) **Dezinformációs kampányok:** A titkosszolgálatok vagy más állami szervek érzelmi csalásokat és social engineering technikákat alkalmazhatnak dezinformációs kampányok végrehajtására. Ilyenkor például álprofilok révén politikai beavatkozást eszközölhetnek más országok politikai folyamataiba, például választásokba.
- f) **Illegális tevékenységek finanszírozására:** A csalások útján megszerzett pénz segítségével fenntartják és tovább fejlesztik az alvilági tevékenységüket, mint például a terrorizmust, a szervezett bűnözést. A megszerzett személyes adatok birtokában a csalók további bűncselekmények elkövetésére követhetik el.

Az érzelmi csalások és a social engineering technikák kiemelkedő szerepet játszanak a modern titkosszolgálati műveletekben, komoly veszélyt jelentve az egyénekre, vállalatokra és az államok nemzetbiztonságára egyaránt. Az ilyen típusú támadásokkal szembeni védekezés legfontosabb elemei a tudatosság növelése, a megfelelő technológiai védelem és a pszichológiai ellenállóképesség fejlesztése.

Ajánlott a nemzetközi együttműködés és információmegosztás fokozása, hogy a titkosszolgálatok és egyéb biztonsági szervezetek gyorsan és hatékonyan reagálhassanak az ilyen támadásokra. Az érzelmi csalások nem csupán egyének, vagy szervezetek problémáját jelentik, hanem globális kihívást, amely alááshatja a nemzetközi stabilitást és biztonságot.

KÖVETKEZTETÉSEK

A téma feldolgozása során egy átfogó áttekintést és megerősítést kaptam arról, hogy egy, a bűnözői oldal által használt reneszánszát élő eszköz, a kibertér, mennyire állandó és folytonosan megújuló kockázatot hordoz magában a számos előnye mellett. A digitalizáció rohamos fejlődésével a kibertér egyre inkább a társadalmi, gazdasági és politikai folyamatok központi színtere lett. A mai generáció már beleszületik a digitális korba és a 70 évvel idősebb korosztály szintén részét képezi a társadalomnak. Függőségek alakulnak ki, ami nem feltétlenül jelent pszichológiai értelemben vett fogalmat, hanem azt, hogy a digitális eszközök használata megkerülhetetlenné válik. Példaként említeném a Magyarországon 2022-ben elfogadott Digitális Állampolgár programját és annak társadalmi következményeit: aki nem képes megfelelő szinten alkalmazni, az lemarad, amely a társadalmi egyenlőtlenséget tovább növeli. A digitális fejlesztés és fejlődés a digitális kiszolgáltatottság irányba tereli a társadalmat, amennyiben nem fordítunk elegendő figyelmet és fektetünk be energiát a szerényebb lehetőségekkel bírók, illetve a területen tapasztalatlanabbak képzésére. Ezzel párhuzamosan együtt mozog a kiberbiztonság kérdése is, ezért kapott részemről is fokozott figyelmet. A kibertámadások egyre kifinomultabbá és pusztítóbbá válásával a kockázatokat is növelik. Az előtálalt szakirodalom, a konferenciákon elhangzott szakértői előadások és megfogalmazott vélemények, valamint a saját szakmai tapasztalatom egyértelműen rámutatnak arra, hogy a kiberbiztonság, illetve annak hiánya és az utóbbinak egyik eredője, a digitális analfabétizmus, szorosan összefonódik a nemzetbiztonság kockázataival.

