ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

BEDERNA ZSOLT

A kiberbiztonság az Európai Unió szabályrendszerében.
A kockázatok és incidensek kezelésére vonatkozó elvárások és lehetőségek, az incidensek potenciális hatásainak elemzése

Témavezető: Prof. Dr. Rajnai Zoltán

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024. március 17.

Nyilvános védés teljes bizottsága:

Elnök:

Prof. Dr. Molnár György

Titkár:

Dr. Pető Richárd

Tagok:

Dr. habil. Sánta Róbert

Dr. habil. Szádeczky Tamás

Dr. habil. Istók Róbert

Bírálók:

Dr. habil. Farkas Tibor

Dr. Jobbágy Szabolcs

Nyilvános védés időpontja:

2024

TARTALOMJEGYZÉK

BEVEZETÉS

A posztindusztriális változások a társadalom számos területére hatást gyakorolnak, amelyeket az információs társadalom fogalma hivatott azonosítani és keretbe foglalni. Bár az első meghatározás az 1960-as évekből származik, de még ma sincs konszenzus a definíciót illetően. Ez abból fakad, hogy a kutatók az elmúlt évtizedek során több szempontból közelítették meg a kérdéskört [1]. E perspektívákat Webster [2] foglalta össze, kiemelve az információs társadalom technológiai, kulturális, térbeli, foglalkozási és gazdasági jellemzőit. Az információs társadalom legelterjedtebb meghatározásai az információs és kommunikációs technológiák (IKT) jelentőségének növekedését okozó technológiai szempontokat hangsúlyozzák, amelyek annak kialakulását és fejlődését biztosítják, amely nem annak fényében nem meglepő, hogy a technológiai változás exponenciális jellegű, ahogy Kurzweil [3, p. 381] szerint a technológia történelmének elemzése rámutat.

A technológia és a globalizáció gyors fejlődésével és konvergenciájával az információs társadalom egy új életformaként is azonosítható. Ezek az életmódbeli változások funkcionális, viselkedési és kulturális változásokat indukálnak [2]. A térbeli megközelítés szerint az IKT használatának és a globalizációnak köszönhetően a fizikai tér jelentősége az embereket körülvevő hálózatok miatt lecsökkent, új keretet biztosítva a társadalmi folyamatokhoz. A kulturális megközelítés szerint az információs társadalom a fokozódó jelentőséggel bíró, globális digitális média (pl. a közösségi oldalak) eredménye, amelyek erodálták az emberek közötti távolságot, számos kulturális jellegű változást okozva [4].

Az információs társadalom gazdasági és foglalkozási vonatkozásai szerint az információs szektor és az információs jellegű munka uralja a gazdaságot. A foglalkozási megközelítés Bell posztindusztriális elmélete alapján írja le az információs társadalmat, amelyben a legtöbb munkakör az információhoz és a kapcsolatos folyamatokhoz köthető [5]. Ezzel összefüggésben az Európai Unió az információs társad almat az IKT alkalmazásán alapuló, az információ létrehozására, elosztására, felhasználására és újra felhasználására összpontosító tevékenységként jellemzi [6]. A gazdasági és foglalkoztatási szempontok kapcsán az Európai Unió számára az egységes közös piac meghatározó jellegű, amely Micossi [7, p. 32] szerint az elmúlt harminc év során lenyűgöző fejlődést ért el, érintve az ipari termeléstől kezdve a közműszolgáltatásokat és az állami szolgáltatásokat. Az Európai Unió Digitális Gazdaság és Társadalom Indexe (Digital Economy and Society Index – DESI) 2014 és 2022 között összefoglalta Európa digitális teljesítményére vonatkozó mutatókat, és nyomon követte az uniós országok előrehaladását. 2023-tól és a 2030-ig tartó időszakra vonatkozó digitális évtized szakpolitikai programmal összhangban a DESI beépül a digitális évtized helyzetéről szóló jelentésbe, és a digitális célok megvalósítása terén elért eredmények nyomon követésére szolgál a (1) Digitális készségek, (2) Digitális infrastruktúra, (3) A vállalkozások digitális átalakulása és (4) A közszolgáltatások digitalizálása

területeken. Mindez jól jelzi, hogy az IKT manapság már nem egy specifikus ágazat, hanem minden modern innovatív gazdasági rendszer alapja [8].

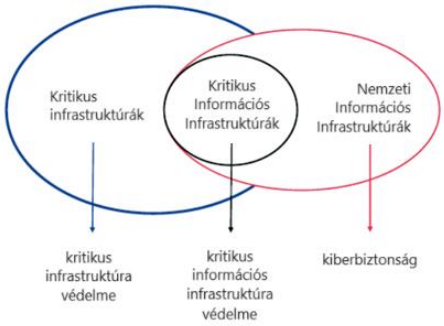
Továbbá az IKT fejlődése alapjaiban járult hozzá a kibertér létrejöttéhez, amely – az információs társadalom fogalmához hasonlatosan – többféle meghatározással bír [9] (pl. Európai Uniós Kiberbiztonsági Ügynökség (European Union Agency for Cybersecurity – ENISA) [10, p. 7], Kuehl [11, p. 28], Kovács [12, p. 18], Haig [13, p. 226]). Mindazonáltal a meghatározások egységesen rávilágítanak arra az összefüggésre, hogy az IKT egyik legnagyobb jelentősége az adatok kezelésében, rendszerezésében és feldolgozásában rejlik, amely alapján információt szolgáltatnak kezelője, felhasználója számára.

Munk [14, pp. 120–123] szerint a kiberteret az információs környezet valós részhalmazának tekintjük, ahol az információs környezet információkat gyűjtő, feldolgozó vagy elosztó személyek, szervezetek vagy rendszerek, valamint maguknak az információknak az összességeként értelmezett. A kibertérben, csökkentve az államhatárok jelentőségét és szerepét, megannyi állami és nem állami szereplő is megjelenik. Berzsenyi szavaival élve „*a kibertérben a nemzetállamok korántsem egyeduralkodók, a társadalom megannyi szereplője megtalálható ott a multinacionális cégektől a szervezett bűnözői és aktivista csoportokon át egészen az egyéni felhasználóig*" [15, p. 70]. Ugyanakkor minden állami és nem állami szereplő különböző módokon és eltérő mértékben képes érdekeinek érvényt szerezni a fölény megszerzése és fenntartása érdekében [16, p. 69]. Másként fogalmazva azt a realitást kívánják kelteni, hogy bizonyos szempontból különb, erősebb, fejlettebb, jobb, hatékonyabb, végső soron eredményesebb a másiknál politikai, gazdasági, katonai stb. szempontok szerint [17, pp. 79–81].

Mindebben nagy szerep jut az IKT szolgáltatásoknak, hiszen az IKT az információs társadalom zavartalan működéséhez számos nélkülözhetetlen rendszert és eszközt, azaz infrastruktúrát biztosít, amelyek a társadalom és a gazdasági élet funkcióit támogatják [18, p. 36]. Ryba elemzése szerint a kritikus infrastruktúrákat változatos információs rendszerek alkotják vagy támogatják azok működését, amelyek vonatkozásában két alapvető kategóriát lehet megkülönböztetni [19]. Az egyik az állampolgárokat közvetlenül célzó szolgáltatásokat (pénzügyek, kommunikáció, segélyszolgálatok stb.) kínáló kritikus infrastruktúra rendszerek, amelyek az üzleti folyamatokat, adatgyűjtést és -feldolgozást támogatják és az információs technológia (information technology – IT) alapú megoldásokra épülnek. A másik az ipari tevékenységekhez (kitermelés, gyártás, feldolgozás stb.) kapcsolódó kritikus infrastruktúrákat megvalósító információs infrastruktúrák, amelyekben az üzemeltetési rendszerek (operational technology – OT) játszanak kulcsszerepet (pl. üzemek vízkezelése, vízgazdálkodás, műtrágya és mezőgazdasági vegyipar, vegyi üzemek, üzemi szennyvízkezelés, bányák és fémek, energiaterv és kazánvezérlés, autógyártás, kohászati feldolgozó üzemek, papírmérföldek és cellulóz, minőségellenőrzés, finomítók és petrolkémiai, élelmiszer-feldolgozás és gyógyszergyártás [20]). A két

eltérő működési környezetet alapjaiban befolyásolja az IT/OT konvergencia, azaz az OT közelítése és integrálása az IT megoldásokban [21], amely következtében a két terület közötti működésbeli különbség egyre inkább elmosódik. Muha és Krasznay [22, p. 11] rámutatott az IT/OT konvergenciából fakadó összefüggésre, miszerint az IKT alapú rendszereket egységesen elektronikus információs rendszereknek nevezzük. „*Figyelemre méltó az a tény, hogy napjainkban szinte valamennyi létfontosságúnak (kritikusnak) minősített, minősíthető infrastruktúra nemcsak használja az elektronikus információs rendszereket, hanem egyre erősebben függ ezektől*" [22, p. 16].

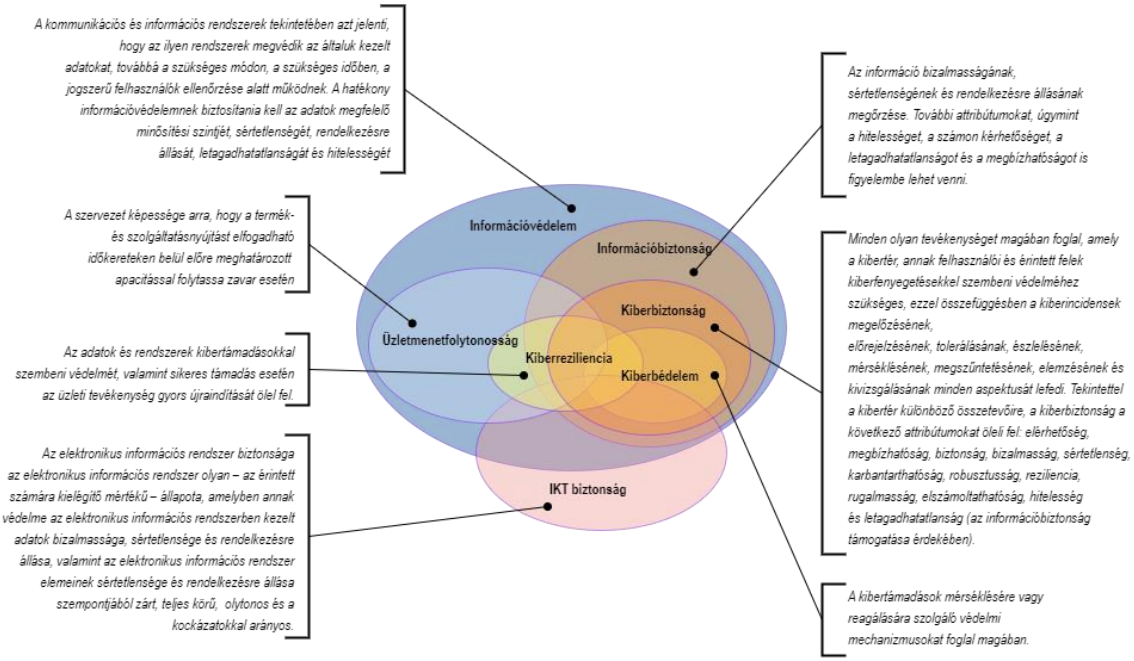
A kritikus infrastruktúra, a kritikus információs infrastruktúra és a kibertér összefüggésében Dunn Cavelty et al. [23, pp. 17–20] rámutatott, hogy míg a kritikus infrastruktúra védelme (CI protection – CIP) egy nemzet infrastruktúrájának minden kritikus szektorát magában foglalja, a kritikus információs infrastruktúra védelem (critical information infrastructure protection – CIIP) annak részhalmaza, továbbá a CIIP, jellegéből adódóan jelentős kitettséggel rendelkezik a kiberbiztonság ellenében (1. ábra). Másként fogalmazva a CIP a kritikus infrastruktúra védelmének összességét fedi le különböző szektorokban, a CIIP a mögöttes információs infrastruktúra védelmére összpontosít. Továbbá tekintettel a kritikus információs infrastruktúrák és a kibertér összefonódására, a CIIP a kiberbiztonsággal is szoros kapcsolatban áll, szerves részét képezve annak. Ezeket az összefüggéseket egy, az ENISA által készített tanulmány [24] is megerősíti.



1. ábra. Kritikus infrastruktúra (védelem), kritikus információs infrastruktúra (védelem) és a kibertér (kiberbiztonság) kapcsolata
Forrás: Saját szerkesztés [23, p. 20] alapján

Mindezek értelmében a kritikus információs infrastruktúra védelem megvalósításában a defenzív kiberbiztonsági képességeknek meghatározó szerepe van. Štrucl által készített összehasonlító tanulmány [25] az Észak-atlanti Szerződés Szervezete (North Atlantic Treaty Organisation – NATO), az Európai Unió, valamint több nemzet kiberbiztonsággal és a kibervédelemmel kapcsolatos megközelítéseit elemzi. A kutatáshoz a szerző egy átfogó, a biztonsági aspektusokat felölelő architektúrát (2. ábra) alkotott meg elemezve számos definíciót. A tanulmányban a szerző megállapítja az eltérő terminológia alkalmazását és az abból fakadó lehetséges problémákat, amelyek a biztonsági fenyegetésekre adott hatékony közös válaszadás kapcsán merülhetnek fel. (Tulajdonképp Ekelhart [26]

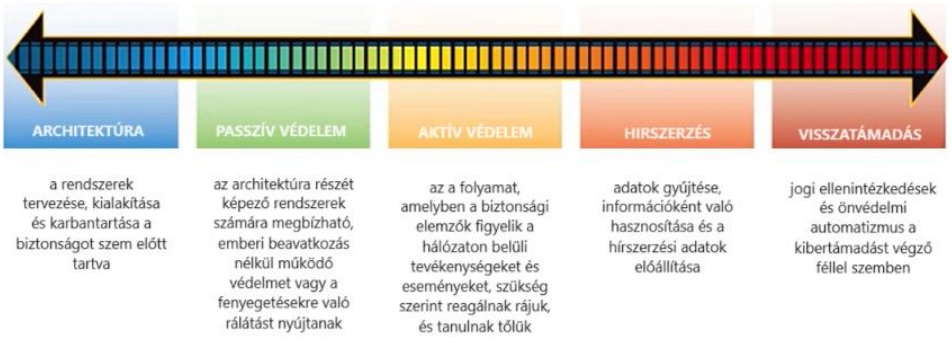
2006-ban tett megállapítása a terminológiai pontatlanságok és eltérések, valamint az okozott problémák kapcsán manapság is érvénnyel bír.) Azonban Solms és Niekerk [27] elemzése alapján a kiberbiztonságnak létezik az információbiztonsággal és az IKT biztonságával összefüggésben nem álló vonatkozása is. Ez az összefüggés abban az esetben áll elő, amikor a kiberfenyegetettséget jelentő fél nem adatot vagy infrastruktúrát, hanem közvetlenül a kiberszemélyiséget támadja, mint például a kibertérben végrehajtott fenyegetés, zsarolás, bántalmazás, hamis információ terjesztése.



2. ábra. Az információs és rendszerbiztonság általános vállalati biztonsági architektúrája
Forrás: Saját szerkesztés [25, p. 7] alapján. A definíciókhoz a következő további forrásokat felhasználva: Információvédelem [28], Információbiztonság [29], Kiberbiztonság [10], Kibervédelem [10], Kiberreziliencia [30], Üzletmenetfolytonosság [31], IKT biztonság [22]

Ryba okfejtése [19] párhuzamba állítható Muha és Krasznay [22] által tett megállapítással, miszerint a kritikus infrastruktúrák egyre növekvő mértékben függenek az IKT szolgáltatásoktól. „*Mindez azt jelenti, hogy a kritikus infrastruktúráink a szolgáltatás jellegétől függően sorolhatóak különböző ágazatokba, de szinte valamennyiük közös metszete a kibertérrel való kapcsolódás és az általa hordozott kockázatok, amelyek az elektronikus információs rendszereiken keresztül fejtik ki hatásukat*" [32, p. 76].

„A kiberbiztonság csúszó skálája" modell („Sliding Scale of Cyber Security" model) (3. ábra) keretként szolgál annak megértésére, hogy egy szervezet vagy vállalat kiberbiztonsági képessége milyen összetevőkre épül, melyek: (1) az architektúra, (2) a passzív védelem, (3) az aktív védelem, (4) a felderítés és (5) a visszatámadás képességek. A modell megadja az egyes képességek egymáshoz való viszonyulását, hogyan járulhatnak hozzá a szóban forgó IKT rendszerek és szolgáltatások biztonságának szavatolásához [33].



3. ábra. „A kiberbiztonság csúszó skálája" („Sliding Scale of Cyber Security") modell
Forrás: Saját szerkesztés [33, p. 4] alapján

Az ISACA információbiztonság üzleti modellje (Business Model for Information Security – BMIS) pediglen megadja, hogy e képességek milyen tényezők függvénye [34]. A modell szerint egy szervezet biztonsága a Szervezeti jellemzők, az Emberek, a Folyamat és a Technológia, mint statikus tényezők függvénye (melyeket a hat dinamikus tényező kapcsol össze, úgymint Kultúra, az Irányítás, az Architektúra, a Képesség és támogatás, az Emergencia, valamint az Emberi tényező). A Szervezeti jellemzők az adott szervezet felépítéséből és működéséből fakadó tényezőket írják le. A mindenkori szervezet emberek, eszközök és folyamatok hálózata, amelyek meghatározott szerepkörben kölcsönhatásba lépnek egymással a kialakított stratégia alapján egy vagy több közös cél elérése érdekében, miközben alkalmazkodnak a külső és belső tényezőkhöz. Az Emberek tényező az emberi erőforrásokat és az őket körülvevő biztonsági körülményeket taglalja, meghatározva belső és külső emberi erőforrások stratégia szerinti működését. A Folyamat formális és informális jelleggel meghatározott feladatokat, feladatcsoportokat foglalja magában, amelyek létfontosságú kapcsolatot biztosítanak az összes többi tényezővel. A Technológia tényező az összes olyan eszközből, alkalmazásból és infrastruktúrából áll, amelyek a folyamatok végrehajtását hatékonyabbá teszik. A BMIS felhívja a figyelmet a belső és külső szolgáltatók által biztosított erőforrások alkalmazásának lehetőségeire, amely egyaránt érintheti a Technológiai tényezőt (pl. IT szolgáltatás), az Emberi tényezőt (pl. szakértelem) és a Folyamat tényezőt (pl. incidenskezelés folyamat), valamint megjelöli a belső és külső erőforrások közötti különbségeket.

Figyelembe véve a BMIS által definiált függőségeket, egy szervezet a biztonsági szintjét és ezáltal a más gazdasági és társadalmi szereplők felé mutatott megbízhatóságát a statikus tényezők (és dinamikus kapcsolatok) jellemzői alapján növelheti. A szervezet működésének egészére kiható, így valamilyen formában az összes tényezőre vonatkozó biztonsági elvárásokat tartalmazó követelményeket fogalmaz meg például az ISO/IEC 27001 [35] szabvány és a vonatkozó ISO/IEC 27002 [36] kontrollgyűjtemény, a NIST Cybersecurity Framework [37], a NIST SP 800-53 [38] kontrollgyűjtemény.

Mindazonáltal a szabványokon, keretrendszereken és kontrollgyűjteményeken túlmenően is adott a lehetőség a tényezők megbízhatóságának növelésére. Egy folyamatot a végrehajtása által elért eredményeken keresztül (eredményesség), valamint folyamatlépések hatékonysági jellemzőit leíró mérőszámokkal lehetséges a minőséget mérni [39]. A Technológiai tényező esetében a Zero trust (Zéró bizalom) koncepció [40] alkalmazása az IKT infrastruktúra biztonsági szintjét növelheti, ahogy egy IKT termék, mint az Értékelés tárgya (Target Of Evaluation – TOE) a biztonsági funkcionalitás ISO/IEC 15408 [41] szabvány – amely újonnan elfogadott uniós változata az európai kiberbiztonsági tanúsítási rendszer (European Common Criteria – EUCC) [42] – szerinti meghatározása, értékelése és szavatolása, vagy épp a OWASP ASVS (Open Web Application Security Project Application Security Verification Standard) kontrollgyűjtemény [43] elvárásának alkalmazása útján.

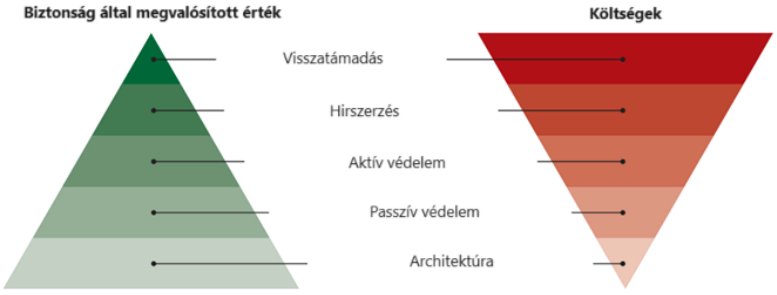
Az Emberi tényező az emberi viselkedés kiszámíthatatlansága, a működését meghatározó bonyolult összefüggések, valamint a (kiber)biztonsági teljesítményére vonatkozó mérési nehézségek következtében a legösszetettebb és a legnehezebb módon kezelhető kérdéskör a BMIS statikus tényezők közül. Az Amerikai Pszichológiai Társaság (American Psychological Association – APA) szótára szerint a tudatosság (awareness) valaminek az észlelése vagy ismerete [44], amelyhez képest az „ISACA Magyar szakkifejezés-gyűjtemény" részletesebb meghatározást alkalmaz. Az alapján a tudatosság „[m]*egismerni, figyelembe venni, tudatában lenni és jól tájékozottnak lenni egy meghatározott témáról, amely magában foglalja a téma ismeretét és megértését, valamint az ennek megfelelő cselekvést*" [45, p. 233]. A tudatos hozzáállás, a tudatos cselekvés alapvetően valaminek a tudásának és az emberi attitűd együttese, amelyre vonatkozóan a tanulási és szocializációs folyamat során az emberi agy tapasztalatokon alapuló koncepciókat és elméleti perspektívákat hoz létre, ezzel adott esetben szűkítve az észlelést. Tversky és Kahneman kutatása szerint a párhuzamos döntések gyakorlati problémáinak összetettsége gátolja az embereket a helyes döntéshozatalban, ráadásul az emberek hajlamosak felerősíteni a negatív hatások jelentőségét, miközben csökkentik a pozitív hatásokat fontosságát [46]. Továbbá pszichológiai nyomás alatt az emberek általában nem figyelnek a valószínűségekre, az agyi működés korlátjai miatt ún. automatikus viselkedés lép életbe, mely a gyors és lassú gondolkodásból eredően különböző heurisztikákat alkalmaz [47]. A limitált kognitív képességek következtében az emberek az információ feldolgozásában és felidézésében a saját véleményüket alátámasztó információkat keresik [48], adott esetben a tömeghatás által vezérelve [49]. Mindezek értelmében a tudásra, az attitűdre és a heurisztikák legyőzésére is hatni kell a (kiber)biztonsági tudatossági programmal [50], amelyet értelemszerűen a Technológia és Folyamat tényezőkkel összehangoltan szükséges megtenni [51].

A tudományos probléma megfogalmazás

Az IKT rendszerektől való általános jellegű függőség következtében egy nemzet működése, az állampolgárainak jóléte a nyújtott szolgáltatások, a kritikus és kritikusnak nem minősített, de gazdasági szempontból jelentős infrastruktúrák működésének folytonosságának, a kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának függvénye. A kibertérben számos érintett fél miatt a védelmi képességek hatékonyságának megtartása vagy épp növelése, úgymint a fenyegetettségekkel szembeni ellenállóképesség, a kiberreziliencia vagy a visszatámadás (a védekezés érdekében tett támadás) képessége az érintett felek közötti bizalom kiépítését is igényli [BZs1].

A BMIS tényezőkre vonatkozó biztonsági kontrollok kiválasztásakor gondoskodni kell arról, hogy a befektetési és fenntartási költségek arányosak legyenek a fenyegetések által okozható károk értékével. A kockázatokkal arányos védelem indukálja az összes lehetséges fenyegetés figyelembevételét (zárt védelem), a védelmi képesség a rendszer valamennyi elemére történő kiterjedését (teljes körű védelem), valamint a dinamikusan változó körülményekhez való alkalmazkodást (folytonos védelem) [52].

A preventív és reaktív képességekből többféle alternatíva, változatos biztonsági szint elérése mellett valósítható meg, azaz többféle kontroll-mix választható. „A kiberbiztonság csúszó skálája” modell esetében a biztonsági szint növeléséhez leginkább a megfelelő architektúra, majd a passzív védelem, az aktív védelem, a hírszerzés és végül legkisebb mértékben a visszatámadás járul hozzá, azaz képez értéket (***4***. ábra). Ezzel szemben a kategóriák megvalósításához szükséges befektetési és operatív költségek ebben a sorrendben növekednek [33]. Értelemszerűen azok a képességek és olyan összetételben fejlesztendők, amelyek a leginkább támogatják az adott szervezet működését.