A társadalom egyre szélesebb rétege rendelkezik informatikai eszközökkel, egyre több családban jelennek meg a kényelmesebb életet biztosító okos eszközök. Ha elfogadjuk tézisként, hogy a kibertámadások egyre szélesebb spektrumban jelennek meg, finomodnak, fejlődnek és mindezek mellé odavesszük azt, hogy a kibertér használatát hány órában tanulják a diákok, hogy a védekezés és kármentesítés ember közeli környezetben legtöbb esetben hiányzik, akkor egyértelműen kijelenthetjük, hogy jelen korunkban a kibertér bűnözőinek pusztítóbbá váló cselekményeire alig vagyunk felkészülve. Ugyanakkor az elmúlt másfél év szakmai tapasztalatai azt is megmutatták, hogy az emberi felelőtlenség határtalan, ha potenciális nyereségről, valaminek az elvesztéséről, vagy éppen szexuális aktus reményéről van szó. Ezekben a helyzetekben az emberi tudat beszűkül és a többszöri felvilágosító előadások ellenére önként lépnek a medvecsapdába, amely ritkán ereszti el őket veszteség nélkül. Azon *feltevésemet, hogy a technológiák fejlődését nem követi le a felhasználók*

tudásának és tájékozottságának gyarapodása kiegészíteném azzal, nem hogy nem követi le, de a megszerezettakat sem alkalmazzák eredményesen.

A szakirodalom bőségesen foglalkozik a kiberbiztonság és a nemzetbiztonság kapcsolatával. Az empirikus tapasztalatok alátámasztják, hogy a kibertámadások gazdasági károkat okoznak, aláássák a társadalmi bizalmat és akár politikai instabilitáshoz is vezethetnek. A nemzetbiztonság szempontjából a kritikus infrastruktúrák, például a honvédelem területe, az energiaszolgáltatás, a közlekedési és a pénzügyi rendszerek védelme kiemelt fontosságú.

A beosztásomból adódó tapasztalatok leginkább humán oldalról láttatják velem ezt a világot. Ezek az empirikus megfigyelések azt mutatják, hogy a kiberfenyegetések rendkívül változatosak és gyorsan fejlődnek. A támadók egyre kifinomultabb technikákat alkalmaznak, és képesek alkalmazkodni a védelmi intézkedésekhez, amely ebben az esetben az egyén felkészültségi szintjének felelnek meg. A kockázatok tekintetében a biztonsági szakértők számos területet azonosítanak. Az egyik legnagyobb veszélyt az államok által támogatott kibertámadások jelentik, amelyek célja lehet az ellenfél gazdasági gyengítése, politikai befolyásolása, vagy katonai előny megszerzése. További aktorok a támadók oldalán a szervezett bűnözői csoportok, akik szintén jelentős fenyegetést jelentenek, hiszen ők állnak a legtöbb kibertámadás mögött. Az anyagi haszonszerzést előtérbe helyező agresszió az egyén, a katona életvitelében okozhat olyan negatív elváltozást, amely fókuszcsökkenéshez vezet. Abban az élethelyzetben, amikor a figyelem alulmúlja a biztonsági protokollok alsó szintjét, a nemzetbiztonsági kockázat mértéke exponenciálisan növekszik, *a digitális analfabetizmus egy bizonyos szint felett kihat egy ország nemzetbiztonságára*. Ennek a tézisnek van egy közvetlen diagnosztizálható hatása, amikor egy akció, vagy annak elmaradása okoz incidenst. Az alapfeltevés megerősítését egyben úgy fogalmaznám át, hogy létezik egy másik síkon létező kockázat, amikor a biztonsági eseménynek a személyre gyakorolt következménye hat ki a katona magatartására (elveszíti vagyonának egy részét, vagy kompromittáló adatok, képek kerülnek ki róla) és vonja el figyelmét a biztonsági protokollok alkalmazásáról.

A nemzetbiztonság szempontjából a kiberbiztonság erősítése ezért több szinten is szükséges. Az egyik legfontosabb feladat az infrastruktúra, az információs hálózatok védelme, a jogosulatlan hozzáférések minimálisra csökkentése, a személyi tévedések, szabotázsok megelőzése. Ez a gondolat megfelel annak a kiberbiztonsági stratégiák kialakításával szemben támasztott követelménynek, hogy figyelembe kell venni a többszintű védelem elvét. Ez azt jelenti, hogy a védekezést több rétegben kell felépíteni, hogy a támadóknak minél nehezebb legyen behatolni a rendszerbe. A technológiai megoldások mellett fontos szerepet játszik az