4. ábra. Hozzáadott érték (balra) és a kapcsolódó költségek nagysága (jobbra)
Forrás: Saját szerkesztés [33, p. 6] alapján

Ennek következtében a lehetséges biztonsági kontrollok közül azokat a preventív, detektív és kompenzáló kontrollokat tartalmazó kontroll-mixet kell megvalósítani a lehetséges kontrollok halmazából, amelyek nem veszélyeztetik az operatív működést és gazdasági szempontból is az

optimumot valósítják meg (vagy legalábbis közelítik azt), másfelől megakadályozzák a szervezet által nem felvállalható jellegű biztonsági incidensek bekövetkezését. Egy kiberincidens „[m]*inden olyan eseményt magában foglal, amely hatással van a kibertér bármely összetevőjére vagy működésére, függetlenül attól, hogy a kibertérben keletkezett vagy a kibertéren kívül okozták, természeti jellegű vagy ember által okozott, rosszindulatú vagy nem rosszindulatú szándék által vezérelt, szándékos, véletlen vagy alkalmatlanság miatt következik be, valamint rendszerfejlesztés vagy rendszerműködéssel kapcsolatban lép fel*" [10, p. 6].

Azonban a nem optimális kontroll-mix kiválasztása és alkalmazása negatív hatással (lehet) az adott szervezetre. A kontrollok tervezési, működési hiányosságainak vagy teljes hiányának folytán bekövetkezett biztonsági incidensek veszélyeztetik az operatív működést és a szervezet működésben érintett feleket, továbbá az IKT függőség, a fizikai tér és a kibertér egymásra hatásának nyomán különböző mértékű gazdasági, társadalmi és környezeti károkat eredményezhetnek [53, p. 345].

A hatások jellegére és mértékére kiváló példát nyújt az Észtországot ért kibertámadási kampány felidézése. Az ismeretlen támadók az adott korra jellemző átlagot meghaladó észt digitalizáció következtében mind minőségében és mennyiségében megnövekedett támadási vektort használták ki 2007 április 27. és 2007 május 18. között az egész nemzetre hatással lévő kibertámadási kampány során [BZs2, p. 138]. Az összetett és hosszabb ideig kitartó kibertámadásban mindössze néhány kritikus online szolgáltatás, illetve a nem jelentős (nem kritikus) szolgáltatások (pl. kormányzati weboldalak és a híroldalak) kiesése nem okozott jelentősebb, maradandó kárt [54]. Például az egyik érintett bank „mindössze" egymillió dollár értékű kárról számolt be [55, p. 56]. Sajnálatosan a kibertámadási kampányra vonatkozó valós idejű és ex post pénzügyi elemzések hiányosan valósultak meg, minthogy azok nem tértek ki a válaszintézkedések költségeire, a meglévő rendszerek bővítésének vagy új eszköz vételezési költségeire, a túlóra díjakra és az elmaradt vagy eltolt beruházások hatására. A közvetett hatások tekintetében az észt Pénzügyminisztérium számítása szerint a tranzitszektort érintő orosz megrendelések elmaradásai az észt GDP 1-3,5 százalékos csökkenését okozta. Ugyanis Észtország tranzitszektorának jövedelme 2007-ben 40 százalékkal csökkent az előző évhez képest, mert Oroszország – a jégmentes balti kikötőktől való függése miatt – az észt fél vádjainak megfogalmazását következtében Tallinn kikötője helyett lettországi és litván kikötőket vett igénybe [54]. 2007. július 2-án az S&P a 2006. július 17-i „A stabil" minősítésről „A negatív" besorolásra módosította Észtország megítélését [56], azonban a nyilatkozatok alapján ez nem kapcsolható össze a kibertámadási kampánnyal [57].

Ugyanakkor az észt kormány az általa készített SWOT analízist felhasználva még 2007-ben elkészítette az észt nemzeti stratégiát [58], valamint 2008-ban az észt nemzeti kiberbiztonsági stratégiát [59]. Észtország a kiberstratégiájában a stratégiai célok elérése érdekében a nemzeti és

vállalati szinten is határozott meg megvalósítandó feladatokat. A nemzeti szinten értelmezett feladatok a kiberbiztonság, a kibervédelem és a bűnüldözés területére vonatkozó hatás elérését célozták a hírszerzés és offenzív jellegű kiberképességek fejlesztése érdekében, valamint vállalati szinten értelmezett feladatok a kiberbiztonság, a kibervédelem és a kiberrezilienca szintjének emelése érdekében kerültek meghatározásra [BZs3, p. 257].

A kampány során mind az Európai Unió, mind a NATO elkezdte felkutatni a lehetséges új módszereket a kiberbiztonság szintjének fokozására, és a megfelelő lehetséges válaszlépéseket és szankciókat megtalálni a digitális hadviselésben részt vevő államok számára. A NATO 2008 áprilisban megalapította a Kooperatív Kibervédelmi Kiválósági Központot (Cooperative Cyber Defence Centre of Excellence – CCDCoE) Tallinnban, Észtország fővárosában, amely összefüggésben állt Észtország kiberbiztonsági kompetencia növelését célzó törekvéseivel. Továbbá felmerült a Washingtoni Szerződés 5. cikkének – miszerint az egyik vagy több tagállam ellen intézett fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek – kiterjesztése a kibertérre [60, pp. 54–55], azaz annak lehetősége, hogy a NATO a kiberteret is műveleti térnek tekinti. A 2016. júliusi *"varsói csúcstalálkozón a szövetséges állam- és kormányfők ismét megerősítették a NATO védekező megbízatását és a már elismert kiberteret a műveletek egyik területeként* […]" [61, p. 8], így a kibertér lett az ötödik műveleti tér.

Az Észtországot ért kibertámadási kampány kiválóan szemlélteti az incidensek hatásainak és következményeinek jellegét és volumenét, így bár kiberbiztonsági kockázatok és incidensek kutatása nem új vagy újszerű terület, kutatásuk és a vonatkozó eredmények visszacsatolása a kockázatelemzés folyamatába és az alkalmazott metodológiába a dinamikusan változó belső működés és a külső környezet következtében szükségszerű.

Célkitűzések

A kutatásommal a teljes körű, zárt, valamint a kockázatokkal arányos védelemre vonatkozó elvárásokra fókuszálok az Európai Unió tekintetében. Kutatásom alapvető céljaként az általános érvényű, széles körben alkalmazható megoldások azonosítását és elemzését célzom meg, kiemelt figyelmet fordítva a jogszabályi követelményeknek, a humán eredetű fenyegető tényezőknek, valamint az általuk okozott incidenseknek, melyek a jövőbeni jogszabályok megszövegezésében és kockázatelemzési módszertanok kialakításában is bemenetet jelenthet. Ennek érdekében a kutatás célkitűzéseit az alábbiak szerint definiálom:

KC1 Áttekinteni és elemezni a vonatkozó aktuális uniós jogszabályokat, amelyek befolyásolják a szupranacionális és nemzeti védelmi képességeket, valamint determinálják az érdekelt

feleket és azok kötelezettségeit. Az érdekelt feleket a tagállami nonprofit szervezetek és profitorientált vállalkozások tekintetében vizsgálom.

KC2 Azonosítani és elemezni a fenyegetettségelemzést jellemző modern módszert vagy módszereket, kiváltképp a humán eredetű fenyegető tényezők vonatkozásában, és a vonatkozó információk megosztásának lehetőségeit.

KC3 Meghatározni a felmerülő kiberbiztonság incidensek gazdasági összefüggéseit.

A téma kutatásának hipotézisei

A kutatásomra vonatkozóan az Európai Unió tekintetében a jogszabályi, a fenyegetettségek és a pénzügyi-gazdasági jellegű összefüggéseket vizsgálom a kiberbiztonsággal összefüggésben. A kutatást alapjaiban meghatározó hipotéziseket e három témakör kapcsán határozom meg:

H1: Léteznek olyan szervezetek, illetve profitorientált vállalkozások, amelyek bár jelentős társadalmi vagy gazdasági funkciót töltenek be, nem vonatkoznak rájuk az uniós jogszabályokban előírt kiberbiztonsági elvárások.

H2: A kiberbiztonsági incidensek menedzselésére vonatkozóan az Európai Unió jogszabályai egymással átfedésben határozzák meg a szabályokat, beleértve a hatóságok tájékoztatását is. A kiberfenyegetettségre vonatkozó információk megosztását szolgáló célrendszerek az incidensek hatósági bejelentési kötelezettség támogatására is alkalmasak.

H3: Annak meghatározása, hogy egy szervezetre egy kiberbiztonsági incidens milyen gazdasági hatással van, többféle szempont alapján is lehetséges. A hatályos jogszabályok helytelenül határozzák meg a kiberbiztonsági incidensek pénzügyi jellegű üzleti hatások vizsgálatára vonatkozó elvárásokat, amelyet a kockázatok elemzésekor figyelembe kell venni.

Kutatási módszerek

A jogszabályi, a kiberbiztonsági és a gazdasági összefüggések következtében a téma összetettsége interdiszciplináris megközelítést kíván, ennek megfelelően a kutatási módszerek területén elengedhetetlen a komplex megközelítés a kutatási témám vizsgálatakor. Felhasználva az indukció és dedukció, valamint az analízis és a szintézis módszereit, a kutatásom során a következő módszereket alkalmazom:

KM1: A szakirodalom alapján, valamint az EURLEX, mint az uniós joganyagokhoz hivatalos online hozzáférést biztosító szolgáltatást felhasználva áttekintem és elemzem a 2007-ben bekövetkezett, Észtországot ért kibertámadási kampány óta eszközölt uniós jogszabályi és szakpolitikai fejlődést a kiberbiztonság tekintetében. Az aktuális és a tervezett jogszabályokat alapul véve elemzem a jogalkotói szándék eredményeként előálló kiberbiztonsági képességeket, a jogalanyok körét és kötelezettségeiket. A magyarországi vonatkozású összefüggéseket a Nemzeti Jogszabálytár adatbázisa alapján vizsgálom.

KM2: Szakirodalmi összefüggéseket felhasználva azonosítom és rendszerezem a szervezeti szintű kiberbiztonsági, kiváltképp a humán eredetű fenyegető tényezők támadói képességeit az információbiztonság üzleti modell modellje (BMIS) szerinti struktúra alapján. Az iparági megoldások és szabványok alapján vizsgálom a humán eredetű fenyegető tényezők tevékenységeiről szóló információk megosztásának módszereit.

KM3: A szakirodalmat felhasználva meghatározom a kiberbiztonsági incidensek pénzügyi-elemzési lehetőségeit és a kapcsolódó módszertani elemeket. Szekunder és szükség szerint primer kutatást hajtok végre konkrét eseteket (incidenseket) elemezve, amely során alkalmazom a megalkotott elemzési módszertant, vizsgálva annak megfelelőségét. Az esetek kiválasztása során nem szorítkozom kritikus infrastruktúrákat érintő, illetve az Európai Unió területén vagy kizárólag uniós állampolgárokat érintő incidensekre, tekintettel a vizsgálandó témakör általános érvényű vonatkozására.

1 A KIBERBIZTONSÁG MEGKÖZELÍTÉSE AZ EURÓPAI UNIÓBAN

A fejezet részeként célom áttekinteni és elemezni az Európai Unió kritikus infrastruktúra védelmének, valamint a kiberbiztonságra vonatkozó megközelítésének és szabályozásának, az Észtországot ért 2007-es kibertámadási kampány óta bekövetkezett fejlődését, annak eredményeképp előálló aktuális kiberbiztonsági közösségi jogszabályokat, amelyek befolyásolják a szupranacionális és tagállami védelmi képességeket. Ezeket az összefüggéseket felhasználva további célom azonosítani az Európai Unió kiberbiztonsági képességét meghatározó érdekelt feleket, valamint a jogszabályban meghatározott kiberbiztonsági kontrollakra vonatkozó elvárásokat.

1.1 Történeti áttekintés (2008-)

A 2003-ban elfogadott európai biztonsági stratégia 2008-ban történő felülvizsgálat eredményeképp a jelentés megállapította, hogy „[a] *modern gazdaságok nagymértékben függnek a létfontosságú infrastruktúrától, ideértve a közlekedési, kommunikációs és energiaellátási infrastruktúrát, de az internetet is*" [62, p. 5]. Mindez összefüggésben áll a 2007-ben Észtországot ért kibertámadási kampánnyal, valamint a 2008-ban bekövetkezett orosz-grúz háborúban Oroszország által alkalmazott hibrid hadviseléssel, amelyben az IKT számára is meghatározó szerep jutott [63]. A jelentés ennélfogva helyesen állapította meg, hogy a támadási vektor „[…] *új dimenzióként jelenik meg, mint esetleges új gazdasági, politikai és katonai fegyver"* [62, p. 13]. A témával összefüggésben a jelentésben megfogalmazott konklúzió szerint „[e] *területen több munkára van szükség egy átfogó uniós megközelítés lehetőségének felderítése, figyelemfelkeltés és a nemzetközi együttműködés fokozása céljából*" [62, p. 5]. Még ebben az évben megvalósult az ENISA megbízatásának három évvel történő kibővítése [64]. (Az ENISA ekkor még az Európai Uniós Hálózat- és Információbiztonsági Ügynökség, azaz European Network and Information Security Agency megnevezéssel bírt.)

2009 márciusban a kritikus informatikai infrastruktúrák védelmére vonatkozóan az Európai Közösségek Bizottsága „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása" mottóval cselekvési tervet adott ki, amelyben a CIP és a kiberbiztonság összefonódását, – hivatkozva többek közt az Észtországot célzó kibertámadási kampányra, – az ebből származó problémákat, illetve megoldási lehetőségeket taglalta [65]. Az Európai Bizottság 2010 márciusában bemutatta az „Európa 2020" stratégiát, kijelölve hét kiemelt kezdeményezést, amelyek közül az egyik az IKT alkalmazásának kulcsfontosságú szerepet szán a kitűzött célok sikeres megvalósításában [66]. Ezt a területet „Az európai digitális menetrend" [67] tárgyalta, amely az általa megnevezett „számítógépes bűnözés terjedése és a hálózatokkal szembeni bizalomvesztés kockázata" csökkentése végett számos intézkedést vázolt fel az elkövetkező időszakra, melyek jelentős része összefüggésbe hozható a 2008-as észt kiberbiztonsági stratégia [59] megállapításaival.

A következő év májusában a Bizottság alelnökeinek kezdeményezésére az uniós intézmények és szervek főtitkárai úgy határoztak, hogy létrehozzák az uniós intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportjának (Computer Emergency Response Team for the EU institutions – CERT-EU) előzetes szervezési csoportját, amelynek felügyeletét egy intézményközi irányítóbizottság látja el, míg 2012 júliusában a főtitkárok megállapodtak a gyakorlati megvalósítás mikéntjéről és arról, hogy a CERT-EU állandó szervként működik tovább [68]. Még 2011 júliusban az ENISA megbízatása újabb másfél évvel meghosszabbításra került [69], amelyet 2013-ban egy új szabályozás váltott [70], kibővítve az ügynökség feladatköröket (pl. „támogatja az uniós politika és jog fejlesztését"), ugyanakkor azok támogató és segítségnyújtó jellegén nem változtatott.

2013-ban az Európai Unió elfogadta az első kiberbiztonsági stratégiát "Nyílt, megbízható és biztonságos kibertér" címmel [71]. A stratégia öt fő célkitűzést határozott meg: (1) kibertámadásokkal szembeni ellenállóképesség elérése, (2) a számítástechnikai bűnözés drasztikus csökkentése, (3) kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (KBVP) tekintetében, (4) kiberbiztonsági ipari és technológiai erőforrások kifejlesztése, és (5) összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára, és az Unió alapértékeinek támogatása. A kiberstratégiával az Európai Unió a többszereplős, többrétegű megközelítést alkalmazta, azaz Unió, tagállami, vállalati szinten a magán- és közszféra együttműködésére építve célozta a biztonsági szint fejlesztését. Ezzel összefüggésben megállapította, hogy az Európai köz- és magánszféra együttműködés az ellenállóképességért (European Public-Private Partnership for Resilience – EP3R) egy hatékony platformmá formálódott, amelyet tovább kell fejleszteni. (Az EP3R a telekommunikációs szektor szereplőinek részvételével 2009 és 2013 között működött [72].) Továbbá a stratégia az Európai Külügyi Szolgálat (European External Action Service – EEAS), az Európai Védelmi Ügynökség (European Defence Agency – EDA) és az Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége (European Union Agency for Criminal Justice Cooperation – Eurojust) szervekkel is megteremtette a kapcsolatot.

Még ugyanebben az évben az Európai Rendőrségi Hivatal (European Police Office – Europol), az Európai Unió bűnüldöző ügynökségének szervezetén belül létrejött a Számítástechnikai Bűnözés Elleni Európai Központ (European Cybercrime Centre – EC3) [73] az Európai Bizottság egy évvel korábbi, „Az európai digitális menetrend" bizottsági javaslatnak [74] megfelelően.

A kiberstratégia eredményeképp 2014-ben az Uniós kibervédelmi szakpolitikai keretet a Tanács 2014. november 18-án fogadta el. A keret a stratégia kapcsán határozza meg a különféle európai érdekelt felek szerepét, valamint meghatározza a KBVP kibervédelem öt prioritási területét [75]: (1) A tagállami kibervédelmi képességek fejlesztésének támogatása, (2) Kommunikációs hálózatok védelmének növelése, (3) A polgári-katonai együttműködés előmozdítása az EU kiberpolitikájával, az EU

intézményeivel, ügynökségeivel és a magánszektorral, (4) A képzési, oktatási és gyakorlati lehetőségek javítása és (5) Együttműködés az érintett nemzetközi partnerekkel, például a NATO-val. Összességében a keretrendszer több, mint negyven javaslatot terjesztett elő.

2015-ben az uniós biztonsági stratégia megállapítása szerint „[…] *a számítástechnikai bűnözés egyre növekvő mértékű fenyegetést jelent a polgárok alapvető jogaira és a gazdaságra, valamint a sikeres digitális egységes piac kiépítésére nézve* […]" [76, p. 14], veszélyeztetve a kritikus infrastruktúrák működését vagy éppenséggel felhasználva a IKT eszközöket és szolgáltatásokat illegális internetes kábítószer- vagy fegyverkereskedelem, pénzmosás vagy a gyermekek szexuális kizsákmányolásának céljából. A stratégia e problémákra vonatkozóan határozta meg a fejlesztési irányokat, melyeket 2016-ban az Európai Unió közös kül- és biztonságpolitika (KKBP) tekintetében erősített tovább, „[…] *a fenyegetések csökkentését célzó technológiai képességek, valamint a kritikus infrastruktúra, a hálózatok és a szolgáltatások sokktűrő képességének megerősítését és a kiberbűnözés visszaszorítását* […]" [77, p. 19] szorgalmazva. Mindez azt eredményezte, hogy a felmerülő kérdéseket minden szakpolitikai területen figyelembe kellett venni, megerősítve a KKBP-missziók és műveletek kibertérrel kapcsolatos elemeit. Ennek megfelelően a továbbiakban az Európai Unió elősegíti a kibertérrel kapcsolatos politikai, operatív és technikai együttműködést a tagállamok között, különösen az elemzés és a következménykezelés terén, továbbá javítja a kibertérrel kapcsolatos együttműködést a fő partnerekkel (pl. USA, NATO).

Már a kiberstratégia hatálybalépését megelőzően megkezdődött egy új, komplexebb szabályozási környezet előkészítése, amely eredményeképp a NIS irányelv [78] 2016-ban lépett hatályba két évet biztosítva a tagállami implementálásra, kötelezve a tagállamokat (1) Illetékes hatóságok kijelölésére; (2) CSIRT-ek felállítására; valamint (3) A meglévő nemzeti kiberbiztonsági stratégia felülvizsgálatára vagy új stratégia elfogadására. A meglévő tagállami kiberstratégia felülvizsgálata mellett, több változással egyetemben a NIS irányelv a 2008/114/EK irányelvben meghatározott szűk elemszámú kritikus infrastruktúra kiegészítéseként alapvető szolgáltatásokat határozott meg. Az irányelv kötelezi az alapvető szolgáltatásokat nyújtó szereplőket és digitális szolgáltatókat arra, hogy megfelelő biztonsági intézkedéseket hozzanak, és tájékoztassák az érintett nemzeti hatóságokat a súlyos eseményekről, továbbá létrehozta a NIS együttműködési csoportot (NIS Cooperation Group). A bevezetett intézkedések mind a stratégiai, mind pedig a műszaki szintű együttműködést erősítik meg az Európai Unióban.

Az Európai Bizottság 2017-ben felülvizsgálta az uniós kiberbiztonsági stratégiát [79]. „*A stratégia fő céljai és elvei – azaz a megbízható, biztonságos és nyitott kiber-ökoszisztéma elősegítése – továbbra is érvényesek. De a folyamatosan változó és súlyosbodó fenyegetettségi helyzet nagyobb aktivitást kíván ahhoz, hogy a jövőben ellen lehessen állni a támadásoknak, és el lehessen hárítani azokat*" [79,

p. 3]. A stratégia három pillért határozott meg: (1) Az Unió kibertámadásokkal szembeni ellenálló képességének kiépítése, (2) Hathatós uniós kibertámadás-elhárítás létrehozása, valamint (3) A kiberbiztonsági nemzetközi együttműködés erősítése. A kiberbiztonságra vonatkozó nemzetközi együttműködés erősítése terén továbbra is a korábban kitűzött célok kerültek megújításra, azonban a másik két pillér esetén a Bizottság új vagy újszerű lépéseket vázolt fel.

Az ellenálló képesség kiépítésének megvalósítása céljából a Bizottság az ENISA számára állandó megbízatást, az egységes kiberbiztonsági piac felé uniós kiberbiztonsági tanúsítási keretrendszer létrehozását, a hálózati és információs rendszerek biztonságáról szóló irányelv teljes körű végrehajtását, az ellenálló képesség javítását gyors vészhelyzeti reagálás útján, uniós kiberkészségbázis kiépítését, valamint a kiberhigiénia és -tudatosság elősegítését tűzte ki célul. A hathatós uniós kibertámadás-elhárítás létrehozásához a rossz szándékú szereplők azonosítása, a bűnüldözési reagálás fokozása, az állami és a magánszféra együttműködése a kiberbűnözés ellen, a politikai válaszlépések erősítése és a kiberbiztonsági támadáselhárítás kiépítése szerepelt a megvalósítandó feladatok között. A bűnüldözési reagálás fokozása céllal összefüggésben az Európai Unió Bűnüldözési Képzési Ügynöksége (The European Union Agency for Law Enforcement Training – CEPOL) széles körben oktatási tevékenységet végez a bűnüldözési szakemberek számára.

A politikai válaszlépések erősítése a fenyegetettség jellegének változás tükrében kiváltképp nagy jelentőséggel bírt, amellyel összefüggésben 2016 júliusban a korábbi észt miniszterelnök, Toomas Ilves azt hangoztatta, hogy a kibertérre vonatkozó elrettentés még mindig nagy problémát jelent [80], amely az Észtországot 2007-ben ért kibertámadási kampány óta eltelt évek tükrében egyre fokozódó hiányosságnak tekintendő.

Összefüggésben a tagállami védelmi kapacitások révén történő uniós kiberbiztonsági támadáselhárítás kiépítésével, a Bizottság elképzelése szerint, „*figyelemmel a kibervédelem és a kiberbiztonság határának elmosódására és a kibereszközök és -technológiák* [k]*ettős felhasználású jellegére, illetőleg a tagállami megközelítések nagyfokú változatosságára, az EU megfelelő helyzetben van ahhoz, hogy elősegítse a katonai és polgári erőfeszítések szinergiáját"* [79, p. 19]. Továbbá „[a] *fejlettebb kiberbiztonsági kapacitásokkal rendelkező és azok egyesítésére hajlandó tagállamok a főképviselő, a Bizottság és az Európai Védelmi Ügynökség támogatásával mérlegelhetnék a kiberbiztonság felvételét az „állandó strukturált együttműködés"* [Permanent Structured Cooperation] *(PESCO) keretébe*" [79, p. 19]. A 2017-től induló PESCO-projektek között 2019-ig bezárólag két kibervédelemmel kapcsolatos projekt szerepelt [81, p. 43].

2018-ban hivatalos alapra helyezték a CERT-EU működését egy, az uniós szervezetek közti megállapodás formájában [68]. Ugyanebben az évben valósult meg a kibervédelmi politikai keretrendszer frissítése, amellyel összefügésben a Tanács kiemelte, hogy „[a] *kibertér az ötödik*

műveleti terület a szárazföld, a tenger, a légtér és a világűr mellett: az uniós missziók és műveletek végrehajtásának sikere egyre nagyobb mértékben függ a biztonságos kibertérhez való zavartalan hozzáféréstől, ezért szilárd és ellenálló kiberműveleti képességeket igényel" [82, p. 2]. Ennek fényében mind az Európai Uniónak, mind az egyes tagállamoknak külön-külön „[…] *meg kell erősíteniük a kiberrezilienciájukat és megbízható kiberbiztonsági és -védelmi képességeket kell kialakítaniuk, hogy meg tudjanak felelni a változó biztonsági kihívásoknak*" [82, p. 2]. A szakpolitikai keret hat prioritási területet határozott meg: (1) A kibervédelmi képességek fejlesztése, (2) Az EU KBVP kommunikációs és információs hálózatainak védelme, (3) Képzések és gyakorlatok, (4) Kutatás és technológia, (5) Polgári-katonai együttműködés, és (6) Nemzetközi együttműködés.

2019 áprilisában a Kiberbiztonsági jogszabályként (Cybersecurity Act) hivatkozott Európai Parlament és a Tanács (EU) 2019/881 rendelet az ENISA számára állandó megbízatást adott, megváltoztatva az ügynökség nevét Európai Uniós Kiberbiztonsági Ügynökségre (European Union Agency for Cybersecurity), mely ugyanakkor továbbra is ENISA maradt, valamint kibővítve a tevékenységi körét [83]. Ennek értelmében az ENISA központi szerepet tölt be a tanúsítási rendszerek kialakításában és fenntartásában, valamint rendszeres uniós szintű kiberbiztonsági gyakorlatok, illetve kétévente egy-egy nagyarányú átfogó gyakorlat szervezésében.

Három évvel Toomas Ilves nyilatkozata után, 2019. májusban A Tanács (EU) 2019/796 rendelete megteremtette a célzott korlátozó intézkedések bevezetésének lehetőségét olyan kibertámadások esetén, amelyek külső fenyegetést jelentenek az EU vagy annak tagállamai számára [84]. 2020 júliusban a Tanács utazási tilalomból és pénzeszközök befagyasztásából álló korlátozó intézkedéseket foganatosított hat olyan személlyel és három olyan szervezettel szemben, akik, illetve amelyek különböző kibertámadásokért voltak felelősek vagy részt vettek azokban [85]. Ezáltal megvalósult az első uniós szankció kibertámadások elkövetőivel szemben.

2020. decemberben a Tanács következtetéseket fogadott el a csatlakoztatott eszközök kiberbiztonságáról, amelyben elismeri, hogy az internetre csatlakoztatott fogyasztási cikkek és ipari eszközök megnövekedett használatát és az ezzel kapcsolatban a magánéletet, valamint az információ- és kiberbiztonságot érintő új kockázatok jelentek meg. Emiatt szükséges a szabályozás felülvizsgálata, valamint az ENISA általi tanúsítási rendszer kibővítése [86].

Ugyanebben a hónapban megjelent „Az EU kiberbiztonsági stratégiája a digitális évtizedre" címmel [87], amely a korábbi stratégiák keretében elért eredményekre alapozva három területre vonatkozóan konkrét javaslatokat tartalmazott három fő eszköz (szabályozás, beruházás és szakpolitika) alkalmazására: (1) reziliencia, technológiai szuverenitás és vezető szerep, (2) operatív kapacitásépítés a megelőzés, elrettentés és reagálás érdekében, és (3) a globális és nyílt kibertér előmozdítása.

Az első pont értelmében a foganatosított kezdeményezések közé tartozik (a) az átdolgozott kiberbiztonsági irányelv elfogadása,·(b) a biztonságos IoT eszközökre vonatkozó szabályozási intézkedések, (c) a mesterséges intelligenciát használó biztonsági műveleti központok uniós hálózata és a kvantumtechnológiákon alapuló biztonságos kommunikációs infrastruktúra, (d) a kiberbiztonsági technológiák széles körű elfogadása a kis- és középvállalatoknak nyújtott támogatás révén a digitális innovációs központok keretében, (e) az uniós DNS címfeloldási szolgáltatás kifejlesztése, amely biztonságos és nyílt alternatívát kínál az uniós polgároknak, vállalkozásoknak és közigazgatásoknak az internet-hozzáférésre és végül (f) az 5G eszköztár végrehajtásának befejezése 2021 második negyedévére. Továbbá, összefüggésben a megerősített jelenlét a technológiai ellátási láncban stratégiai céllal, (g) az Unió tagállami, magán, illetve a létrehozásra az ekkor még javasolt státuszban lévő Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (European Cybersecurity Competence Centre – ECCC) és a koordinációs központok hálózat (Network of National Coordination Centres – NCCs) részvételével uniós beruházásokat javasolt. (Az ECCC 2021 májusában került jogszabályi alapon létrehozásra [88].) Tekintettel az emberi tényező biztonságra gyakorolt hatására, a kiberkészségekkel rendelkező uniós munkaerő kialakítása végett (h) „*a munkaerő készségeinek fejlesztésére, a legjobb kiberbiztonsági tehetségek kibontakozására, vonzására és megtartására, valamint a világszínvonalú kutatásba és innovációba való beruházásokra irányuló uniós erőfeszítések a kiberfenyegetésekkel szembeni általános védelem fontos részét képezik*" [87]. Végezetül (i) az európai kiberpajzs létrehozását az Unió a magánvállalkozás, állami szervezetek és nemzeti hatóságok által létrehozott CSIRT-ek és biztonsági műveleti központokra (security operation center – SOC) támaszkodva szándékozik megalapozni.

Az operatív kapacitásépítés a megelőzés, elrettentés és reagálás érdekében megvalósítandó feladatok – hasonlóképp az előző ponthoz – több réteget érintenek. Szabályozási feladatként jelentkezik (a) a kibervédelmi szakpolitikai keretet felülvizsgálata, (b) „A kibertérre mint műveleti területre vonatkozó katonai jövőkép és stratégia" kidolgozása, (c) a polgári, védelmi és űripar közötti szinergiák kialakítása és (d) a kritikus űrinfrastruktúrák kiberbiztonságának megerősítése. A preventív képességek fejlesztését segítve (e) ki kell alakítani az EU Hírszerző Központján (EU Intelligence and Situation Centre – EU INTCEN) belül a tagállamok kiberhírszerzési munkacsoportját, míg a reaktív képességek fejlesztése érdekében (f) létre kell hozni az európai kiberbiztonsági válságreagálási keretet, valamint (h) ki kell alakítani a kiberbűnözésre való reagálási képességeket (szolgálva a rosszindulatú kibertevékenységek visszaszorítását és a tevékenységtől való elrettentést).

A globális és nyílt kibertér előmozdítása keretében, tekintettel a nem megfelelő állami gyakorlatokból fakadóan a kiberteret érintő cenzúrázásra, tömeges megfigyelésre, adatvédelem megsértésére, az állampolgárok álhírekkel történő befolyásolására, illetve a polgári társadalom, a tudományos közösség

és az állampolgárok elnyomására, valamint a gyermekek szexuális zaklatására és kizsákmányolására, a kiberstratégia megvalósítandó feladata (a) a kibertérben való nemzetközi biztonság és stabilitás elősegítése, (b) gyakorlati útmutató kialakítása az emberi jogok és az alapvető szabadságok kibertérben való alkalmazásához, (c) hatékonyabb védelem biztosítása a gyermekek szexuális zaklatása és kizsákmányolása ellen és gyermekjogi stratégia kialakítása és előterjesztése. Ezzel összefüggésben (d) meg kell erősíteni és elő kell mozdítani a számítástechnikai bűnözésről szóló budapesti egyezmény megvalósítását. Folytatva a megkezdett nemzetközi együttműködést a kibertérre vonatkozó értékek és a jövőkép elérése érdekében, az Európai Unió feltett szándéka (e) a kiberdiplomáciai tevékenység növelése harmadik országokkal, valamint a regionális és nemzetközi szervezetekkel, továbbá (f) a több érdekelt felet tömörítő közösséggel való információcsere megerősítése. Valamint a szabványosításra való törekvések megerősítésre kerültek a (g) a nemzetközi szabványosítási célok meghatározása és elérésének elősegítése révén.

Végezetül a Bizottság, felismerve a kiberbiztonság az uniós intézményekben, szervekben és ügynökségeknél történő kezelésének nem egységes jellegét és esetleges hiányosságait, stratégiai kezdeményezésként jelölte meg (1) Az uniós intézmények, szervek és ügynökségek információbiztonságáról szóló rendeletet, (2) Az uniós intézményekre, szervekre és ügynökségekre vonatkozó közös kiberbiztonsági szabályokról szóló rendeletet; valamint (3) A CERT-EU új jogi alapra történő helyezését a megbízatása és a finanszírozása megerősítéséhez.

Annak ismeretében, hogy a NIS irányelv nem érte el a kitűzött célokat, a NIS 2 irányelv kidolgozása még 2020-ban kezdődött meg [89]. A tervezetre vonatkozóan az Európai Unió Tanácsa egy évvel később alakította ki az általános álláspontját [90]. Az irányelv a szövegtervezet szerint hivatalosan létrehozza az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (European cyber crisis liaison organisation network – EU-CyCLONe), támogatva a nagyszabású kiberbiztonsági események összehangolt kezelését. Továbbá kiterjeszti a szabályok hatályát nélkülözhetetlen és fontos szervezetek számára kötelező jelleggel, azaz míg a NIS irányelv értelmében a tagállamok feladata volt annak meghatározása, hogy mely szervezetek felelnek meg azoknak a kritériumoknak, amelyek alapján alapvető szolgáltatásokat nyújtó szereplőnek minősülnek, a NIS 2 irányelv ezzel összefüggésben bevezeti a méretkorlátra vonatkozó szabályt. Ennek értelmében általános szabályként az irányelv kiterjed a hatálya alá tartozó ágazatokban működő vagy a hatálya alá tartozó szolgáltatásokat nyújtó minden közepes és nagyméretű szervezetre. A NIS 2 irányelv [91] 2022 december 27-én került elfogadásra, a rendelkezéseit 2024. október 18-tól kezdődően kell alkalmazni, ennek megfelelően a NIS irányelv 2024. október 18-i hatállyal hatályát veszti.

1.2 A kiberképességek fejlődése és összehangolása az ágazati szabályokkal

Az Európai Bizottság 2015-ben az „Európai digitális egységes piaci stratégia” kinyilatkoztatásával elismerte, hogy az IKT már nem minősül külön ágazatnak, hanem a modern, innovatív gazdasági rendszerek alapját képezi [8], amelyet az IKT szolgáltatások penetrációjának növekedése, valamint a különböző ágazatok IKT infrastruktúrától és szolgáltatásoktól való függősége is alátámaszt. Ezt a megközelítést erősítve a Bizottság 2021 márciusában előterjesztette a „digitális iránytű” elnevezésű jogszabályi keretet [92], amelyben mindezen tényezők növelését prognosztizálja, illetve segíti elő, kijelölve az Unióban a IKT szolgáltatások elterjedésére vonatkozóan a jövőképet és célokat egészen 2030-ig, úgymint a digitális kompetencia- és infrastruktúra fejlesztést, vállalkozások digitális átalakulását, valamint az elektronikus közszolgáltatások fejlesztését.

Tulajdonképp e területek az elmúlt évtized során is egyértelműen a fejlődés tárgyát képzeték az IKT és a kibertér töretlen penetrációjából kifolyólag – összefüggésben a Bevezetésben tárgyaltakkal. Ehhez kapcsolódóan a digitalizáció, az IKT szolgáltatások és a kibertér kapcsán felmerülő biztonsági kérdések és összefüggések kezelése is folyamatos fejlődésen ment keresztül, amelyet a kihirdetett három kiberbiztonsági stratégia – mint a politikai szándék manifesztációja –, alapozva az Észtországot ért kibertámadási kampány összefüggéseire [BZs2], [BZs3], kiválóan szemléltet.

A felek közötti bizalom kiépítését célozva [BZs1], fontos szerep jutott az incidensek megelőzésének, elhárításának, illetve egyes ágazatokon belüli vagy különböző ágazatok közötti szereplők (kölcsönös) függőségeiből adódó tovaterjedés kezelésének. Ugyanis egy incidensből katasztrofális jellegű krízis esemény bontakozhat ki, hiszen a függőségek mentén két (vagy több) infrastruktúra állapota könnyűszerrel befolyásolhatja a másik állapotát vagy korrelálhat a másik állapotával. Konkrétan lépcsőzetes hiba esetén a (kritikus) infrastruktúra meghibásodása egy másik (kritikus) infrastruktúra meghibásodását okozza, eszkaláló hiba esetén egy (kritikus) infrastruktúra meghibásodása súlyosbítja egy másik (kritikus) infrastruktúra meglévő problémáját, illetve közös hiba esetén ugyanaz az esemény van negatív hatással két vagy több (kritikus) infrastruktúrára [BZs4].

A 2013-ban [71], 2017-ben [79] és 2020-ban [87] elfogadott uniós kiberbiztonsági stratégiai célok és a kapcsolódó feladatok vonatkozásában az uniós, nemzeti és vállalati szintek megkülönböztetése szükséges. Mindhárom stratégia egyaránt a nemzeti és vállalati szintű architektúra, passzív és aktív védelmi képességek kialakításának, valamint az uniós és tagállami szinten az aktív védelmi, hírszerzési és offenzív képességek elősegítését célozta a kiberbiztonság, a kibervédelem és a kiberreziliencia, kiberdiplomácia területét lefedve, valamint 2017-től kezdődően a kiberhigiénia is előtérbe került.

Az idő előrehaladtával a tagállami és vállalati szintet közvetlen módon érintő stratégiai célok mindinkább megjelentek, miközben a kritikus infrastruktúra védelmet célzó szándék is erősödött. (A

NIS irányelv, valamint a NIS 2 irányelv a tagállami és a vállalati képességek kialakítását és fejlesztését célozzák.) Ugyanakkor az uniós szintű entitásokra vonatkozóan a kiberképességek befolyásolása a legutóbbi, 2020-ban elfogadott kiberbiztonsági stratégiában jelent meg újonnan. Továbbá Backman elemzésére [93] alapozva az Unió a problémák azonosításában az idő múlásával egyre inkább fenyegetésalapú megközelítésre helyezte a hangsúlyt, értelemszerűen megtartva mellette a kockázatalapú szemléletet.

A NIS irányelv a 2008/114/EK irányelvvel [94] való kapcsolódást az 1. cikkben fogalmazottak szerint egyértelműen elutasítja, ugyanakkor a 2008/114/EK irányelvben meghatározott szűk elemszámú európai kritikus infrastruktúrák kiegészítéseként további alapvető szolgáltatást határoz meg, ahol a kibervédelemet erősíteni szükséges, és így „[…] *nem egyértelmű az elhatárolhatóság az alapvető szolgáltatások és a kritikus infrastruktúrák között*" [32, p. 76]. A NIS 2 irányelv, ledöntve ezt a korlátot, megteremti a kapcsolatot a kritikus fontosságú szervezetek rezilienciájáról szóló irányelvvel (resilience of critical entities – CER) [95], amely majdani hatálybalépésével a 2008/114/EK irányelv hatályát veszti. Továbbá a NIS 2 irányelv összehangolásra került az ágazatspecifikus jogszabályokkal, így mindenekelőtt a pénzügyi ágazat digitális működési rezilienciájáról szóló rendelettel (digital operational resilience for the financial sector – DORA) [96], valamint az elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról (electronic identification and trust services – eIDAS) szóló rendelet [97] utódjának tervezetével [98]. A NIS 2 irányelv definiálja a kapcsolatot az adatvédelemmel is, hivatkozva Az Európai Parlament és a Tanács (EU) 2016/679 rendeletét, azaz az Általános adatvédelmi rendeletet (General Data Protecion Regulation – GDPR). A rendelet a „*természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg*" [99], amely az IT/OT rendszerekben megvalósuló személyes adatok kezelésével vagy feldolgozásával szükségszerű volt [BZs5].

A DORA megteremti a kapcsolatot a hitelpénzintézeteket szabályozó az Európai Parlament és a Tanács 575/2013/EU rendelettel [100] és az Európai Parlament és a Tanács (EU) 2015/2366 irányelvvel (Second Payment Services Directive – PSD2) [101]. Ez utóbbi elsődleges célja a digitális pénzügyi szolgáltatások fejlődésének előmozdítása, amellyel összefüggésben támogatja új szolgáltatók (mint a számlainformációkat összesítő szolgáltató és a megbízásos online átutalási szolgáltató) belépését a pénzügyi piacokra.

Az 1. táblázat a tárgyalt uniós jogszabályok magyarországi implementációját megvalósító vagy az eltéréseket szabályozó jogszabályokat tartalmazza. Érdekesség, hogy sem a 2013. évi CCXXXVII. törvény [102], sem a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési

vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendelet [103] nem teremti meg a kapcsolatot a NIS, illetve újabban a NIS 2 irányelvvel.

1. táblázat. Uniós és vonatkozó magyarországi jogszabályok

Uniós jogszabály	Magyarországi jogszabály
Az Európai Parlament és a Tanács 575/2013/EU rendelete [100]	2013. évi CCXXXVII. törvény [102]
CER [95]	2012. évi CLXVI. törvény [104]
eIDAS [97]	2015. évi CCXXII. törvény [105] (2024.08.31-ig hatályos) 2023. évi CIII. törvény [106] (2024.09.01-től hatályos)
GDPR [99]	2011. évi CXII. törvény [107]
NIS irányelv [78]	2013. évi L. törvény (Ibtv.) [52]
NIS 2 irányelv [91]	2013. évi L. törvény (Ibtv.) [52] 2023. évi XXIII. törvény (Kibertan. tv.) [108]
PSD2 [101]	2013. évi CCXXXV. törvény [109]

Forrás: Saját szerkesztés

1.3 A szervezeti és vállalati szintű érdekelt felek

A NIS irányelvvel ellentétben a NIS 2 irányelv az alapvető szolgáltatást nyújtó szereplők (operator of essential services – OES) és a digitális szolgáltatók (digital service provider – DSP) megkülönböztetése helyett nélkülözhetetlen és fontos szervezetkategóriákat definiálja. Míg a NIS irányelv értelmében a tagállamok feladata volt annak meghatározása, hogy mely szervezetek felelnek meg azoknak a kritériumoknak, amelyek alapján alapvető szolgáltatásokat nyújtó szereplőnek minősülnek, a NIS 2 irányelv bevezet egy, a méretkorlátra vonatkozó szabályt, amely alapján általános szabályként az irányelvben foglaltak kiterjednek a hatályába tartozó ágazatokban működő vagy a hatálya alá tartozó szolgáltatásokat nyújtó minden közepes és nagyméretű szervezetre. A helyi jelentőségű közigazgatási szerveket a tagállamok az irányelv hatálya alá helyezhetik.

A NIS 2 irányelv további újítása az arányosság jegyében a gazdasági szempontból fontos szerep miatt a tagállamok kijelölhetnek további szereplőket az irányelv hatálya alá helyezve az adott szervezetet, amely a szervezetek és vállalatok bonyolult kapcsolati rendszere miatt [BZs6] üdvözlendő megközelítés. Ugyanakkor alapszabályként az irányelv mellőzi a mikró- és kisvállalatokat, valamint a védelem, a nemzetbiztonság, a közbiztonság, a bűnüldözés és az igazságszolgáltatás területén tevékenységet végző szerveket, valamint a tagállami parlamenteket és a központi bankokat. A 2. táblázat a NIS 2 irányelv által kiemelten kritikus és egyéb kritikus ágazatok alapvető és fontos kategorizálását tartalmazza, összevetve azokat a NIS irányelv alapvető és a CER irányelv kritikus megjelölésével.

2. táblázat. A NIS 2 irányelv ágazatainak és alágazatainak besorolása alapvető és fontos kategóriákba

<table>
<tr><th>Ágazat</th><th>Alágazat</th><th>NIS irányelv</th><th>CER</th><th>Nagyvállalat</th><th>Közép vállalat</th><th>Kis és mikró vállalat</th></tr>
<tr><td colspan="7">I. melléklet A KIEMELTEN KRITIKUS ÁGAZATOK</td></tr>
<tr><td>1. Energia</td><td>a) Villamos energia, b) Távfűtés és -hűtés, c) Olaj, d) Gáz, e) Hidrogén</td><td rowspan="9">OES</td><td rowspan="20">Kritikus</td><td rowspan="13">Alapvető</td><td rowspan="13">Fontos, hacsak a tagállam nem alapvetőnek azonosítja</td><td rowspan="13">Hatályon kívül, hacsak a nemzeti hatóság alapvető vagy fontos elemnek nem nyilvánítja (egyedüli szolgáltatás, jelentős hatás, elengedhetetlen a társadalom számára)</td></tr>
<tr><td rowspan="2">2. Szállítás</td><td>a) Légi, b) Vasúti, c) Vízi, d) Közúti</td></tr>
<tr><td>Speciális eset: Tömegközlekedés, amennyiben CER szerint azonosításra kerül</td></tr>
<tr><td>3. Banki szolgáltatások</td><td>Hitelintézetek</td></tr>
<tr><td>4. Pénzügyi piaci infrastruktúrák</td><td>Kereskedési helyszínek működtetői, Központi szerződő felek</td></tr>
<tr><td rowspan="2">5. Egészség-ügy</td><td>Egészségügyi szolgáltatók, Uniós referencialaboratóriumok, gyógyszerek kutatásával és fejlesztésével foglalkozó szervezetek, gyógyszeralapanyagokat és gyógyszerkészítményeket gyártó szervezetek, népegészségügyi szükséghelyzetben kritikus fontosságú orvostechnikai eszközöket gyártó szervezetek</td></tr>
<tr><td>Speciális eset: gyógyászati termékek forgalmazási engedéllyel rendelkező jogalanyok, amennyiben CER szerint azonosításra kerülnek</td></tr>
<tr><td>6. Ivóvíz</td><td>emberi fogyasztásra szánt víz szolgáltatói és elosztói, azokat az elosztókat kivéve, akik számára az emberi fogyasztásra szánt víz elosztása más áruk és termékek forgalmazásából álló általános tevékenységüknek nem alapvető része</td></tr>
<tr><td>7. Szennyvíz</td><td>települési szennyvíz, háztartási szennyvíz, vagy ipari szennyvíz összegyűjtését, ártalmatlanítását vagy kezelését végző vállalkozások, azokat a vállalkozásokat kivéve, amelyek általános tevékenységének nem alapvető része</td><td></td></tr>
<tr><td rowspan="9">8. Digitális infrastruktúra</td><td>Minősített bizalmi szolgáltatók</td><td rowspan="3"></td><td colspan="3" rowspan="3">Alapvető</td></tr>
<tr><td>DNS-szolgáltatók, a gyökérnév-szerverek üzemeltetőit kivéve</td><td rowspan="3">OES</td></tr>
<tr><td>Legfelső szintű doménnév-nyilvántartók</td></tr>
<tr><td>Nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók</td><td rowspan="3"></td><td colspan="2" rowspan="2">Alapvető</td><td rowspan="2">Fontos, hacsak a tagállam nem alapvetőnek azonosítja</td></tr>
<tr><td>Nem minősített bizalmi szolgáltatók</td></tr>
<tr><td>Internetes exchange pont szolgáltatók</td><td>OES</td><td rowspan="4">Alapvető</td><td rowspan="4">Fontos, hacsak a tagállam nem</td><td rowspan="4">Hatályon kívül, hacsak a nemzeti hatóság alapvető</td></tr>
<tr><td>Felhőszolgáltatók</td><td rowspan="3"></td></tr>
<tr><td>Adatközpont-szolgáltatók</td></tr>
</table>