emberi tényező is, hiszen a legtöbb kibertámadás a felhasználói hibák kihasználásával történik. Ezért a felhasználókat folyamatosan tájékoztatni és képezni kell a legfrissebb kiberbiztonsági kockázatokról és – sokan elfelejtik – a védekezés módjairól. Annak a *hipotézisemnek, miszerint a társadalom egyes szereplői egyedül nem képesek tartós sikert elérni, ehhez együttműködés és koordináció szükséges*, a fenti többszintű védelmi szint megalapításáról szóló védelmi tézis ad megerősítést. Ennek egyik megközelítése szerint az intézkedéseket adott intézményre kell letükrözni, de államirányítási és nemzetgazdasági szinten gondolkodva globális kereteket teremtenek és eszközöket adnak a szereplők kezébe. A dinamikusan változó kiberkockázatok kezelése folyamatos interakciót igényel.

Összefoglalva elmondható, hogy a kiberbiztonság és a nemzetbiztonság szorosan összefonódott. A kibertámadások egyre kifinomultabbá válnak, és jelentős kockázatot jelentenek az államok, a vállalatok és az egyének számára. A kiberbiztonság erősítése nemcsak a gazdasági érdekeket, hanem a politikai stabilitást és a társadalmi biztonságot is szolgálja. A szakirodalom, a konferenciákon elhangzottak és a szakértők által elmondottak egyértelműen rámutatnak arra, hogy a kiberbiztonság komplex kérdés, amelynek megoldása hosszú távú és összetett feladat, számos megközelítési módot említ, többek között a technológiai fejlődés hatásait, a kiberfenyegetések fajtáit és a védekezési stratégiákat. A személyes tapasztalatok is jelentős szerepet játszanak a kiberbiztonsági intézkedések kialakításában, mivel a különböző szinteken dolgozó szakemberek eltérő látásmódot és megoldásokat hoznak a problémák kezelésére. A szakértők által elmondottak különösen értékesek, mivel gyakran első kézből származó tapasztalatokat és mélyreható elemzéseket tartalmaznak, többek között az előbbi miatt született meg ez az írás.

Értékelésem szerint a kiberbűnözés okozta incidensek hagyományos kezelése mellett (felismerés és jelzés, értékelés, válasz, tanulás és javítás) a jövőbeni kihívásokra is proaktív módon kell felkészülni és felelni az alábbi jellemzők alkalmazása mellett: tervezés, tárolás, fejlesztés, rendszeresség, folyamatosság, együttműködés. Ahogyan a bevezetőben is megemlítettem: a technológia fejlődés sztrádáján nincs megállás, újabb és újabb kihívások jelennek meg, amelyekből párat már most is láthatunk: az MI szerepe és alkalmazása, kvantum számítógépek megjelenése, a hálózatok és a hálózatra kapcsolat okos eszközök számának emelkedése. A gép forog, de az alkotó nem pihenhet...

FELHASZNÁLT IRODALOM

Jogszabályok

Magyarország Alaptörvénye

Elérhető: <https://www.parlament.hu/irom39/02627/02627.pdf>

Letöltés dátuma: 2024. október 15.

2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

Elérhető: <https://njt.hu/jogszabaly/2023-23-00-00.7>

Letöltés dátuma: 2024. november 14.

2024. október 23-ig volt véleményezhető az új, Magyarország kiberbiztonságáról szóló törvénytervezet. Az új jogszabály hatályon kívül helyezné a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvényt. A törvénytervezet egyrészt az Európai Unió jogának való megfelelést szolgálja a NIS 2 irányelv nemzeti jogba történő átültetésével, másrészt az állami szervek és az állam szempontjából kritikus tevékenységet ellátó szervezetek stabil működéséhez járul hozzá, elektronikus információs rendszerei kiberbiztonságának növelése révén.

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

Elérhető: <https://njt.hu/jogszabaly/1995-125-00-00.77#CI>

Letöltés dátuma: 2024.október 15.