	Tartalomszolgáltató hálózati szolgáltatók				alapvetőnek azonosítja	vagy fontos elemnek nem nyilvánítja
	Nyilvános elektronikus hírközlési hálózatok szolgáltatói					
9. IKT-szolg. irányítása	Irányított (biztonsági) szolgáltatók					
10. Közigaz-gatás	A tagállam által a nemzeti joggal összhangban meghatározott, a központi kormányzathoz tartozó közigazgatási szerve (kivéve nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés – többek között a bűncselekmények megelőzése, kivizsgálása, felderítése és büntetőeljárás alá vonása – területén végzik tevékenységeiket)			Alapvető		
	regionális szintű közigazgatási szerv, amely kockázatalapú értékelés alapján olyan szolgáltatásokat nyújt, amelyek zavara jelentős hatást gyakorolhat kritikus fontosságú társadalmi vagy gazdasági tevékenységekre			Fontos, hacsak a tagállam nem alapvetőnek azonosítja		
	opcionális: helyi szintű közigazgatási szervek			Hatályon kívül, hacsak a nemzeti hatóság fontos elemnek nem nyilvánítja		
11. Világűr	Földi infrastruktúra üzemeltetők, amelyek támogatják az űralapú szolgáltatások nyújtását, kivéve a nyilvános elektronikus hírközlő hálózatok szolgáltatóit			Alap vető	Fontos, hacsak a tagállam nem alapvetőnek azonosítja	Hatályon kívül, hacsak a nemzeti hatóság alapvető vagy fontos elemnek nem nyilvánítja
II. melléklet EGYÉB KRITIKUS ÁGAZATOK						
1. Postai és futárszolg.				Fontos, hacsak a tagállam nem alapvetőnek azonosítja		Hatályon kívül, hacsak a nemzeti hatóság alapvető vagy fontos elemnek nem nyilvánítja (egyedüli szolgáltatás, jelentős hatás, elengedhetetlen a társadalom számára)
2. Hulladék-gazdálkodás	hulladékgazdálkodással foglalkozó vállalkozások, kivéve azokat a vállalkozásokat, amelyeknek nem a hulladékgazdálkodás a fő gazdasági tevékenységük					
3. Vegyszerek	gyártása, előállítása és forgalmazása					
4. Élelmiszer	termelés, -feldolgozás és -forgalmazás		Kritikus			
5. Gyártás	a) Orvostechnikai eszközök és in vitro diagnosztikai orvostechnikai eszközök gyártása, b) Számítógépek, elektronikai és optikai termékek gyártása, c) Villamos berendezések gyártása, d) Máshova nem sorolt gépek és gépi berendezések gyártása, e) Gépjárművek, pótkocsik és félpótkocsik gyártása, f) Egyéb szállítóeszközök gyártása					
6. Digitális szolgáltatók	Online piacterek szolgáltatói, Online keresőmotorok szolgáltatói, A közösségimédia-szolgáltatási platform szolgáltatói	DSP				
7. Kutatás	Kutatóhelyek (kivéve oktatási intézmények)					

	opcionális: oktatási intézmények, különösen, ha kritikus fontosságú kutatási tevékenységeket végeznek				

Forrás: Saját szerkesztés [91], [110] alapján

A közigazgatási szereplők a fenti értelemben vett operatív szereplők közé történő felvételét a tagállamok akadályozták meg még 2013-ban, így a NIS irányelv hatálya az eredeti tervekhez képest nem tért ki e kategóriára, meghagyva a vonatkozó szabályok definiálását a tagállamok számára [111, p. 19]. Ugyanakkor a NIS irányelv hatályba lépését követően az APT28 csoport [BZs7], 2017 decembertől 2018 február végéig bezárólag a Berlin és Bonn között szövetségi hálózatban (Informationsverbund Berlin-Bonn – IVBB) hálózaton jelen volt [112], amellyel a német szövetségi kancellária, a német parlament, a minisztériumok, a Szövetségi Számvevőszék és biztonsági szervek adataihoz férhettek hozzá, amelyek uniós és más tagállami adatokat is magukban foglalhattak. 2019 júniusában 7 millió bolgár állampolgár közül több mint 4 milliót érintett incidensben [113] a kiberbűnözők személyes adatokat (nevek, címek, személyazonosító számokat és személyi igazolványok adatai) és pénzügyi nyilvántartásokat tulajdonítottak el a bolgár adóhivataltól. Felmerült az Európai Unió tagállamainak együttműködését támogató nemzetközi adatcsere mechanizmus (Eurofisc) [114] kapcsán kezelt adatok érintettsége is. E két eset alapján megállapítható, hogy a NIS irányelv hatályából elhibázott lépés volt a közigazgatási szektor elhagyása, amelyet a NIS 2 irányelvvel az Európai Unió helyesbíteni kíván. A NIS 2 irányelv a központi kormányzatok közigazgatási szerveire és a regionális szintű közigazgatási szervekre is alkalmazandó, ezzel szemben a tagállamok dönthetnek úgy, hogy az irányelvet helyi szintű közigazgatási szervekre is alkalmazzák-e. Ugyanakkor nem zárható ki, hogy a helyi jelentőségű közigazgatási szervek ne férnének hozzá magasabb szerveződési szinthez tartozó adatokhoz. Továbbá kérdéses, hogy az egyes hatóságok milyen hatékonysággal végzik a kockázatalapú besorolásokat, amely alapján egyes szervezetek a jogszabály hatálya alá tartoznak majd.

Ennélfogva körültekintő megoldást aposztrofál, hogy a magyarországi szabályozás szigorúbban jelöli ki az érintetteket. A 2023. évi XXIII. törvény (Kibertan. tv.) [108] a Szállítás ágazat esetén a tömegközlekedési szolgáltatókat, valamint a Gyártás ágazat esetén a Cement-, mész-, gipszgyártás alágazatokat a hatálya alá helyezi. Továbbá a Digitális infrastruktúra ágazatot ketté bontva kezeli: Hírközlési szolgáltatás (az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési szolgáltató, adatkicserélő szolgáltatást nyújtó szolgáltató, az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló törvény szerinti bizalmi szolgáltató) és Digitális infrastruktúra (felhőszolgáltató, adatközponti szolgáltatást nyújtó szolgáltató, legfelső szintű domainnév-nyilvántartó, a DNS-szolgáltató, tartalomszolgáltató hálózat szolgáltatója).

A 2013. évi L. törvény (Ibtv.) [52] hatályába a Kormány és a kormánybizottságok kivételével a központi államigazgatási szervek, a Sándor-palota, az Országgyűlés Hivatala, az Alkotmánybíróság Hivatala, az Országos Bírósági Hivatal és a bíróságok, az ügyészségek, az Alapvető Jogok Biztosának Hivatala, az Állami Számvevőszék, a Magyar Nemzeti Bank, a fővárosi és vármegyei kormányhivatalok, a helyi önkormányzatok képviselő-testületének hivatalai és a hatósági igazgatási társulások, valamint a Magyar Honvédség tartozik. Továbbá a törvény rendelkezéseit kell alkalmazni: a meghatározott szervek és ezen szervek számára adatkezelést végzők, valamint a jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói esetén is. Az Ibtv. vonatkozik az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeknek a létfontosságú tevékenységben közreműködő, az elektronikus információs rendszert működtető, a központi államigazgatási és kormányzati tevékenység szempontjából fontos, nemzetbiztonsági védelem alá eső szervek elektronikus információs rendszereinek védelmére.

1.4 Felügyeleti tevékenységek

A NIS irányelv előírta a tagállamok számára a felügyeleti hatóságok felhatalmazását és szankciók kiszabását, amennyiben az érintett (adott jogalany) nem tartja be az előírásokat, azonban a konkrét hatáskörök és szankciók meghatározását a tagállamokra bízta. A NIS 2 irányelv továbbra is előírja a konkrétumok kidolgozását, de sokkal részletesebb elvárásokat fogalmaz meg a hatóságok végrehajtási jogkörére vonatkozóan. Ezzel összefüggésben a 3. táblázat a joghatóság rendszerét ismerteti az ágazatok vonatkozásában.

Az illetékes nemzeti hatóságoknak arra is felhatalmazással kell rendelkezniük, hogy lépéseket tegyenek a jogalanyok megfelelő intézkedések meghozatalára való ösztönzése érdekében. Ez a figyelmeztetésektől vagy kötelező érvényű utasításoktól a hiányosságok kijavításáig és az ügyfelek tájékoztatásáig terjedhet. Az adminisztratív intézkedések mellett hatékony, arányos és visszatartó erejű közigazgatási bírság is kiszabható. Alapvető jogalanyok esetében legfeljebb 10 000 000 euróig terjedő vagy annak a szervezet által az előző pénzügyi évében elért teljes éves világméretű forgalmának legalább 2%-ával közigazgatási bírság a mérvadó. Fontos jogalanyok esetében legfeljebb 7 000 000 euróig terjedő közigazgatási bírság, vagy az előző pénzügyi évében elért teljes éves világméretű forgalom legalább 1,4%-a a mérvadó, attól függően, hogy melyik a magasabb. A közszféra esetében az átültető jogszabály előírhatja, hogy a közigazgatási bírság nem vonatkozik az államigazgatási szervekre. Azonban a többi közigazgatási szankciót alkalmazni kell.

A tagállamok előírhatnak kényszerítő bírság kiszabására vonatkozó hatáskört is annak érdekében, hogy az illetékes hatóság előzetes határozatával összhangban egy alapvető vagy fontos szervezetet az irányelv megsértésének felhagyására kényszerítsenek. Annak érdekében, hogy a felső vezetés motiválja az ezen irányelvben foglalt kötelezettségek teljesítését, az alapvető jogalanyokat képviselő

természetes személyek felelősségre vonhatók a kötelezettségek elmulasztásáért. (Ez utóbbi lehetőséget a 2023. évi XXIII. törvény (Kibertan. tv.) [108] mellőzi.)

3. táblázat. A NIS 2 irányelv joghatóságra vonatkozó szabályozása

Alapvető ágazat	Fontos ágazat	Joghatóság
1. Energia, 2. Szállítás, 3. Banki szolgáltatások, 4. Pénzügyi piaci infrastruktúrák, 5. Egészségügy, 6. Ivóvíz, 7. Szennyvíz, 8. Digitális infrastruktúra (Minősített bizalmi szolgáltatók, DNS-szolgáltatók, a gyökérnév-szerverek üzemeltetőit kivéve, Nem minősített bizalmi szolgáltatók, Internetes exchange pont szolgáltatók), 10. Közigazgatás	1. Postai és futárszolgáltatások, 2. Hulladékgazdálkodás, 3. Vegyszerek, 4. Élelmiszer, 5. Gyártás, 7. Kutatás (Kutatóhelyek kivéve oktatási intézmények)	Az a tagállam, ahol az üzleti tevékenység szerinti fő hely található
8. Digitális infrastruktúra (Legfelső szintű doménnév-nyilvántartók, Felhőszolgáltatók, Adatközpont-szolgáltatók, Tartalomszolgáltató hálózati szolgáltatók, Nyilvános elektronikus hírközlési hálózatok szolgáltatói), 9. IKT-szolgáltatások irányítása	6. Digitális szolgáltatók, 7. Kutatás (oktatási intézmények, különösen, ha kritikus fontosságú kutatási tevékenységeket végeznek)	Letelepedés szerinti tagállam(ok)
	8. Digitális infrastruktúra (Nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók), 11. Világűr	Szolgáltatás-nyújtás szerinti tagállam

Forrás: Saját szerkesztés

A NIS 2 irányelvvel összefüggésben a 2023. évi XXIII. törvény (Kibertan. tv.) [108] szerinti felügyeleti hatóság a Szabályozott Tevékenységek Felügyeleti Hatósága, illetve a 2013. évi L. törvény (Ibtv.) [52] szerinti hatóság a 187/2015. (VII. 13.) Korm. rendelet [115] értelmében a Nemzetbiztonsági Szakszolgálat. A pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendelet [103] értelmében a Magyar Nemzeti Bank az illetékes hatóság, amely az érintett intézménnyel szemben a 2013. évi CXXXIX. törvényben meghatározott intézkedéseket alkalmazhatja [119 75.§].

Érdemes szem előtt tartani, hogy az adott tevékenységek kapcsán is létezhet felügyeleti hatóság. Például a 2003. évi C. törvény értelmében az elektronikus hírközlési infrastruktúra felügyeletét, valamint a 2015. évi CCXXII. törvény [105], illetve a 2023. évi CIII. törvény [106] alapján a bizalmi szolgáltatások eIDAS Rendelet 17. cikk (1) bekezdése szerinti felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság. A Magyar Nemzeti Bank többek között a 2013. évi CCXXXVII. törvény [102] szerinti hitelintézetekről és a pénzügyi vállalkozások, valamint a 2013. évi CCXXXV. törvény [109] szerinti fizetési szolgáltatók felügyeletét is ellátja. Végezetül a személyes adatok kezelése kapcsán az illetékes

hatóság a 2011. évi CXII. törvény [107] értelmében egységesen a Nemzeti Adatvédelmi és Információbiztonsági Hatóság.

1.5 A kiberbiztonsági követelmények

A hatálya alá tartozó alapvető és fontos szervezeteknek megfelelő és arányos intézkedéseket kell tenniük a hálózatuk és információs rendszereik biztonságát fenyegető kockázatok kezelése, valamint az incidensek megelőzése, illetve az incidensek szolgáltatásaik címzettjeit és más szolgáltatásait érintő hatásainak mérséklése érdekében. Ezek az intézkedések az összes veszélyt átfogó megközelítésen alapulnak, amelynek célja a hálózati és információs rendszerek, valamint e rendszerek fizikai környezetének védelme az incidensekkel szemben. Ezek az intézkedések legalább a következőket tartalmazzák: kockázatelemzés és információs rendszerek biztonsági politikái, kockázatalapú biztonsági program megvalósítása, incidenskezelés, üzletmenetfolytonosság, az ellátási lánc biztonsága, kockázatkezelési intézkedések hatékonyságának értékelésére szolgáló irányelvek és eljárások, kiberhigiéniai gyakorlatok és kiberbiztonsági képzés, kriptográfia, humánerőforrás-biztonság, hozzáférés-ellenőrzési szabályzatok és vagyonkezelés, többtényezős hitelesítési vagy folyamatos hitelesítési megoldások, biztonságos hang-, video- és szöveges kommunikáció, valamint biztonságos vészhelyzeti kommunikációs rendszerek alkalmazása az entitáson belül. Továbbá a vezetőknek elegendő tudást és készségeket kell elsajátítaniuk ahhoz, hogy azonosítsák a szervezetüket fenyegető kockázatokat, és értékeljék a kiberbiztonsági intézkedéseket és azok szervezetükre gyakorolt hatását.

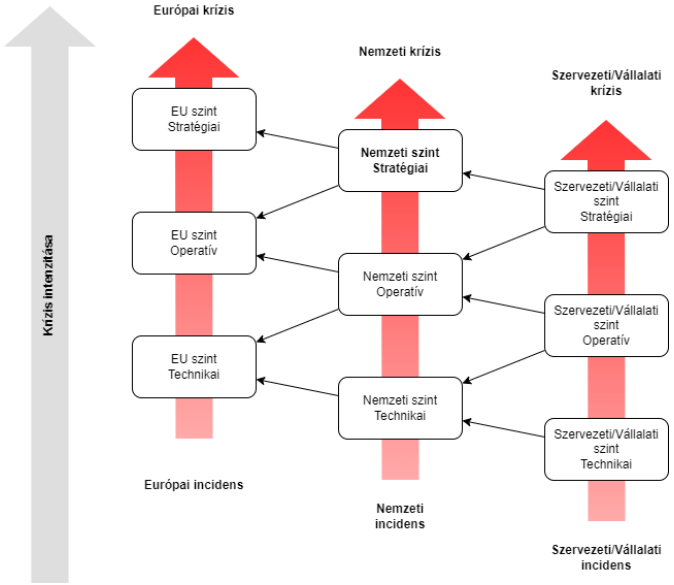
Az Ibtv. Végrehajtási rendelete (Vhr.) 2015-től a 41/2015 BM rendelet [117], amely meghatározza a konkrét követelménypontokat az Ibtv. hatálya alá eső szervezetek számára. Az Ibtv. Vhr 3. mellékletének 2. pontja a védelmi intézkedések katalógust definiál, – amely alapját a NIST SP 800-53 Rev4 [118] adta, – amelyeket a szervezeti vagy elektronikus információs rendszer biztonsági besorolásának megfelelő mértékben kell teljesíteni az érintett feleknek. Az Ibtv. Vhr. majd hatályát veszti, amint „a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről” rendelkező Miniszterelnöki Kabinetirodát vezető miniszteri rendelet hatályba lép [119]. A rendelet a NIST SP 800-53 Rev5 [38] alapján határozza meg a törvényi szinten definiált három biztonsági osztályokhoz az elvárásokat, amely a 2013. évi L. törvény és a 2023. évi XXIII. törvény esetén is alkalmazandó lesz. Érdekesség, hogy míg az Olaszországban hatályos jogszabályi környezet [120] – az alkalmazott kontrollazonosítók alapján megítélve – szintén a NIST követelményekre (egészen pontosan a NIST Cybersecurity Framework [37] meghatározásaira) épít, addig ezzel szemben – Schmidz-Berndt és Pier elemzésére [121] támaszkodva – Németországban a jogszabályi környezet a Szövetségi Információbiztonsági Hivatal (Bundesamt für Sicherheit in der Informationstechnik – BSI) által jóváhagyott ágazatspecifikus

biztonsági előírásokat tesz lehetővé [122]. Az említett kritériumokat a tagállamok eltérő időpontban kezdték el alkalmazni.

A Banki szolgáltatások és Pénzügyi piaci infrastruktúrák ágazatok tekintetében a 42/2015 Kormányrendelet [103] fogalmazza meg az auditálás kritériumait. A követelmények tekintetében értelemszerűen a DORA rendelet a NIS 2 irányelvvel összehangban meghatározott részletszabályai a tagállami elvárásokkal együtt érvényesek.

1.6 Incidensjelentési kötelezettségek

A kiberincidensek, illetve a kiberválság kezelése annak természetétől és hatásától függően a polgári, a bűnüldözési és a védelmi szektor köz- és magánszektorbeli szereplőit vonja be stratégiai, operatív és technikai szinten. Ezek a szereplők különböző szinteken tevékenykednek: szervezeti és vállalati szint, ágazati szint, országos szint, EU szint, nemzetközi szint [123]. A CSIRT-ek hálózata az EU technikai szinten, míg az EU-CyCLONe az EU operatív szinten jelenik meg. A szintek közötti eszkalációs összefüggéseket az ***5***. ábra szemlélteti.



5. ábra. Incidens és krízis eszkalációs modell
Forrás: Saját szerkesztés [124] alapján

A kiberbiztonsági incidensek kezelési módja kapcsán átfedő szabályozásokat azonosítottam, amely eredményeképp az incidensben érintett szervezet számára, feltéve, hogy a jogszabályok hatálya alá tartoznak. A tagállami szabályozás függvényében akár három különböző illetékes hatóságokhoz történő értesítési és együttműködési kötelezettség merülhet fel például a NIS rányelv 6., 14. és 16. cikk, NIS 2 irányelv 23. cikk, a GDPR 33. és 34. cikk, az eIDAS 19. cikk, valamint a PSD2 19. cikk alapján, mely a hazai jogszabályi környezetben is megjelenik (pl. 2013. évi L. törvény (Ibtv.) 13.§ (3)], 2023. évi XXIII. törvény (Kibertan. tv.) 27.§ (1), 2011. évi CXII. törvény 25/J.§, 2013. évi CCXXXV. törvény 92/A.§

(3)). A jogszabályi kötelezettségként előálló különböző incidensjelentések között fennálló átfedéseket az Európai Unió is felismerte [125].

1.7 Összefoglalás és következtetések

A fejezetben áttekintettem 2008-tól kezdődően az Európai Unió kiberbiztonságra vonatkozó fejlődését és elemeztem e fejlődés eredményeképp kialakult aktuális jogszabályi környezetet. A digitalizációs folyamatok következtében az IKT rendszerektől való egyre növekvő mértékű társadalmi és gazdasági függőség a politikai szereplőket és jogalkotókat is újra és újra lépéskényszerbe helyezi. A 2013-ban, 2017-ben és 2020-ban elfogadott uniós kiberstratégia egyaránt a nemzeti és vállalati szintű architektúra, passzív és aktív védelmi képességek kialakításának, valamint az uniós és tagállami szinten az aktív védelmi, hírszerzési és offenzív képességek elősegítését célozta. Míg az uniós szintű entitásokra vonatkozóan a kiberképességek befolyásolása a legutóbbi, 2020-ban elfogadott kiberbiztonsági stratégiában jelent meg újonnan.

A hatályba lépett NIS 2 irányelv több ponton hoz előrelépést elődjéhez képest. Megteremti a kapcsolatot a kritikus infrastruktúravédelemmel, amelyet a NIS irányelv megalkotásakor a jogalkotók tudatosan kerültek, valamint kibővíti az érintett szereplők körét, melyhez egyrészt szakít az OES és DSP megkülönböztetésének módjával, helyette a nélkülözhetetlen és a fontos szervezetek kategóriákat definiálja, és a két új kategória kapcsán megadva az ágazatok, alágazatok és szervezettípusok körét, melyhez immáron a központi kormányzatok közigazgatási szervek és a regionális szintű közigazgatási szervek is csatlakoznak. Azonban a helyi jelentőségű közigazgatási szervek hatályba tartozását a tagállamok mérlegelhetik, valamint kizárja a védelem, a nemzetbiztonság, a közbiztonság, a bűnüldözés és az igazságszolgáltatás területén tevékenységet végző szervek, valamint a tagállami parlamentek és a központi bankok körét. Továbbá a kiberbiztonság piaci szereplői sem tartoznak a jogszabály hatálya alá. A NIS 2 irányelv bevezet egy, a méretkorlátra vonatkozó szabályt, amely alapján általános szabályként az irányelvben foglaltak kiterjednek a hatályába tartozó ágazatokban működő vagy a hatálya alá tartozó szolgáltatásokat nyújtó minden közepes és nagyméretű szervezetre, a bevezetett méretkorlát miatt a mikro- és kisvállalkozások jellemzően hatályon kívül maradnak.

A NIS 2 irányelv meghatározza a teljesítendő minimum követelményeket, azaz minimálisan teljesítendő biztonsági kontrollokat a hatálya alá tartozó entitások vonatkozásában. Ezáltal a vállalati szintű kiberbiztonsági képességeket az Európai Unió egészét tekintve közelíti egymáshoz. Ugyanakkor fennmaradó probléma a jogszabályi átfedések miatt (pl. NIS/NIS 2 irányelv, GDPR) egy esetleges kiberbiztonsági incidens több hatóságnak adott esetben eltérő tartalommal és fókusszal (pl. kiberbiztonsági és adatvédelmi incidens esetén) történő bejelentési kötelezettség fennállása, amelyet a tagállamok eltérő módon valósítanak meg.

2 KIBERBIZTONSÁGI INTERAKCIÓK JELLEMZÉSE ÉS MODELLEZÉSE

Alapozva az Európai Unió által eszközölt kiberfenyegetésekre történő hangsúly áthelyeződésre, a fejezet célja azonosítani és elemezni azokat az összefüggéseket, melyek befolyásolják a fenyegetettségelemzés modellezését és a kiberfenyegetéseket leíró információk megosztását. Valamint ezzel összefüggésben elemzem a kiberbiztonsági incidensek bejelentési módjára vonatkozó technológiai támogatások lehetőségét.

2.1 Fenyegetések azonosításának és elemzésének lehetőségei

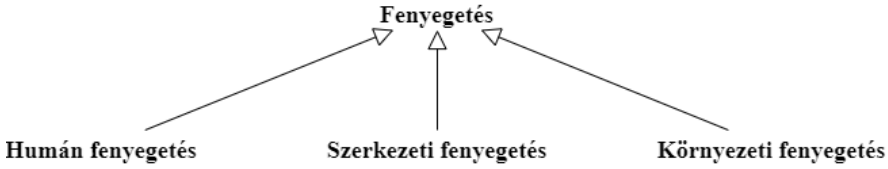
A kockázatok meghatározása a releváns fenyegetettségek azonosítására és a bekövetkezési valószínűségük és a kiváltott hatás mechanizmusának meghatározására alapul. A lehetséges fenyegetettségek szisztematikus azonosítását és elemzését számos módszertani leírás segíti [126]. E módszertanok Bodeau et al. [127, p. 2] összegzése szerint (1) az általános jellegű kockázatelemzési keretrendszerek és módszertanok részeként, (2) az általános kiberfenyegetés modellezés, (3) az IT rendszerekre fókuszált modellezés, illetve a (4) az OT rendszerekre fókuszált modellezés kategóriákba sorolhatóak, ahol mindegyik kategória két-két alkategóriával rendelkezik. Az (1) kategóriába az általános kockázati keretek és módszerek (pl. NIST SP 800-39 [128]) és a kiberkockázatok elemzését támogató általános keretrendszerek (pl. ISO/IEC 27005 [129], NIST SP 800-30 [130]) tartoznak. A (2) kategória a fenyegetés modellezési keretrendszereket (pl. Cyber Threat Framework [131], Attack tree modelling [132]) és a tervezést és tesztelést támogató modellezést sorolja a szerző. Ez utóbbira példaként adódik a DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users and Discoverability) és a STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege) [133]. A (3) kategória az eszközök, taktikák, folyamatok (tactics, techniques, and procedures – TTP) alapú modellezésre (pl. NIST SP 800-30 30 elemű fenyegetés listája [130, pp. E1–E7], MITRE ATT&CK [134], MITRE CAPEC [135]) és a technológia orientált modellezésre (pl. PASTA (Process for Attack Simulation and Threat Analysis) [136]) bontható. A (4) kategória a kiber-fizikai rendszerek (Cyber-Physical Systems – CPS) (pl. MITRE ATT&CK) és az Okos környezetek (pl. ENISA okosautókat érintő fenyegetések modellezése [137]) kapcsán előálló fenyegetettség modellezésére fókuszál.

A fenyegetés az ISO/IEC 27005 szerint „*egy olyan esemény lehetséges oka, amely a rendszerek és a szervezet károsodásához vezethet*” [129, p. 3]. Ehhez képest az ENISA által alkalmazott definíció túlságosan korlátozó jellegű: „*Bármilyen körülmény vagy esemény, amely potenciálisan káros hatással lehet egy eszközre jogosulatlan hozzáférés, megsemmisítés, nyilvánosságra hozatal, adatok módosítása és/vagy szolgáltatás megtagadása révén*” [138]. Ezzel szemben a NIST egy összetett

meghatározást alkalmaz: „*Bármilyen körülmény vagy esemény, amely potenciálisan káros hatással lehet a szervezeti működésre (beleértve a küldetést, a funkciókat, az imázst vagy a hírnevet), a szervezeti vagyon vagy az egyének kompromittálásával az információs rendszeren keresztül, az információk jogosulatlan hozzáférése, megsemmisítése, nyilvánosságra hozatala, módosítása és/vagy szolgáltatás megtagadása révén. Valamint annak lehetősége, hogy egy fenyegetés sikeresen kihasználjon egy adott információs rendszer sebezhetőségét*" [139, p. 9]. Az előző három definícióból az ENISA meghatározásának felhasználásától annak korlátozó jellege miatt eltekintek. Ugyanakkor az ISO/IEC 27005 és a NIST definíciója is kiegészítésre szorul a kiberszemélyiség rétegre jelentett fenyegetések jellegében a személyek, szervezetek, nemzeti vagy szupranacionális aktorok vonatkozásában. Mindazonáltal a fenyegetések – függetlenül azok jellegétől – alapvető jellemzője a bekövetkezési valószínűség, amelyet az adott fenyegetés valamilyen támadási vektoron keresztül fejt ki.

Több módszertani leírás részét képezi egy alapvető fenyegető tényezőket felölelő katalógus, mint például az ISO/IEC 27005 és a NIST SP 800-30. Az ENISA a jelentéseiben a saját taxonómiáját [140] követi, amelyben az ENISA a NIST SP 800-30 rendszerezéséből fakadó fenyegető tényezők mellett azok tevékenységeit is fő kategóriaként alkalmazza. Ugyanakkor a NIS együttműködési csoport által létrehozott 2018-ban kiberbiztonsági incidens taxonómia [141] ettől eltérő módon, a NIST SP 800-30 taxonómia főkategóriához közelebb álló módon öt fő incidens okot különböztetett meg. (Ezzel összefüggésben az ENISA a Threat Landscape 2021 [142, p. 7] jelentésével megkezdte az általa alkalmazott fenyegetettségi kategóriák konszolidálását.)

A NIST SP 800-30 szerint szerkezeti fenyegetést jelentenek berendezések, környezetfelügyeleti eszközök meghibásodása, szoftver elavulása, erőforrás-kimerülés vagy egyéb ok miatt olyan körülmények, amelyek meghaladják a várt működést paramétereket. A taxonomóia ide sorolja az információtechnológiai (IT) eszközöket (tárolás, feldolgozás, kommunikáció, kijelző, érzékelő, vezérlő), a környezetszabályozást (hőmérséklet és páratartalom szabályozás, tápegység), valamint a szoftvereket (operációs rendszer, hálózati, általános célú alkalmazás, célspecifikus alkalmazás). Környezeti fenyegetésnek tekintendő a természeti katasztrófák és kritikus infrastruktúrák meghibásodásai, amelyektől a szervezet működése függ, ugyanakkor a szervezetnek nincs ráhatása az adott tényezőre. Ide tartozik a természeti vagy ember okozta katasztrófa (tűz, árvíz/cunami, szélvihar/tornádó, hurrikán, földrengés, bombázás, megszállás, szokatlan természeti események, mint például napkitörések) és az infrastruktúra meghibásodás/kimaradás (távközlés, elektromosság). A NIST SP 800-30 fő kategóriáit koncepcionális jelleggel a ***6***. ábra szemléltet.



6. ábra. Fenyegetéstípusok a NIST SP 800-30 alapján
Forrás: Saját szerkesztés

A NIST SP 800-30 a humán külső szándékos és belső nem szándékos kategóriákra bontja. Előbbi olyan egyének, csoportok, szervezetek vagy államok, amelyek a szervezet kibererőforrásoktól (azaz elektronikus formában lévő információktól, információs és kommunikációs technológiáktól, valamint az e technológiák által biztosított kommunikációs és információkezelési képességektől) való függőségét kívánják kihasználni. Utóbbi az egyének által a mindennapi feladataik végrehajtása során vétett hibás intézkedések. A belső felhasználók továbbá megkülönbözteti a hozzáférési szinteket.

2.2 Humán fenyegetések jellemzése

A humán eredetű fenyegetésekhez tartozóan a jellemzők meghatározásához a BMIS szerinti tényezőket veszem figyelembe. Ennek megfelelően a szervezeti jellemzőket, az emberi tényezőt, a folyamatokat és az alkalmazott eszközöket vizsgálom, amelyek befolyásolják a szervezeti célokat, a célok mögött meghúzódó indítékot, az effektív képességeket. Ez a megközelítés nem bír korlátozó jelleggel a humán eredetű fenyegetés jellegére vonatkozóan, amennyiben lehetőséget biztosítunk arra, hogy a BMIS modellben megkülönböztetett Szervezetet akárcsak egy személy is alkothasson. Ebben az esetben az alábbiakban ismertetett absztrakció a belső-külső, egyén-csoport-szervezet összetételű humán fenyegetés jellemzésére egyaránt alkalmas leírást biztosít [BZs8, pp. 71-72].

2.2.1 Szervezeti jellemzők

Egy humán fenyegető tényező szervezeti jellemzőiként (1) a szervezeti célok alapja, (2) az együttműködési hajlandóság és (3) az üzleti modell paramétereket tárgyalom [BZs9, pp.27-28].

A szervezeti célok alapja a kibertámadások kivitelezése mögötti, a fenyegető tényező egészét egységesen jellemző indítékot takarja. A szervezeti célok alapja vagy másként a szervezet működésének motivációja az egyének motivációját tükrözi (feltételezhetően különböző mértékben súlyozva az egyes egyéneket). E gondolat mögött a szervezeti magatartás alapvetései és összefüggései húzódnak meg, úgymint a szervezeti felépítés, vezetés, szervezeten belüli együttműködés és döntéshozatal [143]. Feltételezhető, hogy a szervezeti működést még a humán fenyegető tényezők esetében is az együttműködési normák, köztük a kölcsönösség elve szabályozzák [144].

A fenyegetések kapcsán Gandhi et al. [145] politikai, társadalmi-kulturális és gazdasági hajtóerő közt tett különbséget, míg a szubjektív módon kiválasztott piaci szereplő, a Verizon [146] a pénzügyi, a

kémkedés és a szórakozás, ideológia és ellenszenv (Fun, Ideology, and Grudges – FIG) hármasát különbözteti meg, véleményem szerint hibásan tekintettel arra, hogy a kémkedés nem kiváltó tényező, hanem eszköz politikai vagy gazdasági indíttatású célok megvalósítására. (Mindez ismételten terminológiai problémák meglétére hívja fel a figyelmet.) A továbbiakban a politikai, társadalmi-kulturális, gazdasági és FIG szervezeti szintű motívumokat különböztetem meg, mindazonáltal ez a lista nem tekintendő teljeskörűnek.

Ugyanakkor napjaink bonyolult gazdasági és társadalmi működése összetett interakciókat indukálnak nem csak a legitim szereplők, hanem a humán fenyegető tényezők soraiban is, akik a fenti motívumokból származtatható célok elérése végett hajlandóságot mutathatnak a különböző jellegű és mértékű kollaborációra kölcsönös előnyszerzés céljából üzleti ellentételezés nélkül vagy éppenséggel üzleti alapokon. Előbbi megközelítést az együttműködési hajlandóság, az utóbbit üzleti modell megnevezéssel illetem.

Az együttműködési hajlandóság megkülönböztetésének szükségességét a következő példákkal támasztom alá. Elsőként adódik az Észtországot 2007-ben ért kibertámadási kampány, amely első fázisa során több szerényebb képességekkel bíró humán eredetű fenyegető tényező működött együtt észt entitások ellen irányuló túlterheléses (denial of service – DoS) támadások kivitelezése során. Másfelől a 2022. évet meghatározó Ukrajna ellen irányuló orosz támadás következtében több humán fenyegető tényező intézett különböző jellegű kibertámadást (pl. DoS, kiberkémkedés) Oroszország ellen [147]. Kevésbé „látványos" együttműködésre kerülhetett sor 2016 júniusában az Egyesült Államok Demokrata Nemzeti Bizottsága (Democratic National Committee – DNC) ellenében, ahol két orosz fejlett perzisztens fenyegetés (advanced persistent threat – APT) csoport, az APT28 és az APT29 tevékenységére vonatkozóan találtak bizonyítékot a szakemberek [112]. Arról nincs információ, hogy a két csoport ténylegesen együttműködött-e vagy sem.

Ráadásul az együttműködési hajlandóság az alkalmazott eszközök (2.2.4 fejezet) működésére is hatással van. A különböző botnet infrastruktúrák együttműködhetnek más botnethez tartozó botokkal [148, pp. 648–649], másfelől a fenyegető tényezők átvehetik az infrastruktúra irányítását [149], illetve az egyes botok feletti irányítást vagy törölhetik más botnetekhez tartozó bináris állományokat a fertőzött eszközökről [150, p. 11].

Az üzleti alapú együttműködés a kereslet-kínálat törvényszerűségeire [151, pp. 3–8] épül. Az üzleti modell tehát két humán fenyegetés bizonyos típusú együttműködéséből adódó kapcsolatát írja el, amely során az egyik fél a másiktól szolgáltatást vagy eszközt vesz igénybe valamilyen (jellemzően pénzügyi) ellentételezés fejében. E szolgáltatások és eszközök tulajdonképp a „kiberbűnözés mint szolgáltatás" (Cybercrime as a Service) [152] égisze alá tartoznak. A *Crimeware as a Service* keretén belül a (nulladik napos, azaz zero-day) sérülékenységek és az azokat kihasználó, valamint az azt

alkalmazó szándékának eleget tevő exploitok (pl. rootkit, ransomware) érhetők el. Továbbá e kategóriába tartoznak a különböző támogatóeszközök (úgymint dropper, keylogger, bot stb.) és a rejtőzködést megvalósító megoldások (úgymint cryptor, polimorf modulok stb.) [153]. Mindezek alapján a szerényebb képességgel bíró fenyegető tényezők is képessé válhatnak saját támadó eszköz vagy infrastruktúra létrehozására [154, p. 445]. Valamint a felsorolt elemeken túlmenően a fizikai eszközök feltöréséhez szükséges hardverek is ide sorolandóak. A *Cybercrime Infrastructure as a Service* keretén belül teljes infrastruktúra vagy annak egy részhalmaza fölötti teljes vagy részleges irányítási képesség cserélhet (átmenetileg) gazdát. A *Hacking as a Service* modell alapján a támadó az egész támadási folyamatot kiszervezheti egy „szolgáltató" felé, így a támadást a szolgáltató fél tervezi meg és hajtja végre a megrendelő szándékának megfelelően.

Tehát az offenzív képességek tekintetében a műveletek támogatása érdekében, ahogy a MITRE ATT&CK T1587 azonosítójú Fejlesztési képességek (Develop Capabilities) technika [155] összegzi, a humán eredetű fenyegető tényezők kártékony szoftvereket és azok komponenseit, valamint sérülékenységeket kihasználó kódokat, azaz exploitokat fejleszthetnek, illetve mindezekhez külső forrásból pro bono vagy ellenszolgáltatás fejében is hozzájuthatnak a T1588 Képességekhez való hozzáférés (Obtain Capabilities) technika [156] szerint. Ez utóbbira példa a TA542 nevezetű, orosz eredetű humán fenyegetés, amely az Emotet botnet menedzselésével 2017 óta más botnetek, például a Trickbot, Ryuk és számos további botnet terítéséért felelős [157].

2.2.2 Emberi tényező

Az emberi tényező vonatkozásában (1) a motiváció, (2) a tudás, (3) az attitűd és (4) a tudatos cselekvés jellemzőket különböztetem meg. Tekintettel arra, hogy a tudás, az attitűd, valamint a tudatos cselekvés és azzal összefüggésben a heurisztikák témaköröket a Bevezetésben már tárgyaltam, e fejezetben a motivációra térek ki.

A motiváció az az ösztönző erő, amely célt ad a viselkedésnek vagy befolyásolja azt tudatos vagy nem tudatos módon [44], megkülönböztetve külső (extrinzik) és belső (intrinzik) motivációt. Ahogy Ryan és Deci kifejtette [158], az extrinzik motiváció esetén egy adott személy valamilyen külső nyomás hatására (pl. jutalom, társas nyomás) érez késztetést egy adott cselekvés elvégzésére, míg az intrinzik motiváció alapvetően a személyen belül születő (pl. biológiai, pszichológiai) késztetés.

A motivációelméletek arra keresik a választ, hogy mi, azaz milyen szükséglet vagy folyamat magyarázza az emberek viselkedését. Ennek megfelelően két alapvető csoportot különböztetünk meg, a tartalomelméletet és a folyamatelméletet [159]. A tartalomelméletek a motiváció az emberi szükségleteket és a kapcsolódó ösztönző tényezőket vizsgálják, míg a folyamatelméletek azokat a folyamatokat elemzik, amelyek során az emberek bizonyos viselkedésformákat kiválasztanak, illetve utasítanak el a kitűzött eredmények elérése érdekében.

Woodworth [160] szerint a hajtóerő (drive) egy belső erő, amely az emberi magatartást motiválja. A drive-megközelítések a belső feszültség fontosságát hangsúlyozzák a motiváció folyamatában [161], amelyre építve a drive-redukció elmélete [162] azt mondja ki, hogy az ember a szükségállapotból kifolyólag felmerülő feszültség csökkentése, azaz a szükséglet kielégítésének érdekében cselekszik. Bár a kutatók már nem részesítik előnyben ezt a megközelítést, a drive-redukció több elmélet megalkotásához is hozzájárult [163], melyek közül az egyik a tartalomelméletek prominens képviselője, a Maslow piramis.

Maslow [164] szerint az emberek motiváltak bizonyos szükségletek elérésére. Első gondolatai szerint a szükségletek hierarchiába szerveződnek, az alacsonyabb szintű igények nem csak nagyobb prioritást élveznek, hanem azokat előbb ki kell elégíteni, mielőtt a magasabb szintű szükségletek motivátorként működnének. Az ebben a formában Maslow által meghatározott szükséglethierarchia (Maslow piramis) öt szintet különböztetett meg: (1) Fiziológiai szükségletek, mint az emberi túlélés biológiai követelményei, (2) Biztonsági szükségletek, mint az állandóság és kiszámíthatóság, rendezettség iránti igény, (3) Szeretet és közösség iránti igény szükségletek, mint a csoporthoz tartozás, elfogadottság, (4) A megbecsülés, siker, illetve elismerés iránti igények, (5) Önmegvalósítás, azaz az egyéniségben rejlő képességek kibontakoztatása, a fejlődés iránti szükséglet. A hierarchia később a Kognitív szükséglettel és az Esztétikai szükséglettel [165], valamint a Transzcendencia szükségleteivel [166] bővült ki. A bírálatok hatására Maslow [167] rugalmassá tette a hierarchiában a szükségletek sorrendjét a külső körülmények vagy az egyéni különbségek alapján, például egyes egyének számára az önbecsülés iránti igény fontosabb, mint a szeretet iránti igény, míg mások számára a kreatív kiteljesedés igénye a legalapvetőbb szükségleteket is felülírhatja.

Tekintettel arra, hogy a humán fenyegetés számos személyből tevődhet össze, esetükben nem csak a személyes motivációt kell a szervezethez illeszteni, hanem a képességeket is. Miller a 2010-ben zajlott 18. Def Con konferencián megtartott előadása [168] alapján egy (saját részre vagy bérbeadásra szánt) botnet hálózat (2.2.4 fejezet) létrehozásához és működtetéséhez a következő szükséges kompetenciákat sorolta fel: (1) sérülékenység elemzők, (2) exploit (azaz sérülékenységet kihasználó szoftverkomponenst készítő) fejlesztők, (3) az exploit kódok terjesztését, a fertőzéseket végrehajtó bot gyűjtők, (4) bot karbantartók, (5) operátorok, (6) az interneten közvetlenül nem elérhető eszközök botnet részévé tevő távoli személyzet, (7) fejlesztők, (8) tesztelők, (9) rendszergazdák és (10) menedzserek.

2.2.3 Folyamatok

Miller által ismertetett kompetenciák jellegüket tekintve a szakmai feladatok végrehajtása és a vállalat működtetéséhez szükségesek. E kategorizálást a folyamatokra kivetítve a humán fenyegető tényező vonatkozásában a kibertámadói képességeket realizáló, a fenyegetést megvalósító folyamatokat,

valamint a szervezeti működést megvalósító folyamatokat (HR, pénzügyi, beszerzési, logisztikai stb.) különböztetem meg.

Az offenzív kibertevékenységek modellezésére 2011-ben a Lockheed Martin vállalat dolgozta ki a több fázisból álló Cyber Kill Chain (CKC) [169] szisztémát: (1) felderítés (reconnaisance), (2) fegyverkezés (weaponnisation), (3) kézbesítés (delivery), (4) sérülékenység kihasználása (exploitation), (5) telepítés (installation), (6) irányítás (command and control) és a cél megvalósítása (act on objective). A fázisok nem különálló cselekmények, hanem kölcsönhatásba lépnek, átfedik egymást, ugyanakkor a cselekmények szekvenciális lefolyását írják le.

Míg a MITRE 2013-ban kezdte az ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) módszertan fejlesztését, mely hivatalosan 2015 májusában jelent meg. A MITRE ATT&CK egy globálisan elérhető tudásbázis a humán eredetű fenyegető tényezők tevékenységének TTP alapú jellemzésére, amely az alkalmazott taktika és technika leírására szolgál [134]. A Cyber Kill Chain fázisaival ellentétben az ATT&CK keretrendszer nem korlátozódik egy meghatározott műveleti sorrendre. Az ATT&CK alapja, hogy a technikák (techniques) és altechnikák (subtechniques) összessége olyan cselekményeket reprezentálnak, amelyeket a humán fenyegetések végrehajthatnak a meghatározott szervezeti célok elérése érdekében. A technikák azt jelzik, hogy az ellenfél hogyan ér el egy taktikai célt egy akció végrehajtásával, illetve más értelemben azt, hogy „mit nyer” a fenyegető tényező az adatt cselekményt megvalósító támadási minták, eljárások (procedure) végrehajtásával. Az ATT&CK három technológiai tartományt különböztet meg: (1) ATT&CK Enterprise [170], amely a hagyományos vállalati hálózatok és felhőtechnológiák, (2) ATT&CK Mobile [171], amely a mobil kommunikációs eszközök, valamint (3) ATT&CK ICS [172], amely az ipari vezérlőrendszerek elleni támadások leírására szolgál.

A MITRE CAPEC (Common Attack Pattern Enumeration and Classification) [135] számos általános támadási mintát felölelő nyilvánosan elérhető katalógus, amely a humán eredetű fenyegetések által alkalmazott megoldások részleteit és tulajdonságait rendszerezi, rögzítve a támadás egyes részei tervezésének és végrehajtásának módját. A CAPEC a támadási mintákat összekapcsolja a gyengeségek (Common Weakness Enumeration – CWE) [173] és a sérülékenységek (Common Vulnerabilities and Exposures – CVE) [174] adatbázisaival, ezáltal útmutatást adva a támadások hatékonyságának csökkentésére. Míg az ATT&CK keretrendszer a hálózati védelemre összpontosítva írja le a humán fenyegetés életciklusát és részletezi azokat a taktikákat, technikákat és eljárásokat (TTP-k), amelyek az APT típusú fenyegetések modellezését is szolgálják, addig a CAPEC az alkalmazások biztonságára összpontosít megadva az általános attribútumokat és technikákat az ismert gyengeségek és sérülékenységek kihasználásával összefüggésben. A két keretrendszer nem kizárólag

az IT/OT eszközökre fókuszál, hanem az emberi tényező hiányosságainak kihasználása social engineering útján [175] is a részüket képezi.

2.2.4 Alkalmazott eszközök

Míg a fizikai támadás és a social engineering támadás kivitelezése során nem feltétlenül, addig a kibertámadások kivitelezése során az IT eszközök használata egyenesen megkerülhetetlen. Egy támadó által használt IT infrastruktúra bonyolultsága széles skálán mozoghat – kezdve az egyedi, az operátora által útjára indított kártevőtől vagy manuálisan működtetett eszközöktől egészen a több száz vagy épp több ezer, beépített automatizmus szerint működő rendszerekig, változatos offenzív képességeket megvalósítva.

A botnet a számítógépek, okostelefonok, IoT eszközök stb. azon csoportja, amely erőforrásait az eszköz tulajdonosának és/vagy használójának tudta és akarata ellenére egy központi irányítószerveren vagy szervereken keresztül egy támadó vagy támadói csoport ártó szándékkal használja offenzív tevékenység kivitelezésére [BZs7]. A botnetek struktúrájukban, saját működés és az offenzív képességeikben is különbözőek. A struktúrájukat tekintve általánosan elmondható, hogy a botnetek egy irányító felet (botmaster vagy botherder), egy vagy több irányító szervert (Command and Control – C&C) és több irányított gépet (bot) tartalmaznak. A botmaster a teljes botnetet vagy annak egy részhalmazát csökkentett funkcionalitással irányító entitás (támadó). A botmaster által kiadott utasításokat a C&C szerver juttatja el a botok számára, betöltve a botnet operatív irányításának feladatát. A bot a fertőzött eszközön futó szoftver (agent), amely végrehajtja a C&C szervertől kapott utasításokat. A C&C szerver elérésének, elérhetőségének módja szabja meg a botnet felépítését. Ennek függvényében centralizált (hierarchikus felépítésű), decentralizált (peer-to-peer – P2P), valamint hibrid botneteket különböztetünk meg.

A centralizált felépítésű botnetek esetében statikus jellegű a botok vezérlése, azaz előre meghatározott számú, elérési móddal rendelkező egy vagy több fix C&C szerver található a hálózatban. A C&C elérése IP cím alapján vagy DNS rekord lekérdezésével valósul meg. Az utasítások átadása push és pull módon egyaránt megvalósított. A centralizált botnetek esetében a botmaster számára magas fenyegetettséget jelent a C&C szerverek viszonylagosan könnyű azonosítása és azok elérhetőségének lekapcsolása, azaz kiiktatása.

A decentralizált felépítésű botnetek vezérlésében nem azonosítható megkülönböztetett C&C szerver. Ehelyett mindegyik bot nyilvántartja a hálózatban elérhető botok számát, P2P lekérdezési mechanizmussal feltérképezi a környezetében jelenlévő botokat és lekérdezi az utasításokat (pull), vagy épp egy – a botmastertől vagy egy másik bottól – megkapott instrukciót adja tovább (push). A decentralizált botnetek esetén magas fenyegetettséget jelent a botmaster számára a P2P működés kiépítésének és fenntartásának magas bonyolultsága, ezzel összefüggésben a botnet dinamikus

hálózati felépítés jellege (dynamic routing), amelyet megzavarva a rendszer részeire eshet szét, adott esetben működésképtelenné válhat.

A hibrid botnetek kialakítás a centralizált és a decentralizált architektúra előnyeit hivatott egyesíteni. A C&C szerverek esetén a felépítés decentralizált jellegű, ezzel szemben a botok C&C P2P hálózat egy-egy eleméhez csatlakoznak. Ezáltal jelentősen csökken a teljes botnet hálózat detektálásának esélye, így, amennyiben egy C&C szerver azonosításra és eliminálásra kerül, az a botnet hálózatnak mindössze egy részhalmazát érinti.

Az ENISA szerint [176, pp. 130–131] a botnetek működésüket tekintve többlépcsős és moduláris fenyegetést jelentenek a következő jellemzőkkel: (1) az önálló terjedés, (2) önmegsemmisítés, (3) névtelen kommunikáció, (4) az adott cél elérése érdekében történő állhatatos működés, (5) származás elrejtése, és (6) hasznos adatok letöltése és telepítése a fertőzött eszközön akár a memóriában történő elhelyezéssel, akár a tárhelyen történő állandó tárolással.