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

Elérhető: <https://njt.hu/jogszabaly/2013-50-00-00>

Letöltés dátuma: 2024.október 28.

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

Elérhető: <https://njt.hu/jogszabaly/2011-112-00-00.47#CI>

Letöltés dátuma: 2024.október 28.

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

Elérhető: <https://njt.hu/jogszabaly/2023-10-20-8K>

Letöltés dátuma: 2024.október 28.

10/2023. (V. 15.) SZTFH rendelet az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról

Elérhető: <https://njt.hu/jogszabaly/2023-10-20-8K>

Letöltés dátuma: 2024.október 28.

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

Elérhető: [1139/2013. \(III. 21.\) Korm. határozat - Nemzeti Jogszálytár](#)

Letöltés dátuma: 2024.október 28.

186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről

Elérhető: [186/2015. \(VII. 13.\) Korm. rendelet - Nemzeti Jogszálytár](#)

Letöltés dátuma: 2024.november 10. (hatályos: 2024. december 31.)

187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

Elérhető: [187/2015. \(VII. 13.\) Korm. rendelet - Nemzeti Jogszálytár](#)

Letöltés dátuma: 2024.november 10.

270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről

Elérhető: [270/2018. \(XII. 20.\) Korm. rendelet - Nemzeti Jogszálytár](#)

Letöltés dátuma: 2024.november 10.

271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól

Elérhető: [271/2018. \(XII. 20.\) Korm. rendelet - Nemzeti Jogszabálytár](#)

Letöltés dátuma: 2024.november 08.

214/2020. (V. 18.) Korm. rendelet az elektronikus információbiztonsági korai figyelmeztető rendszerről

Elérhető: [214/2020. \(V. 18.\) Korm. rendelet - Nemzeti Jogszabálytár](#)

Letöltés dátuma: 2024.november 08.

1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról

Elérhető: [1838/2018. \(XII. 28.\) Korm. határozat - Nemzeti Jogszabálytár](#)

Letöltés dátuma: 2024.október 28.

7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

Elérhető: [7/2024. \(VI. 24.\) MK rendelet - Nemzeti Jogszabálytár](#)

Letöltés dátuma: 2024.november 14. (hatályos: 2024. december 31.)

Európai Parlament és Tanács 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról

Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0679>

Letöltés dátuma: 2024.október 28.

Európai Unió Kiberbiztonsági Ügynökség, ENISA (European Union Agency for Cybersecurity)

Elérhető: [ENISA](#)

Letöltés dátuma: 2024. október 28.

CETS 185 Convention on Cybercrime, avagy a Budapesti "A kiberbűnözés elleni " Egyezmény, (2001)

Elérhető: [CETS 185 - Convention on Cybercrime](#)

Letöltés dátuma: 2024. október 22.

Council of Europe: Cybercrime and Cybersecurity Strategies in the Eastern Partnership region. (2019), Results of series of national workshops Eastern Partnership countries Cybercrime, EAP 2018

Elérhető: <https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c>

Letöltés dátuma: 2024. október 25.

Deborah Fry: We found over 300 million young people had experienced... (2024)

Elérhető: <https://theconversation.com/we-found-over-300-million-young-people-had-experienced-online-sexual-abuse-and-exploitation-over-the-course-of-our-meta-study-229039>

Letöltés dátuma: 2024. október 23.

Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról (2005)

Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52005DC0576>

Letöltés dátuma: 2024. november 10.

2004. évi XXIX. törvény az európai uniós csatlakozással összefüggő egyes törvénymódosításokról, törvényi rendelkezések hatályon kívül helyezéséről, valamint egyes törvényi rendelkezések megállapításáról

Elérhető: [2004. évi XXIX. törvény - Nemzeti Jogszabálytár](#)

Letöltés dátuma: 2024. október 22.

Szakirodalom

Krasznay Csaba: Húsz év a globális kiberbűnözés elleni küzdelemben – A Budapesti Egyezmény értékelése. (2021), Külügyi Szemle

Elérhető: https://doi.org/10.47707/Kulugyi_Szemle.2021.2.09

Letöltés dátuma: 2024. október 22.