A támadói képességek tárgyalásához az ENISA által 2022-ben készített jelentést veszem alapul, amely szerint abban az évben a jellemző fenyegetés a kártékony szoftverek, a social engineering, kezelt adatokat érintő műveletek, túlterheléses (DoS) támadás, rendelkezésre állást érintő internetes fenyegetések, dezinformáció és félretájékoztatás volt, amelyek adott esetben az ellátási láncot érintette közvetlenül [177, pp. 7–9]. A továbbiakban a teljeség igénye nélkül ezekre az eljárásokra vagy támadási mintákra adok példát. Ugyanakkor érdemes megjegyezni azt a tényt, hogy az ENISA által alkalmazott kategorizálás nem diszjunkt, például a kártékony kódok közül az adatok érintő műveletek, valamint a rendelkezésre állást érintő internetes fenyegetések és a DoS támadás egyaránt átfedésben vannak. Ez utóbbi két kategória közül a DoS támadásra térek ki.

A kártékony szoftverek és szoftverkomponensek (malware) olyan változatos és sokszínű megoldások összessége, amely például a vírusok, a férgeket, trójai, kémprogramokat is magában foglalja, ahogy Szőr fogalmaz [153]. A vírus (virus) olyan kód, amely célja önmaga rekurzív másolása, melyet a hordozófájlok megfertőzésével és az irányítás átvételével ér el. A féreg (worm) olyan önsokszorosító program, amelyhez nincs szükség gazdaprogramra. A trójai (trojan) nem tud önállóan terjedni, ezért vagy manuálisan, vagy egy másik rosszindulatú programnak kell letöltenie és telepítenie, miközben mindvégig valódi és legális alkalmazásnak mutatja magát. A kémprogram (spyware) a felhasználó beleegyezése nélkül gyűjt és oszt meg személyes és bizalmas információkat [178]. Az információk magukban foglalhatják a vállalat védett adatait, számítógépes, hálózati adatait, a felhasználó személyes adatait beleértve a tevékenységeket és viselkedést is. Az adware a kéretlen reklámozás eszközeként működik, miközben az érintett felek hozzájárulása nélkül képes lehet a felhasználói információk és viselkedésének gyűjtésére.

A kriptovalutabányászat (cryptojacking) arra a módszerre utal, amely az áldozat eszközének feldolgozási teljesítménye beleegyezése nélkül kriptovaluták bányászásához kerül felhasználásra és annak eredménye a támadó fél kriptopénztárcájába kerül [179]. Egy sikeres ransomware támadás megakadályozza, hogy az érintett fél hozzáférjen az adataihoz, és adott esetben az eszközök használatát is meggátolja. A zárolás feloldásához váltságdíjat követelnek, jellemzően kriptovalutában [180]. A Disruptionware a rosszindulatú programok egy sajátos kategóriája, amely célja a működés felfüggesztése és az üzletmenetfolytonosság megzavarása, melyet az adatok visszaállítás lehetősége nélküli titkosításával vagy törlésével ér el a produktív célú rendszerekben és a mentésekben egyaránt [181]. A túlterheléses támadás (DoS) megkísérli megzavarni a célzott entitás IKT szolgáltatását azáltal, hogy túlterheli a célpontot vagy a környező infrastruktúrát. A TCP/IP-modell [182] szerint létezik (1) internetes rétegbeli támadás, mint ICMP flood, smurf támadás és ping of death, (2) szállítási réteg támadás, mint SYN flood és UDP flood, és (3) alkalmazási réteg. Támadások hibás formátumú SSL-kérésekként, valamint HTTP, Telnet, FTP kérések vagy DNS támadások [183].

Az álhír (fake news vagy hoax) [184] nem újkeletű jelenség, azonban a digitalizáció elősegítette ezek elterjedését a különböző weboldalakon és a közösségi médián keresztül egyaránt. Ez utóbbit elősegíti az ún. social botok működése [185], amelyek a szélesebb közönség elérése mellett álhírekről szóló bejegyzéseket terjesztenek, valamint valós közösségi média felhasználók bejegyzéseire reagálnak hamis információk megadása mellett.

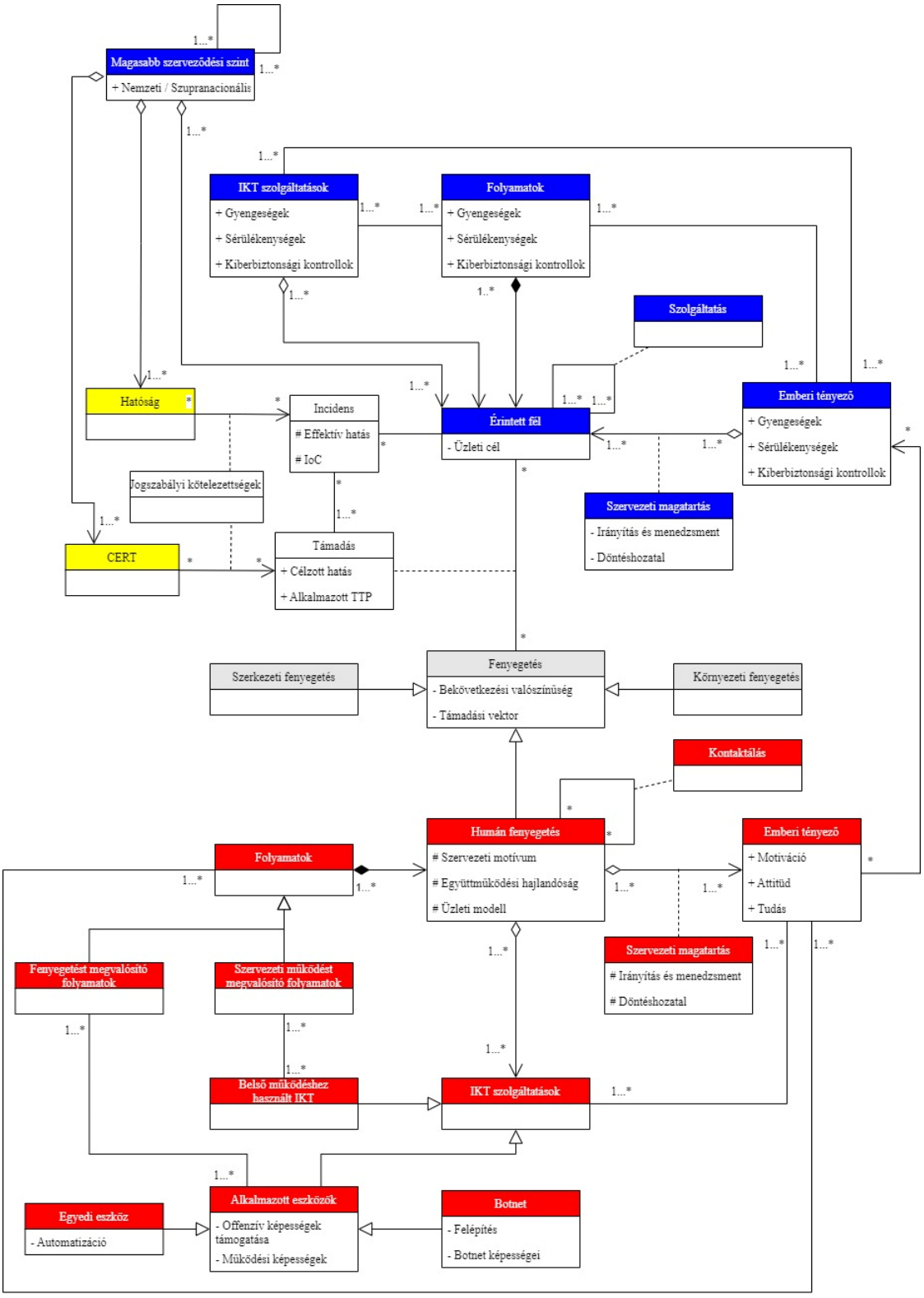
Az álhírek kézbesítése kéretlen levelekkel is lehetséges, ugyanakkor ez inkább a social engineering egy bevett módja a kártékony kódok terjesztésének vagy bizalmas információk megszerzésének érdekében. Az adathalászat olyan üzenetek létrehozásának mechanizmusa, amelyek a felhasználóktól érzékeny információk megszerzésére irányulónak [186]. Ennek speciális fajtája a célzott adathalászat (spear phishing), amely konkrét személyekre irányul.

2.3 A fenyegető tényezők és kiberbiztonságban érintettek kapcsolati modellje

A fenyegető tényezők (mint támadók) és a fenyegetést elszenvedő „érintettek”, vagyis a kiberbiztonságban érdekelt felek (mint védekezők), az attribútumaik, valamint a két oldal közötti kölcsönhatás modellezése kulcsfontosságú a szereplők viselkedésének megértése, továbbá az érdekelt fél (felek) kockázatainak mindinkább valósághű azonosítása érdekében. A modell az eddig tárgyalt összefüggések alapján tevődik össze. A felépítéséhez és szemléltetéséhez az UML (Unified Modeling Language) szabályait [187] követem. A modell ismertetéséhez kétféle nézetet mutatok be, ahol a fenyegetésekkel összefüggésben szemléltetett osztályokat konzekvensen piros, míg az érintett féllel összefüggésben megadott osztályokat kék színnel jelölöm a „red team” és „blue team” analógiájára.

Az első nézet (**7**. ábra) a fenyegetések és az érintettek attribútumait és kapcsolatának jellegét ismerteti. Az érdekelt felek és a humán eredetű fenyegető tényező a BMIS szerint az IKT szolgáltatásokból, folyamatokból és az emberi tényezőből, valamint e három tényezőt összefogó szervezeti egységből épül fel, amely az IKT szolgáltatás és a folyamat esetén aggregáció (rész-egész vagy részben kapcsolat), míg a folyamatok esetén kompozíció alapú a tulajdoni viszony (azaz a folyamat az adott szervezet megszűnésével egyaránt megsemmisül). Az adott szervezetben az emberi tényező működését a szervezeti magatartás összetevő, úgymint a szervezeti hierarchia és vele a döntéshozatal, az irányítás és menedzsment alapvetően meghatározza. Az érintett az üzleti cél, míg a humán fenyegető tényező a szervezeti motívum érdekében cselekszik. Előbbi a piaci alapú együttműködéseivel üzleti folyamathoz, illetve IKT, folyamat és emberi tényező kapcsán szolgáltatást vesz igénybe a szolgáltatóitól és nyújt szolgáltatást az ügyfelei számára. Utóbbi működését az együttműködési hajlandóság és az alkalmazott üzleti modell alapján megvalósított kontaktálás más humán fenyegető tényezővel (együttműködik vagy ellenséges módon viselkedik). A belső fenyegetést megadva az érintett fél emberi tényezője egyirányú kapcsolatban áll a humán fenyegetés emberi tényezőjével, amely a belső fenyegetést hivatott megadni. Továbbá nem szabad arról a tényről elfelejtkezni, hogy a humán fenyegető tényező a szerkezeti és környezeti fenyegetésekkel egyetemben a fenyegetések egy-egy speciális fajtája.

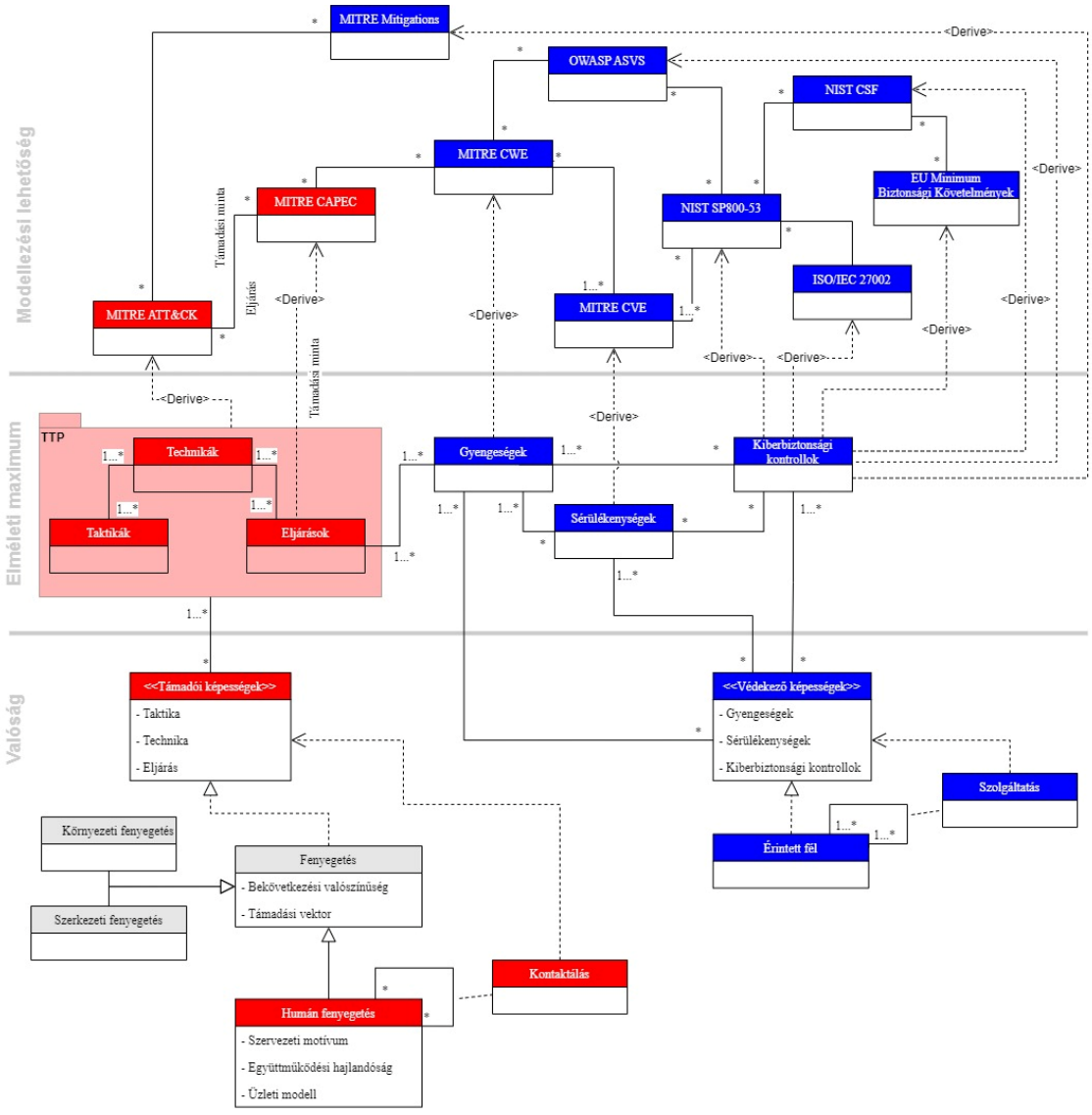
Az érintett fél összetevőinek egységesen a gyengeségek, sérülékenységek és az alkalmazott kiberbiztonsági kontrollok az attribútumai, míg a humán eredetű fenyegetés fenyegető jellegét a folyamatival implementált és az IKT szolgáltatásival és eszközeivel támogatott támadói képességek jelentik. Ennek megfelelően a folyamatok és az IKT szolgáltatások esetén a belső működés és a fenyegetést megvalósító folyamatokat és az alkalmazott eszközöket különböztetem meg, az utóbbit szétbontva egyedi eszközökre és botnetekre. A fenyegető tényező bármilyen tevékenysége vagy működése, amely az érintett ellenében hat, támadásnak minősül, amely a két szemben álló oldalt összeköti és rendelkezik egy célzott hatás, valamint a tényleges tevékenységet megadó TTP leíróval. Ez utóbbi a humán fenyegető tényező tevékenységének leírására szolgáló CTI terminológia (2.4 fejezet), ugyanakkor némi absztrakció mellett a taktika-technika-eljárás hármasa általános jelleggel alkalmazhatóvá válik a fenyegetések egészére vonatkozóan. Értelemszerűen egy támadásból származtatható egy incidens, amelynek tényleges (effektív) hatása és az IoC leíró az attribútuma. A támadásokról és az incidensekről pediglen a jogszabályi kötelezettségek szerinti érdekelt felek (1.3 fejezet) is értesítésre kerülnek, úgymint a CERT-ek és a különböző hatóságok. Végezetül az érintett és érdekelt felek egy magasabb szerveződési szintbe szerveződnek.



7. ábra. A fenyegetések és az érintettek attribútumainak és kapcsolatának modellje
Forrás: Saját szerkesztés

A második nézet (***8***. ábra) a fenyegetések és az érintettek kapcsolatának és attribútumaik meghatározásának lépéseit, illetve lehetőségeit ismerteti, megkülönböztetve a valóság, az elméleti maximum és mindezek gyakorlati szempontból lehetséges modellezési lehetőségeit. Az ábra az

átláthatóság végett a humán entitások BMIS elemeit nem szemlélteti. A valóságot a humán fenyegetés, szerkezeti fenyegetés és a környezeti fenyegetés hármasából előálló fenyegetések és a kiberbiztonság megvalósításában érintett fél reprezentálja. A fenyegetés oldalán interfészként jelenik meg a támadói képességek osztály, amelyet a humán fenyegető tényező esetén a kontaktálás befolyásol (erősít vagy gyengít). A védekező fél esetén az interfészt a védekező képességek osztály reprezentálja, amelyet az igénybe vett szolgáltatás osztály befolyásolhatja (erősítheti vagy gyengítheti). A két interfész tulajdonképp az elméleti maximumban létező lehetőségekből tevődik össze, azaz támadói képességek esetén a TTP aggregált osztállyal, míg a védekező képességek esetén a gyengeségek, sérülékenységek és kiberbiztonsági kontrollok osztályokkal van asszociációs kapcsolatban.



8. ábra. A fenyegetések és az érintettek modellezési lehetőségei
Forrás: Saját szerkesztés

A TTP, valamint a gyengeségek, sérülékenységek és kiberbiztonsági kontrollok a valóságban létező vagy elérhető lehetőségeket testesítik meg, melyek leírására, jellemzésére a rendelkezésre álló

keretrendszerek nyújtanak lehetőséget. A fenyegetések számára az ábra a MITRE ATT&CK és a MITRE CAPEC keretrendszereket tünteti fel. Az ellenkező oldal tekintetében a gyengeségeket a MITRE CWE, a sérülékenységeket a MITRE CVE reprezentálja, azonban a kiberbiztonsági kontrollokhoz a NIST SP 800-53, a NIST CSF, az ISO/IEC 27002, az OWASP ASVS és a MITRE Mitigations, valamint az EU Minimum Kiberbiztonsági Követelmények keretrendszer szerepel példaként.

A fenyegetés (vagy támadó) és a fenyegetett fél (védekező) közötti kapcsolatot, azaz az ATT&CK taktikák és az ismert sérülékenységek között a kapcsolati láncolatot a Taktika – Technika – Eljárás – Támadási minta – Gyengeség – Sérülékenység szekvencia alapján lehetséges meghatározni [188]. A keretrendszerek ily módon történő összekapcsolása választ adhat arra a kérdésre, hogy egy adott eszköz milyen módon támadható és védhető meg.

2.4 Kiberfenyegetés felderítés

A kibertérfölény elérésének egyik eleme az elektronikai és informatikai adatgyűjtő eszközökre, szenzorokra és kommunikációs eszközökre alapozva az információ biztosítása egy másik fél képességeiről, a saját lehetőségekről és a környezetről. Ezzel összefüggésben az intelligence, azaz a felderítés az adatok gyűjtése, információként való hasznosítása és a felderítési adatok előállítása feladatok láncolataként került definiálásra. A kiberfenyegetés felderítés (Cyber threat intelligence – CTI) a Gartner definícióját [189] alapul véve bizonyítékokon alapuló tudás egy adott külső humán eredetű fenyegetésre vagy veszélyre adott válaszlépések meghozatalára egy meglévő vagy kialakulóban lévő fenyegetésről vagy veszélyről, beleértve a fenyegetésre vonatkozó kontextust, eszközöket, kompromittálódás mutatókat (Information of Compromise – IoC), következményeket és a védekezésre vonatkozó információkat.

A kiberfenyegetések felderítése azok folyamatos változása, fejlődése következtében nagy kihívást ennek megfelelően nagyobb erőforrásbefektetést jelent, – ahogy „„A kiberbiztonság csúszó skálája” is szemlélteti (4. ábra), – amelyhez a kiberbiztonságban különböző szinten érintett szereplők gyors alkalmazkodása szükséges. (Ez indukálhatta a kiberfenyegetés felderítésének az ISO/IEC 27002:2022 biztonsági kontrollok [36] közé történő felvételét is.) A kiberfenyegetésekre vonatkozó hírszerzési ciklus az érintettek számára egy erőforrásoptimalizálás és hatékonyságnövelés megvalósítására biztosít keretet [190]:

1) A hírszerzés céljainak és megvalósításra vonatkozó módszertan meghatározása, továbbá a kritikus eszközök, azok gyengeségeinek és sebezhetőségeinek (mint támadási felület), valamint a kapcsolódó információszükséglet azonosítása a fenyegető tényezők és azok motivációja és a jövőbeli kibertámadási kísérletek és azok elleni védelmi lehetőségek vonatkozásában.

2) A meghatározott célok elérése érdekében az adott szervezet szempontjából belső (pl. naplóbejegyzések) és külső információforrások (pl. közösségi hálók) azonosítása és az adatgyűjtés megkezdése.
3) A beszerzett nyers adatok elemzésre alkalmas állapotba történő konvertálása, amely magában foglalhatja az adatok táblázatokba rendezését, a bináris állomány visszafejtését, a titkosított adatok dekódolását, a külföldi forrásokból származó információk lefordítását, valamint az adatok relevanciájának és megbízhatóságának értékelését.
4) Az adatelemzés során az adatkészlet alapján a meghatározott céloknak megfelelő intézkedések foganatosítása és ajánlások megfogalmazása.
5) Az elemzés eredményének az elvárt formában történő disszeminációja az érintett felek számára.
6) Az érintett felek részéről visszacsatolás az elvárások teljesítésére és változtatási igényekre vonatkozóan.

A kiberfenyegetés felderítést több szempontból lehetséges kategorizálni, amelyek közül a folyamat eredményeképp kinyert információ felhasználási célja és felhasználója a legjelentősebb kategorizálási mód [191, pp. 214–215]. E téren Chismon és Ruks [192], valamint Korstanje [193] is a kiberfenyegetés felderítést négy különálló tartományra osztotta: stratégiai fenyegetés-felderítés, operatív fenyegetés-felderítés, taktikai fenyegetés-felderítés és műszaki fenyegetés-felderítés.

A stratégiai fenyegetés-felderítés célja a döntéshozók számára az ismert kockázatok mélyrehatóbb megértésének és a további, korábban nem ismert kockázatokat azonosításának elősegítése. Az ismertetett információ kiterjedhet a kiberbiztonsági incidensek pénzügyi hatásaira vagy a kibertámadási trendekre formális vagy informális jelentések és tájékoztatók formájában. Az operatív fenyegetés-felderítés által szolgáltatott információ az érintett szervezet elleni közelgő támadásokat öleli fel, amelyet elsődlegesen a szervezet biztonsági vezetője és az incidensreagálási csoport vezetője használ fel. A taktikai fenyegetés-felderítés a fenyegető tényezők által végzett tevékenységekre jellemző TTP jellemzésére nyújt információt a kibervédelem megerősítése céljából vagy éppenséggel egy bekövetkezett incidens reagálása során. A technikai fenyegetés-felderítés jellemzően egy szervezet preventív és detektív jellegű eszköz- és hálózatfelügyeletéhez, illetve az incidensek kivizsgáláshoz nyújt technikai IoC leírókat, mely a fenyegető tényezők által kivitelezett kibertámadások és a szervezet kibervédelme közötti szakadékot csökkenti, ahogy Manco fogalmaz [194, p. 8].

A fenti kategorizálás piaci alkalmazásának ellenőrzése végett a Gartner által megkülönböztetett (vizsgált), CTI szolgáltatást közvetlenül vagy más szolgáltatáshoz kapcsolódóan nyújtó, meghatározó kiberbiztonsági piaci szereplők közül szubjektív alapon kiválasztottam a Crowdstrike [195], a Check Point [196] és a Recorded Future [197] piaci szereplőket. A három szolgáltató egységesen három CTI

kategóriát különböztet meg a négy helyett. Azonban míg a Crowdstrike [190] és a Check Point [198] esetében az operatív felderítés a TTP és a taktikai az IoC, addig a Recorded Future [199] esetében a taktikai felderítés a TTP és operatív az IoC információk megismerését szolgálja. Ez alapján megállapítható, hogy a Bevezetésben említett terminológiai problémák a CTI területét is jellemzi a kutatók és az iparág között, továbbá az iparági szereplők közt egyaránt. Függetlenül a kategorizálás módjától és a kategóriák megnevezésétől, a TTP, az IoC és a stratégiai vonatkozású információk egységesen jelentős értéket képviselnek és meghatározóak a CTI területén.

2.5 Információk megosztása

A kiberfenyegetésekkel kapcsolatos aktuális és releváns információk megosztása a kiberbiztonságban érdekelt felek számára kulcsfontosságú az aktuális kockázatok azonosítása, valamint azok csökkentése érdekében történő preventív és reaktív biztonsági kontrollok finomhangolása végett. Ráadásul ami az egyik szervezetnek incidenst jelentett, más felek számára létfontosságú információ lehet. Ahogy a NIST SP 800-150 kimondja [200, pp. 2–3], jellemzően az IoC, a TTP, a biztonsági riasztások, a kiberfenyegetésekről szóló jelentések és az eszköz beállítások tartoznak ezen információk közé.

Másfelől az információk bárminemű publikálása, megosztása (pl. versenytársak felé) érthető okból kifolyólag érzékeny terület minden szervezet számára. A szervezetek közötti bizalom kialakítása mellett a folyamatszintű és technológiai együttműködés megszervezése, a megosztott információ védelmének biztosítása és megfelelő módon történő feldolgozása egyaránt kihívást jelent a CTI kialakításában. Ugyanakkor olyan előnnyel jár, mint a gyorsabb és hatékonyabb reagálás a fenyegetésekre, ezáltal magasabb szintű kibervédelmi képességek kialakulása és fenntartása [200, pp. 3–5]. Ennek megfelelően az Európai Unió a NIS irányelv [78] és a NIS 2 irányelv [91] alkalmazásával az információmegosztást igyekezett, illetve igyekszik megfelelő módon kialakítani.

2.5.1 Platformok

Ahogy Wagner et al. [201] rámutat, a jelenlegi megosztási módszerek nagymértékben manuálisan megadott bementi adatokon alapulnak, például e-maileken, telefonhívásokon, weboldalakon, közösségi platformokon, megosztott adatbázisokon keresztül, és ezért erőforrás- és időigényesek. Ezek csökkentése, a CTI sikeres disszeminációjának kulcsa az automatizálás, amelyhez értelemszerűen támogató célmegoldások szükségesek. A szerzők számos CTI platformot meg is adnak példaként [201, p. 5]. A felsorolt platformok közül az Európai Unió szempontjából kiemelkedő jelentőségű a Malware Information Sharing Platform (MISP) [202], amely az eredeti funkcionalitását túlhaladva egy közösség által vezérelt projektté fejlődött a különféle típusú fenyegetések összegyűjtésére, megosztására és korrelációjára, mint például az IoC, a pénzügyi csalásokkal kapcsolatos információk és a terrorizmusellenes információk.

2017-ben keltezett, az Európai Távközlési Szabványügyi Intézet (European Telecommunications Standards Institute – ETSI) által jegyzett dokumentum [203], amely a NIS irányelvvel összefüggésben tett javaslatokat tartalmazza, a CTI platformok között jegyezte a MISP platformot. Az Európai Unió által finanszírozott ECOSSIAN projekt [204], amely az ECI kapcsán a kiberbiztonsági incidensek kezelésére vonatkozó, a vállalati SOC, valamint a nemzeti és uniós CSIRT, illetve CERT szervezetek együttműködését támogató rendszer lehetséges architektúráját adta meg, már a MISP platformra alapult. Így nem okozott meglepetést, amikor 2017 október végén tartott CTI-EU eseményen a CERT-EU képviseletében Satlas előadásában a MISP platformra támaszkodva ismertette a hallgatósággal a támogató infrastruktúra architektúráját [205].

Manapság a MISP platformot az egyik vezető OSINT platformnak tekintik, amely különböző területeken – beleértve a NATO ügynökségeket és védelmi minisztériumokat, uniós szereplőket, a CSIRT közösségeket, a magánszektor szereplőit – aktívan alkalmaznak [206], melyhez a CSIRT és a rendvédelmi szervek közötti információcsere támogatása is [207], valamint a NIS irányelvnek való megfelelés támogatása [208] is hozzájárult.

2.5.2 Fenyegetéseket leíró szabványok

Az automatizáláshoz a CTI megosztó platformok olyan szabványokra támaszkodnak, mint az OpenIOC (Open Indicators of Compromise), az IODEF (Incident Object Description Exchange Format), a VERIS (Vocabulary for Event Recoding and Incident Sharing) és a STIX (Structured Threat Information Expression), melyek bár nem merítik ki az összes rendelkezésre álló lehetőséget, de reprezentálják az alkalmazott megoldások jelentős részét [201], [206]. Továbbá a megosztásban az előírások és elvárások függvényében az Érzékeny Dokumentumok Megosztási Alapelveket (Traffic Light Protocol - TLP) [209] szükséges alkalmazni, amely az érzékeny információk megosztásának de facto jelölési rendszere [210].

Az OpenIOC [211] egy nyílt keretrendszer, amely a IoC információk XML (Extensible Markup Language) alapú megosztására szolgál, melyet a Mandiant fejlesztett ki 2011 novemberében. Az IODEF [212] az IETF (Internet Engineering Task Force) által létrehozott XML séma az incidensek támadásközpontú reprezentálásához. Az alapstruktúra előre definiált attribútumokat és mezőket biztosít, melyhez szabadszöveges mezőket kínál további, nem strukturált információk rögzítéséhez. A 2. verzió a metrikák, a támadók és a védekező intézkedések számára vezet be leírókat. A VERIS [213] a Verizon által létrehozott, JSON (JavaScript Object Notation) formátumú leíró. A specifikáció a tényleges események leírásán kívül kiterjed a lehetséges hatásokra vonatkozó becslésekre, továbbá lehetővé teszi a JSON objektumok és mezők egyedi meghatározását (pl. rosszindulatú programok típusai).

A STIX a MITRE és Egyesült Államok kormánya által fejlesztett, széles körben elfogadott leíró struktúra [201, p. 7]. A STIX 1 verziócsalád [214] XML alapú kiterjedt incidens jelentési képességeket biztosít, amelyhez a komponenseket hierarchikus struktúrában reprezentálja, előre meghatározott attribútumokkal és mezőkkel az IoC, fenyegetések, a megfelelő ellenintézkedésekről és az incidensekre vonatkozó jelentések vonatkozásában, valamint támogatva a külső hivatkozások megadását, melyhez a CybOX (Cyber Observable eXpression) külső szabványként integrálódott. A CybOX [215] támogatja többek közt a fenyegetések leírását, jellemzését és értékelést (beleértve a részletes támadási mintákat), a rosszindulatú programok jellemzését, valamint az eseménykezelési, a naplózási, incidensreagálási információk rögzítését.

A STIX szabványt 2015 június 18-tól az *OASIS Cyber Threat Intelligence (CTI) Technical Committee (TC)* [216] tartja karban, így a STIX 2 létrehozása már e bizottsághoz kötődik. Az elődjével ellentétben a STIX 2 dinamikus megközelítést alkalmaz a kiberfenyegetések JSON alapú leírására, megváltoztatva az alapmodellt, valamint integrálva a CybOX leírót, amely megszűnt független struktúrának lenni. A STIX 2 képes kezelni a MITRE MAEC (Malware Attribute Enumeration and Characterization), MITRE ATT&CK, a MITRE CAPEC és a MITRE CVE leírókra való hivatkozásokat [217]. A MAEC (kiejtve: „mike") [218] JSON alapú strukturált leíró, amely a CybOX képességeire alapozva a rosszindulatú programokkal kapcsolatos információk precízebb kódolására hivatott.

A STIX a TAXII (Trusted Automated eXchange of Indicator Information) [219] alkalmazásszintű protokollra támaszkodik a CTI HTTPS-en keresztül megvalósított cseréjéhez, amelyhez RESTful API-t definiál, meghatározva a követelményrendszert a TAXII ügyfelek és kiszolgálók számára. A TAXII kifejezetten a STIX alapú CTI megosztásának támogatására készült, a STIX 2.1 alapú információmegosztás támogatása pedig kötelező jellegű. A TAXII azonban független szabvány, más formátumú adatok megosztására is használható.

Ahogy Ramsdale et al. [220] felhívja a figyelmet, az OpenIOC és az IODEF formátumok kapcsán évek óta nincs változás, így a szerzők elavult sztenderdnek tekintik őket. Bár ez a megállapítás 2020 májusában történt, annak ellenére, hogy a FireEye a változásleíró (changelog) szerint 2019-ben változtatott az OpenIOC formátumon. Az IODEF 2016 óta valóban nem változott. Másfelől a MITRE jelentős erőfeszítést tett annak érdekében, hogy a STIX a CTI domináns leíró nyelve és a TAXII a CTI megosztásának meghatározó alkalmazásprotokollja legyen [201]. Ennek jelentős eredménye lett, hogy az ENISA 2016 novemberében megfogalmazott ajánlásával összhangban [221] az ETSI az Európai Unió tagállamai számára a STIX/TAXII bevezetését javasolta [203]. Még ugyanebben az évben, 2017-ben az Európai Unió hivatalos határozatot [222] fogadott el, amelyben a STIX 1.2 és TAXII 1.1 szabványokat alkalmasnak mondta ki a közbeszerzésekben történő kiírásra. A STIX/TAXII támogatása

2022-ben is változatlan jellegű volt [223]. (A MITRE szabványok támogatása nem egyedülálló, például az ENISA éves fenyegetettségi jelentéseiben a MITRE ATT&CK taxonómiát is alkalmazza [224].)

MISP projekt 2019-ben új struktúrát alakított ki azzal a céllal, hogy szabványosítsa a formátumot, mely eredményeként 2019 novemberétől öt hivatalos szabvány jelent meg [225]: (1) MISP alapformátum (MISP core), (2) MISP objektum sablon formátum (MISP object template format), (3) MISP taxonómia formátum (MISP taxonomy format), (4) MISP galaxis formátum (MISP galaxy format) és (5) SightingDB formátum (SightingDB format). A MISP alapformátum JSON alapú formátum, mely az IoC és a fenyegetési információk cseréjére szolgál a MISP példányok között. A MISP objektum sablon formátum egy egyszerű JSON formátumot ír le, amely a MISP objektumok létrehozásához használt különféle sablonokat definiálja. A MISP által a kiberbiztonsági események, fenyegetések, gyanús események vagy IoC osztályozására alkalmazott taxonómia nyilvánosan elérhető, mely a MISP taxonómia formátumra alapul. A MISP taxonómiai formátum egy egyszerű JSON formátumot ír le. A MISP galaxis formátum egy JSON formátumot takar a galaxisok és klaszterek megjelenítésére, amelyek MISP eseményekhez vagy attribútumokhoz kapcsolhatók. A MISP galaxisok további információs struktúrák, például MISP események vagy attribútumok csatolására szolgálnak. A MISP galaxis ismert rosszindulatú programok, fenyegető szereplők és különféle egyéb adatgyűjtemények nyilvános tárháza, amelyek felhasználhatók adatok megjelölésére, osztályozására vagy címkézésére a fenyegetéssel kapcsolatos információk megosztása során. A SightingDB formátum a Sightings szolgáltatással történő együttműködést biztosítja. (A SightingDB egy olyan adatbázis, amely egy adott attribútum időbeli előfordulásaira vonatkozó statisztikákat biztosít.)

2.6 A kapcsolati modell elemzése

Tekintettel arra az összefüggésre, hogy bár a MISP platformspecifikus formátumot követ, de biztosítja a STIX formátummal történő kompatibilitást, a fenyegető tényezők és kiberbiztonságban érintettek kapcsolati modelljét (7. ábra) a STIX 2.1 szabvány alapján elemzem. Az összehasonlítás eredményét a 4. táblázat ismerteti, alkalmazva a modell színkódjait a könnyebb átláthatóság végett. A táblázat az áttekinthetőség végett nem tartalmazza az összes STIX objektumot és attribútumot.

Az összehasonlítás eredményeként pozitívumként megállapítom, hogy a STIX képes kezelni (P1) incidenseket. Ugyanakkor az incidensek kezelése jelenleg nem a hatósági bejelentések szerint valósul meg. Azonban ahogy a MISP platform a pénzügyi csalásokkal kapcsolatos információk és a terrorizmusellenes információk megosztására alkalmassá vált, úgy a hatósági bejelentésre is képessé tehető. További pozitívum (P2) humán fenyegetések együttműködésének modellezése. Másfelől, mint negatívum, (N1) leegyszerűsítve kezeli az emberi tényező attitűd, tudás és szervezeti magatartás attribútumait, (N2) az érintett fél IKT szolgáltatásait megvalósító infrastruktúra sérülékenységeire és az azokat kihasználó támadásokra fókuszál, az emberi tényező, a folyamatok hiányosságait nem kezeli,

valamint (N3) nem képes a fizikai támadások modellezésére, továbbá (N4) nem képes a kiberfenyegetésektől eltérő, általános jellegű fenyegetések modellezésére.

4. táblázat. A fenyegető tényezők és kiberbiztonságban érintettek kapcsolati modelljének összehasonlítása a STIX 2.1 szabvány elemeivel

Modell (7. ábra)		**STIX 2.1** [226]	
Osztály	**Attribútum**	**Objektum**	**Attribútum**
Emberi tényező	Támadás/Célzott hatás	*Threat actor*	*Type*
Humán fenyegetés	Motiváció		*Primary_motivation, Secondary_motivation*
			Personal_motivation
	Attitűd		*Sophistication*
	Tudás		
	Szervezeti magatartás		
	Kontaktálás		*Threat Actor Role - Az ellenséges viszony*
Alkalmazott eszközök	Offenzív képességek	*Tool & Infrastructure*	*Attack pattern*
Egyedi eszköz	-	*Tool*	-
Botnet	-	*Infrastructure*	-
Belső működéshez használt IKT	-	-	-
Támadás	Célzott hatás	*Campaign*	*Objective*
	Alkalmazott TTP		*Attack pattern*
Incidens	IoC	*Incident*	-
	Effektív hatás		-
Érintett fél	Üzleti cél	*Identity*	*Sector*
Emberi tényező	Szervezeti magatartás		*Roles*
IKT szolgáltatások	Sérülékenység	*Infrastructure*	*Vulnerabilities*

Forrás: Saját szerkesztés

2.7 Összefoglalás és következtetések

A fejezetben a kiberfenyegetéseket tárgyaltam. A kitűzött biztonsági szint eléréséhez és fenntartásához szükséges a lehetséges fenyegetések szisztematikus azonosítása és elemzése, amelyet számos módszertani leírás segíti, melyek: (1) az általános kockázati keretek és módszerek (pl. a NIST SP 800-39 és az ISO/IEC 27005), (2) a fenyegetés modellezési keretrendszerek (pl. Attack tree modelling), (3) az eszközök, taktikák, folyamatok (TTP) alapú modellezésre (pl. NIST SP 800-30 30 elemű fenyegetés listája, MITRE ATT&CK, MITRE CAPEC) és (4) a kiber-fizikai rendszerek (CPS) (pl. MITRE ATT&CK) és az Okos környezetek elemzése.

A fenyegetésekről szóló információk megosztása kulcsfontosságú, tekintettel arra, hogy azok alapján a védelmi képességek az adott fenyegetés ellenében megerősíthetőek. A kiberfenyegetés felderítés

(CTI) bizonyítékokon alapuló tudás egy adott külső humán eredetű fenyegetésre vagy veszélyre adott válaszlépések meghozatalára egy meglévő vagy kialakulóban lévő fenyegetésről vagy veszélyről, beleértve a fenyegetésre vonatkozó kontextust, eszközöket, kompromittálódás mutatókat (IoC), következményeket és a védekezésre vonatkozó információkat.

A kiberfenyegetésekre vonatkozó információk szervezeten belüli és szervezetek közötti megosztása gyakorta manuálisan megadott bementi adatokon alapulnak (e-mail, telefonhívás, weboldal, közösségi platform, megosztott adatbázis), és ezért erőforrás- és időigényesek. A CTI sikeres disszeminációjának kulcsa az automatizálás, amelyhez értelemszerűen támogató célmegoldások és azok széleskörű alkalmazása szükséges. Az Európai Unióban de facto megoldásnak a MISP platform bizonyul, amely a saját modellezése mellett támogatja az Egyesült Államok kormányzati szervei részvétele mellett fejlesztett STIX leíró alkalmazását.

Részletesen jellemeztem a humán fenyegetéseket, amelyet két UML alapú nézetben ismertettem. Az első nézet a fenyegetések és az érintettek attribútumait és kapcsolatának jellegét ismerteti. Az érdekelt felek és a humán eredetű fenyegető tényező a BMIS szerint az IKT szolgáltatásokból, folyamatokból és az emberi tényezőből, valamint e három tényezőt összefogó szervezeti egységből épül fel. A második nézet a fenyegetések és az érintettek kapcsolatának és attribútumaik meghatározásának lépéseit, illetve lehetőségeit ismerteti, megkülönböztetve a valóság, az elméleti maximum és mindezek gyakorlati szempontból lehetséges modellezési lehetőségeit. A modellt összehasonlítottam a STIX képességeivel és megállapítottam, hogy a STIX, valamint a MISP platform képes a kiberfenyegetések modellezésére, valamint a kiberfenyegetésekre vonatkozó információk (TTP és IoC) megosztására, beleértve az incidenseket is. Ugyanakkor ezek a megoldások némi fejlesztés árán képesek lennének a fenyegetések általános jellegű modellezésére, ahogy az emberi tényezőt és a fizikai térben kivitelezett behatások modellezésére is. Jelen formában a stratégiai fenyegetés-felderítést közvetlenül nem támogatja sem a STIX, sem a MISP saját modellje.

3 KIBERBIZTONSÁGI INCIDENSEK VIZSGÁLATI MÓDSZERTANA ÉS MEGVALÓSULÁSA

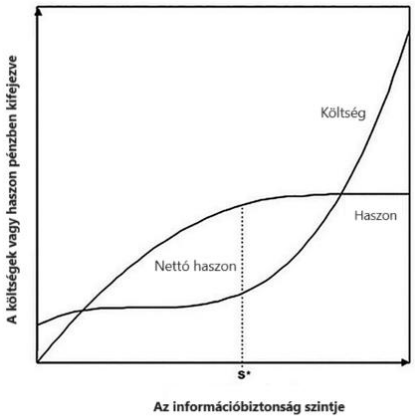
A fejezettel összefüggésben a célom a kiberbiztonság tervezésének, valamint a megvalósulására vonatkozó visszamérés elméleti keretének pénzügyi-gazdasági szempontú meghatározása, továbbá a kialakított elmélet gyakorlati alkalmazhatóságának tesztelése, amelyhez a fejezet tartalma általános jelleggel épít az 1. függelékben meghatározott összefüggésekre. A függelék a vállalkozások pénzügyi tervezésének és visszamérésének lehetőségeit tárgyalja, amelyek adott pénzáramokra (cash flow – CF) [227], [228] építenek. A nettó jelenérték (net present value – NPV) és a nettó jövőérték (net future value – NFV) a pénzáramok egyszerű vizsgálatát valósítják meg [229]. Tervezésnél a pénzáramok becslése explicit és implicit időszakra bomlik, ahol az explicit időszak részletes pénzáramokkal, míg az implicit időszak a maradványértékkel számol. A pénzáramok gazdasági profitabilitás jellegű vizsgálatához bonyolultabb összefüggéseket is figyelembe kell venni, melyekre számos diszkontált cash-flow módszer rendelkezésre áll, például a Diszkontált pénzforgalom (Discounted Cash Flow – DCF) [230], a Szabad pénzáram (Free Cash Flow – FCF) [231], [232] és a Módosított jelenérték (Adjusted Present Value – APV) [233]. A diszkontált cash-flow módszerek végrehajtásuk részleteiben különböznek, ennek megfelelően eltérő algoritmussal és változókkal dolgoznak [234], a mutatók pedig igen érzékenyek a pénzáramok és a kamatlábak minél pontosabb meghatározására [235].

A részvényesi tőkeköltség (kamatláb) meghatározásának prominens módja a Capital Asset Pricing Model (CAPM) [236] alkalmazása (részletesen tárgyalva Elbannan [237] által) az adott részvény kockázatosságára építve, melyben figyelemmel kell lenni, hogy a tőzsdén nem jegyzett vállalat magasabb kockázattal működik a tőzsdén működő ugyanolyan vagy hasonló vállalathoz képest [238], valamint a tőkeáttétel meglétére és mértékére [239]. A faktormodellek olyan statisztikai modellek, amelyek a tőkeköltség alakulását több tényező figyelembevételével magyarázza a CAPM egyváltozós modelljével szemben, amelyek például piaci anomáliák vagy makroökonómiai tényezőkre reagálnak. Neves faktormodell Fama-Franch 3 faktor modellje [240], Carhart 4 faktor modellje [241], Pastor-Stambaugh 5 faktor modellje [242] és Fama-French 5 faktoros modellje [243]. A kormányzati projektekkel összefüggésben a kamatlábak meghatározására két számítási modell áll rendelkezésre, ezek a társadalmi időpreferencia (social rate of time preference – SRTP) [244] és a társadalmi lehetőségköltség (social opportunity cost of capital – SOC) [245], [246], [247].

3.1 A kiberbiztonság tervezésének elméleti kerete

Egy adott szervezetnek az adatkezelői és adatfeldolgozói minőségében kezelt adatok, a vállalati működés, valamint számos lehetséges hatás vizsgálata alapján a kockázatokkal arányos módon szükséges kiválasztania és optimalizálnia a preventív és reaktív képességeket. Ennek

megvalósításában segít a határbevétel és a határköltség mikroökonómiai fogalmak biztonsági beruházásokra vetített alkalmazása [248]. Egy szervezet ugyanis akkor költi el optimálisan a biztonsági büdzsét, amikor a vonatkozó határbevétel és határköltség megegyezik (***9***. ábra). Ez a pont reprezentálja az optimális biztonsági szintet, amelyet az ábrán S^* jelöl [249, p. 9]. Az S^* optimális biztonsági szint meghatározása a szervezet által kezelt (adat)vagyon, a jogszabályi környezet, a fenyegetettségek és a kiberbiztonsági incidensek a szervezetre, társadalomra gyakorolt hatása és a társadalmi reakciók változása miatt összetett, valószínűségeken alapuló, nehéz feladat.



9. ábra. Az információbiztonság költség-haszon elemzése
Forrás: Saját szerkesztés [249, p. 9] alapján

A kiberbiztonság tervezése a külső jogszabályi követelmények (1. fejezet) teljesítése mellett a fenyegetettség (2. fejezet) és az üzleti vagy ügymenetre gyakorolt hatások alapján meghatározott kockázatokra épül. A kiberbiztonsági, kibervédelmi képességekre vonatkozó egyenszilárdság megteremtését célzó jogalkotói szándék ellenére a NIS irányelv [78] és a nyomdokaiba lépő NIS 2 irányelv [91] sem határoz meg szabályokat a hatásvizsgálatra vonatkozóan, meghagyva ezt a feladatot a tagállamok számára. A vizsgálandó hatásokat Magyarországon jelenleg még a NIS irányelv tagállami implementációját megvalósító Ibtv. [52] hatálya alá tartozó szervezetek számára az Ibtv. vhr. [117] definiálja a biztonsági osztályonkénti bontásban. Az 5. táblázat e szempontokat kategorizálja a követelmények jellege (sorok) és a hatás kárvallottjai (oszlopok) szerint.

A három vizsgálati szint (magánszemély, szervezet, nemzet) megkülönböztetését támasztja alá, hogy az IKT szolgáltatásoktól való függőség következtében a kiterjedt adatkezelés és a kritikus infrastruktúrák nem csak az adott szervezetre, hanem magánszemélyekre és magára a nemzet működésére is hatással lehetnek [BZs10], [BZs11] [250], [251], melyek elemzése során kvalitatív és kvantitatív szempontokat szükséges figyelembe venni. A kvalitatív szempontokat az indokolja, hogy bár a gazdasági hatások megkerülhetetlen jelentőséggel bírnak egy-egy incidens bekövetkeztekor, azonban a kvantitatív alapú kockázatértékelés az emberi életre vagy épp a nemzetbiztonságra gyakorolt hatásokat nem veszi figyelembe. A 1.3 fejezetben említett németországi és bolgár

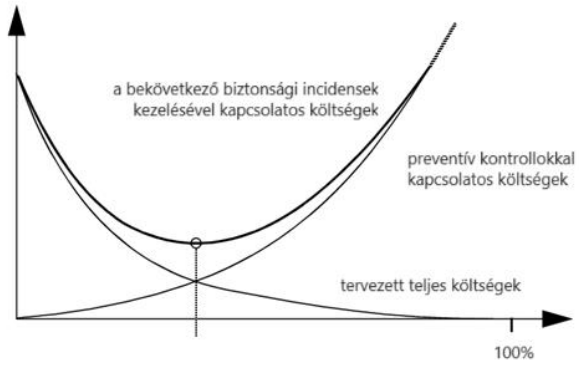
közszférába tartozó feleket ért incidensek is alátámasztják mindezt, hiszen nemzetbiztonsági, állampolgári és uniós adatok is illetéktelen kezekbe kerültek. Ezzel kapcsolatban [BZs12] további példákat tartalmaz, rámutatva arra az összefüggésre, hogy az egészségügyi, energetikai vagy épp a közlekedési szektor esetén az adott vállalatot ért pénzügyi hatás eltörpül az ügyfeleiket ért hatások mellett.