Kovács László – Krasznay Csaba: Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. (2010), Nemzet és Biztonság

Elérhető: https://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo_krasznay_csaba-digitalis_mohacs_.pdf

Letöltés dátuma: 2024. október 22.

Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. (2017), Nemzet és Biztonság

Elérhető: http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_1_03_kovacs_laszlo-krasznay_csaba_-_digitalis_mohacs_2.0_kibertamadasok_es_kibervedelem_a_szakertok_szerint.pdf

Letöltés dátuma: 2024. október 22.

Simon László – Dr. Magyar Sándor: A terrorizmus és indirekt hatása a kiberterében. (2017), Nemzetbiztonsági Szemle MMXVII/III, 89.101. o.

Elérhető: <https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1685/991>

Letöltés dátuma: 2024. október 22.

Steklács János: Funkcionális analfabetizmus a hipotézisek, tények és számok tükrében. (2005), Akadémiai Kiadó, 132 oldal

Steklács János: A funkcionális írásbeliség társadalmi és pedagógiai kontextusban. (2005) In: Anyanyelvi nevelési tanulmányok I., Iskolakultúra, Pécs. 170–183.

Riantodi (Rian Rian): Digital Literacy as an Effort to Build National Resilience. (2022), Journal of Digital Law and Policy

Elérhető: <https://typeset.io/papers/digital-literacy-as-an-effort-to-build-national-resilience-3vb63131>

Letöltés dátuma: 2024. október 23.

Vivi Ringnes Wilhelmsen: Kommersiell sporing – nasjonal risiko. (2022), International Politikk

Elérhető: <https://typeset.io/papers/kommersiell-sporing-nasjonal-risiko-12jespyd>

Letöltés dátuma: 2024. október 23.

Lieutenant Colonel (US Army) Mitchell S. Ross: National Information Systems: The Achilles Heel of National Security. (1997), Startegy Research Project

Elérhető: <https://typeset.io/papers/national-information-systems-the-achilles-heel-of-national-821iyg3mup>

Letöltés dátuma: 2024. október 24.

Mák Bence: A kibertérben elkövetett bűncselekmények különösen a társadalmi megítélés tükrében. (2024), Comparative Law Working Papers – Volume 8. No. 2. 2024 - Hallgatói különszám

Elérhető: [A kibertérben elkövetett bűncselekmények](#)

Letöltés dátuma: 2024. október 24.

Steve MORGAN: McAfee Vastly Underestimates The Cost Of Cybercrime. (2020), Cybercrime Magazine

Elérhető: [McAfee Vastly Underestimates The Cost Of Cybercrime](#)

Letöltés dátuma: 2024. október 24.

Simon Béla, Gyarakai Réka, at all: „Kiberbűnözés” in Kiss Tibor (szerk.): Kibervédelem a bűnügyi tudományokban. (2020), Ludovika Egyetemi Kiadó, 95–119.

Elérhető: [Kibervédelem a bűnügyi tudományokban - Ludovika könyvek](#)

Letöltés dátuma: 2024. október 26.

Egyéb forrás

Nemzetközi statisztikai adatok

Elérhető: www.statista.com

Letöltés időpontja: 2024. október 20 2024. november 13.)

Kaspersky (private international cybersecurity company): What is cybercrime? How to protect yourself. (2024)

Elérhető: <https://www.kaspersky.com/resource-center/threats/what-is-cybercrime>

Letöltés dátuma: 2024. október 24.

SEON: Global Cybercrime Report, (2023)

Elérhető: <https://seon.io/resources/global-cybercrime-report/>

Letöltés dátuma: 2024. október 24.

FBI: Parents, Caregivers, and Teachers: Protecting Your Kids

Elérhető: <https://www.fbi.gov/how-we-can-help-you/parents-and-caregivers-protecting-your-kids>

Letöltés dátuma: 2024. október 23.