5. táblázat. Hatásvizsgálati szempontok

		Természetes személy	Érintett szervezet	Nemzet
Kvalitatív	**Adat**	személyes adat	üzlet- vagy ügymenet szempontjából	nemzeti adatvagyon
	IKT		kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer	az ország és a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer
	Egyéb	emberi élet		lehetséges társadalmi-politikai hatás
Kvantitatív	**Pénzügyi**		közvetlen és közvetett anyagi kár aránya a szervezet költségvetéséhez képest	

Forrás: Saját szerkesztés [52] felhasználásával

A továbbiakban a kvantitatív, egészen pontosan a pénzügyi hatások vizsgálatát tárgyalom [BZs11], [BZs13] alapján. Olovsson a biztonsággal kapcsolatos tervezett teljes költséget a preventív kontrollokkal kapcsolatos költségekre, valamint a bekövetkező biztonsági incidensek kezelésével kapcsolatos költségekre bontja fel [252], [253]. Mindezt a 10. ábra szemlélteti, ahol a függőleges tengely a költségeket, míg a vízszintes tengely a biztonság szintjét reprezentálja.



10. ábra. Az információbiztonság költség elemzése
Forrás: Saját szerkesztés [252, p. 6] alapján

Az optimális biztonsági szint meghatározása, melyet a 9. ábrán az *S** reprezentál, a jövőre vonatkozó pénzügyi hatások becslése, az arra vonatkozó időbeliség kezelése és a fenyegetésre vonatkozó

bekövetkezési valószínűség meghatározása miatt nem egyszerű feladat. Ugyanakkor az olyan módszerek, mint a pénzügyi kockázatszámításból a kiberbiztonság területére származtatott kockáztatott érték (value at risk – VAR) számítás e bonyolult feladatot hivatottak támogatni. A VAR a normális körülmények között, adott szignifikanciaszinten, adott időhorizonton vett maximális várható veszteséget hivatott meghatározni [254], [255].

A VAR fontos bemenete a kockázatarányos tervezés eredményeképp előálló várható pénzáramok. A várható éves veszteség (annualised loss expectancy – ALE) módszertan e várható pénzáramok meghatározását hivatott támogatni [256]. Az ALE az adott biztonsági szint mellett az egyszeri várható veszteség (single loss expectancy – SLE) és az egy évre vonatkozó előfordulási ráta (annualised rate of occurrence – ARO) szorzata:

$$ALE = SLE * ARO \tag{1}$$

Az ARO az adott kockázat egy éven belüli előfordulásának becsült gyakorisága. Az SLE a biztonsági incidensnek az entitás működésére, adataira és informatikai eszközeire stb. gyakorolt hatásának összesített várható pénzbeli veszteségének összege. Így az SLE elméletben összefoglalja a várható közvetlen és közvetett kárértékeket, amely a vizsgált kockázat bekövetkezéséből fakadó incidens kapcsán előáll. Az SLE értéke az eszköz értékének (asset value – AV) és egy expozíciós tényező (exposure factor – EF) szorzata:

$$SLE = AV * EF \tag{2}$$

ahol SLE az egyszeri várható veszteség, AV az eszköz értéke, EF az expozíciós tényező. Az AV értékének meghatározásakor olyan szempontokat kell figyelembe venni, mint az eszköz (vagy eszközök) beszerzéséért vagy megalkotásáért kifizetett pénzmennyiség, mekkora a reprodukálás költsége, az emberi és gépi erőforrás esetén kieső hasznos munkaidő költsége, elmaradó bevétel, hatósági bírságok. Az EF a kár vagy veszteség százalékos aránya az AV-hoz képest.

Ennek értelmében a várható éves veszteség egy kockázat kapcsán előálló várható értéket adja meg, melyeket összegezve adódik a várható éves összes veszteség ($\sum_{i \in kockázatok} ALE_i$). A várható éves összes veszteség egy adott biztonsági szint mellett képződik, melyet egy (vagy akár több) biztonsági kontrollmix, másként fogalmazva különböző biztonsági megoldások együttese valósít meg. Így a várható veszteség mellett az adott megoldás költségével (solution cost – SC) is számolni szükséges, amely szerint az adott alternatíva megvalósítása mellett az éves költség az ismert kockázatok függvényében a következőképp adódik:

$$\text{Éves költség}^A = \sum_{i \in kockázatok} \left(\overbrace{AV_i^A * EF_i^A * ARO_i^A}^{ALE_i^A} \right) - SC^A \tag{3}$$

ahol $A \in Alternatívák$, ALE a várható éves veszteség, AV az eszköz értéke, EF az expozíciós tényező, ARO egy évre vonatkozó előfordulási ráta, SC a megoldás költsége.

Több éves időtáv elemzése során gyakorta elkövetett hiba az Éves költség egyszerű összegzése, amely a pénz értékének időbelisége miatt hibás eredményre vezet. A nettó jelenérték (NPV) e probléma feloldására kiválóan alkalmas [257]. Az NPV számítása évvégi pénzáramokat feltételezve a következőképpen történik:

$$NPV^A = \sum_{t=1}^{n} \frac{\text{Éves költség}_t^A}{\prod_{i=1}^{t}(1+r_i)} \tag{4}$$

ahol $A \in Alternatívák$, NPV^A az adott alternatíva megvalósítása mellett a vizsgált időszakra vonatkozó teljes költség, Éves költség_t az adott alternatíva megvalósítása mellett az éves költség, r_i az éves tőkeköltség értéke a vizsgált vállalat tőkeösszetételének függvényében. Az NPV egy adott időpontra vetített várható éves pénzáramok összegét adja meg, amely a vállalat eredményeit befolyásolja.

Több lehetséges kontrollmix vizsgálata esetén az alternatívák összehasonlíthatók, amely eredményeképp az optimumot adó legkisebb költséget jelentő A^* alternatíva kiválasztható, alapjául szolgálva a kiberbiztonságra vonatkozó éves költségvetés meghatározásához vagy legalább becsléséhez:

$$\text{Éves költség}^{A^*} \approx -\text{Büdzsé}^{tervezet} \tag{5}$$

Több évre vonatkozó tervezés esetén:

$$\sum_{t=1}^{n} \frac{\text{Éves költség}_t^{A^*}}{\prod_{i=1}^{t}(1+r_i)} \approx \sum_{t=1}^{n} \frac{-\text{Büdzsé}_t^{tervezet}}{\prod_{i=1}^{t}(1+r_i)} \tag{6}$$

A vállalati hatások pontosabb összefüggéseinek (pl. adózásra gyakorolt hatás) vagy egy hosszútávú elemzés esetén az implicit tervezési időszak figyelembevétele során az NPV számításhoz képest precízebb módszer, valamely diszkontált pénzáram módszertan [234] alkalmazása szükséges. Azonban a precíz tervezéshez elengedhetetlen a pénzáramok minél pontosabb meghatározása. Ennek alapvető módja az eredménybeszámoló tételei alapján levezetett várható tényleges és virtuális pénzáramok feltűntetése. (Mindezeket a szükséges eszközök árainak, munkabérek, infláció, árfolyam stb. alakulása is alapvetően befolyásolja.) A 6. táblázat ennek egy egyszerűsített változatát szemlélteti több éves bontásban, szétválasztva az elmaradó bevétel, valamint a felmerülő operatív költségek (operating expenditure – OPEX) és tőkeköltségek (capital expenditure – CAPEX) kategóriákat. Az OPEX kategóriákat tekintve adódhat az eseményre való reagálás többletköltségei, bírságok, kártérítés,

nyilvános kommunikációra, lobbitevékenységre vonatkozó többletköltség. A CAPEX tekintetében az elromlott berendezések értékcsökkenése, valamint a teljes leírása és újbóli beruházás költsége is felmerülhet.

A diszkontált cash flow módszerek a számviteli szabályok szerinti bevétel és kiadás kategóriák alkalmazását követeli meg, így például a biztosítási bevételekből származó pénzáramlások értékelése során figyelemmel kell lenni a követelés természetére. Amennyiben a kártérítés részben az üzleti tevékenység megszakítására, részben pedig az ingatlanokra, gépekre és berendezésekre vonatkozik, a pénzbevételeket fel kell osztani a működési tevékenységből származó pénzáramok (pl. a követelés üzletmegszakítási része) és a befektetési tevékenységekből származó pénzáramok (pl. a követelés tárgyi eszközre vonatkozó részére) közt, valamint kezelni kell a pénzáram adóvonzatainak a kérdéseit is [258].

6. táblázat. NPV alternatíva számítása

	Vizsgált évek			
	$\boldsymbol{t=1}$	$\boldsymbol{t=2}$	**…**	$\boldsymbol{t=n}$
Bevételeket módosító tételek				
OPEX növelő tételek			…	
CAPEX növelő tételek			…	
Az incidens éves pénzárama	$\boldsymbol{CF_1}$	$\boldsymbol{CF_2}$	…	$\boldsymbol{CF_n}$
r	r_1	r_2	…	r_n
$\boldsymbol{NPV}$				

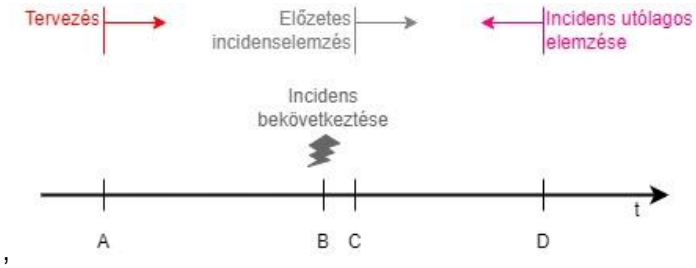
Forrás: Saját szerkesztés

3.2 A nem tervezett incidensek hatásainak elemzési kerete

Egyes esetekben előállhat az az állapot, amikor egy negatív pénzáramot reprezentáló I incidens nagyobb mértékű negatív hatást gyakorol az előzetes tervezéshez képest, vagy éppenséggel az incidens bekövetkezésével egyáltalán nem is számolt az adott szervezet a költségvetés kalkulálása során. Feltételezésem szerint bár az adott incidens a vizsgált szervezet működésében következett be, de a vele kapcsolatban lévő más szervezetekre, az államra és a nemzetközi pénzügyekre is hatással lehet a jelenlegi globalizált működési környezetben. A következő alfejezetek mindezekre vonatkozóan a vizsgálati keretet tárgyalják.

Egy incidens vonatkozásában kétféle elemzés is azonosítható, melyhez négy időpontot, $A < B < C < D$, kell megkülönböztetni, ahogy 11. ábra szemlélteti. Az A időpontban bekövetkező incidens előzetes elemzése, azaz tulajdonképp a pénzáramok becslése az incidens B időpontban történő bekövetkezésétől számítva Δt idő elteltével az C időpontban valósul meg, feltételezve, hogy $]B, C[$

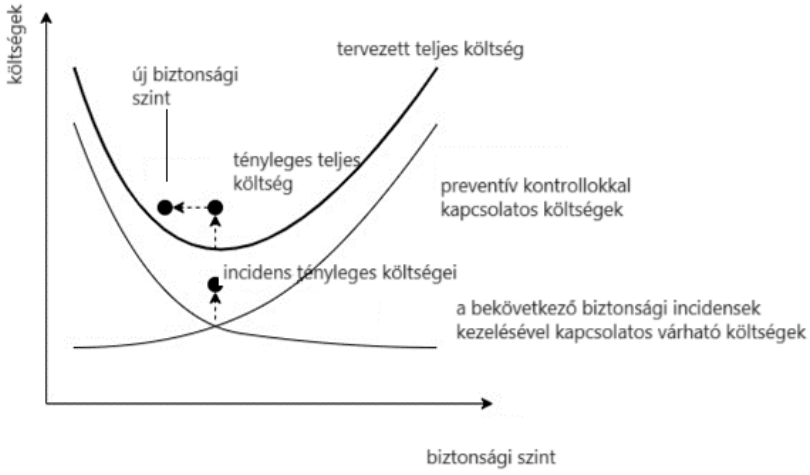
intervallumon az incidens kapcsán nem keletkezett pénzáram. Az incidens teljes értékű utólagos elemzése az D időpontban lehetséges. A $]C, D[$ intervallumon az előzetes elemzés a hátralévő várható pénzáramot, míg az utólagos elemzés az addig felmerült pénzáramok jelenértékét adja meg, ennélfogva ezek összege alkotja az incidens (várható) teljes hatását. (Mindez azt jelenti, hogy A időpontot megelőzően kockázatelemzésről és a büdzsé tervezéséről beszélhetünk.) A továbbiakban feltételezem, hogy az C időpont és az D időpont között több év is eltelhet.



11. ábra. A tervezés és az elemzés időtengelye
Forrás: Saját szerkesztés

3.2.1 Szervezetre és tulajdonosaira gyakorolt hatások

Az érintett szervezetet ért hatásmechanizmus vizsgálatához felhasználva a 10. ábra jelöléseit, a 12. ábra által szemléltetett összefüggések állapíthatók meg. A nem tervezett vagy a hatás szempontjából alultervezett biztonsági incidens költsége magasabb a bekövetkező biztonsági incidens kezelési költségekhez képest, ennélfogva a tényleges teljes költség is magasabb a megállapított biztonsági büdzséhez képest. Ráadásul az incidens magával vonhatja a teljes rendszer biztonsági szintjének rövid vagy akár hosszabb távú csökkenését is [BZs13].



12. ábra. A bekövetkezett incidensek hatása a költségekre
Forrás: Saját szerkesztés [252, p. 6] felhasználásával

A C időpontban kivitelezett előzetes incidenselemzés egy több évre kiterjedő I incidens hatásának megállapítása az NPV alapján évvégi pénzáramokat feltételezve a következőképp adódik:

$$NPV^I = \sum_{t=1}^{n} \frac{I_t}{(1+r)^t} \tag{7}$$

ahol I a vizsgált incidens, I_t az I incidenssel összefüggésben várható éves pénzáramok, azaz veszteségek, C nulladik időpont az incidens bekövetkezésének időpontja (ekkor még nem keletkezett pénzáram az incidenssel kapcsolatban). Míg az I incidens több évre kiterjedőn kifejtett hatására vonatkozó D időpontban történő utólagos elemzés egyenletét az NFV formulából származtatom, melyhez szintén az évvégi pénzáramok megadását feltételezem:

$$NFV^I = \sum_{t=0}^{n-1} \left(I_t * \prod_{i=t}^{n} (1 + r_{i+1}) \right) + I_n \tag{8}$$

Az incidensek utólagos elemzése lehetőséget biztosít a tervezett költségvetés és az incidens hatásaival növelt tényleges költségvetés összehasonlítására, amely egy év időtáv vizsgálata esetén adódik az alábbi egyszerű formula:

$$B\ddot{u}dzs\acute{e}^{t\acute{e}nyleges} = B\ddot{u}dzs\acute{e}^{tervezet} + |I| \tag{9}$$

Az $Incidens\ hat\acute{a}sa$ mérőszámot egy év vonatkozásában az I incidens által kifejtett negatív pénzáram abszolútértékének és a $B\ddot{u}dzs\acute{e}^{tervezet}$ százalékos formában megadott hányadosaként határozom meg:

$$Incidens\ hat\acute{a}sa = \frac{|I|}{B\ddot{u}dzs\acute{e}^{tervezet}} [\%] \tag{10}$$

Az $Incidens\ hat\acute{a}sa$ megadja, hogy az adott incidens hány százalékkal módosította a költségvetéstervezetet. Amennyiben a vizsgált időszak során több incidens is hatással volt a tervezett költségvetésre, úgy a vizsgált incidensek hatásait vizsgáló $Incidensek\ hat\acute{a}sa$ mérőszám meghatározásához a hatások pénzáramainak abszolútértékét összegezni szükséges:

$$Incidensek\ hat\acute{a}sa = \frac{\sum_{i \in vizsg\acute{a}lt\ incidensek} |I_i|}{B\ddot{u}dzs\acute{e}^{tervezet}} [\%] \tag{11}$$

Azonban a több évre kiterjedő vizsgálat esetén el kell kerülni, hogy a két összehasonlított érték eltérő időpontra legyen diszkontálva és eltérő időintervallumot öleljenek fel. Másként fogalmazva az előzetes költségvetés és az utólagos tényleges költségvetés vizsgálata ugyanazt az időintervallumot vizsgálja, a pénzáramaikat pediglen ugyanarra az időpontra, ugyanazzal a kamatlábbal kell diszkontálni.

Így több évre vonatkozó elemzés esetén az NFV számítást kell alapul venni. Az egy incidens hatását vizsgáló $Incidens\ hat\acute{a}sa^*$ mérőszám a következőképp adódik:

$$Incidens\ hatása^* = \frac{NFV^I}{NFV^{Büdzsé^{tervezet}}} = \frac{\sum_{t=1}^{n-1}(I_t * \prod_{i=t}^{n}(1+r_{i+1})) + I_n}{\sum_{t=1}^{n-1}\left(\ Büdzsé_t^{\ tervezet} * \prod_{i=t}^{n}(1+r_{i+1})\right) +\ Büdzsé_n^{\ tervezet}}\,[\%] \quad (12)$$

A több incidens több évet felölelő módon vizsgáló $Incidensek\ hatása^*$ mérőszám esetén az incidensekre vonatkozó NFV értékek összege teszi ki a számlálót:

$$Incidensek\ hatása^* = \frac{\sum_{i \in vizsgált\ incidensek} |NFV^{I_i}|}{NFV^{Büdzsé^{tervezet}}}\,[\%] \quad (13)$$

A fenti képletekkel a vállalati (A) és tulajdonosi (E) értékekben bekövetkező változások vizsgálata egyaránt lehetséges. A vállalati érték meghatározásához az I_A vállalati pénzáramok, illetve a tőkeszerkezet függvényében a tőkeáttétel nélküli tőkeköltség (r_A) vagy a tőkeáttételes tőkeköltség (r_{wacc}) alkalmazása szükséges. A tulajdonosi értékben bekövetkező változások vizsgálata az incidensekhez köthető I_E tulajdonosi pénzáramok és az r_E tőkeköltség alkalmazását igényli.

A tulajdonosi pénzáramok megítélése az emberek elfogultságaiból, a viselkedési heurisztikákból fakadóan összetettebb folyamat. Az emberek gondolkodásmódja gyakorta nem a tudatosan átgondolt következtetésekre épít, hanem felhasználva az emberi agy korlátait és egyszerűsítésre való hajlamát, a korábban tanultak és tapasztaltak alapján egyszerűsít. Ez a tény a gyors és lassú gondolkodásból ered [47], amely a mindennapok része, ugyanúgy kihat a vállalatok biztonságára, mint a befektetői viselkedésre. Az emberi agy a gyors gondolkodási képességet használja fel az olyan gondolkodási heurisztikák kialakítására, mint keretezés, komplex problémák kezelése, negatív hatások észlelése, elérhetőségi heurisztika, vékony szeletelés és a kis döntések zsarnokságának alkalmazására [46]. Mindezek mellett, ahogy Matthew Rabin [259] rámutat, a részvényesek túlnyomórészt kerülik is a veszteségek realizálását.

A tanulási és szocializációs folyamat során az emberi agy tapasztalatokon alapuló koncepciókat és elméleti perspektívákat hoz létre, amelyek intenzíven szűkítik az észlelést, keretet adva, manipulálva a valóság észlelését, feldolgozását és kommunikációját. A legtöbb ember szívesebben szerzi meg a személyes tapasztalataikon alapuló információkat, ugyanakkor a különböző információforrások pontos kombinálása nehéz feladatnak mutatkozik. Ennek eredményeként mindenki hajlamos az egyszerűsítésre, ami bizonyos mértékig segíthet, másfelől téves döntéseket is okozhat [48]. Tversky és Kahneman [46] úgy találta, hogy az egyidejű döntésekből fakadó komplex problémák esetén többnyire nem sikerül a helyes következtetést megalkotni. Azt is megállapították, hogy az emberek által a döntéseik során alkalmazott értékfüggvények általában S-alakúak, amely a semleges értéket reprezentáló referenciapont felett a pozitív értékeket konkáv függvény, a referenciapont alatt lévő negatív értékeket pedig konvex függvény írják le. Ez azt jelenti, hogy az értékek megítélésekor az

emberek felerősítik a negatív hatásokat, miközben csökkentik a pozitív hatásokat. Az elérhetőségi heurisztika [260] szerint az emberek hajlamosak arra, hogy döntéseiket a frissebb információk felé mérlegeljék. Másrészt az erre alapú döntés lehetőséget ad a gyors reakcióra. A vékony szeletelés [261] a minták megtalálásának és a gyors következtetések levonásának képessége minimális rendelkezésre álló információmennyiség esetén. Bár elősegíti a döntéshozatalt, de az előzetes tudás, a tudatosság és a hasonló események tapasztalatai nélkül gyakorta rossz döntéseket eredményez. Ahogy Barry Schwartz saját fordításban megfogalmazta a könyvében [262] Fred Hirsch „Kis döntések zsarnoksága" című könyvével kapcsolatban, a lehetőségek széles skálája csökkentheti a kiválasztott alternatíva vonzerejét, mert a nem választott opciók vonzereje, az azokban történő elmerengés csökkenti a választott alternatíva által okozott örömöt. További általános probléma, ahogy Barabási Albert László könyvében [49] kifejti, az egyéni döntéseket a nyájhatás is alapjaiban képes befolyásolni, amely elősegítheti a rossz döntések terjedését.

Mindezek alapján a nyilvánosan működő részvénytársaságok esetén feltételezhető a tulajdonosi értékben és a részvényárfolyamban bekövetkező változások közötti különbség legalább átmeneti jellegű kialakulása. Az incidensekre vonatkozóan az alábbi képlet az $Incidensek\ érzékelési\ eltérése$ mérőszámot definiálja, mely összehasonlítja az incidensekből fakadóan rövidtávon előálló részvényárfolyam változást (I_P) és a tulajdonosi érték változását (I_E):

$$Incidensek\ érzékelési\ eltérése^* = \frac{NFV^{I_P}}{NFV^{I_E}} = \frac{\sum_{t=1}^{n-1}\left(I_{P,t} * \prod_{i=t}^{n}\left(1 + r_{E,i+1}\right)\right) + I_{P,n}}{\sum_{t=1}^{n-1}\left(I_{E,t} * \prod_{i=t}^{n}\left(1 + r_{E,i+1}\right)\right) + I_{E,n}}\,[\%] \quad (14)$$

3.2.2 A vállalat működési környezetét ért hatások

Tekintettel arra, hogy a vállalatok nem buborékban, egymástól elkülönülten működnek, egy vállalatot ért kiberbiztonsági incidens az üzleti kapcsolatokon keresztül tovagyűrűzhet. Ez a hatásmechanizmus végül az államkasszát közvetlen módon is elérheti. A 7. táblázat az incidensben közvetlenül érintett vállalat perspektívájából a vele kapcsolatban álló jellemző entitásokra vonatkozóan vezeti végig a bevételek, a működési költségek és a tőkeköltség nyilvánvaló és lehetséges módosulásait, ahol a vizsgált entitás a Beszállítók, Vásárlók, Versenytársak, Biztosítók, Hitelezők csoportjai, valamint az Állam. Multinacionális vállalat esetén vagy az érintett vállalat nemzetközi kapcsolatinak következtében több állami entitás is érintett lehet.

7. táblázat. Egy incidens lehetséges pénzügyi hatásai az érintett vállalat és környezete számára

	Érintett szervezet	Beszállítók	Vásárlók	Versenytársak	Biztosítók	Hitelezők	Állam(ok)
Bevételek							
Elmaradt új értékesítések	-	(-)	(-)	(-/+)			-
Korábbi megrendelések lemondása	-	(-)	(-)	(-/+)			-
Biztosításból befolyó összeg	+				-		
Működési költségek (OPEX)							
Az incidenselhárítás következtében felmerülő extra költségek	-	(-/+)					(-/+)
Az utólagos vizsgálatok többletköltségei	-	(-/+)					(-/+)
Bírság	-	(-)					+
Kártalanítások	-	(-)	+				
Extra PR költségek	-	(-/+)					+
Drágább hitelfinanszírozás	-					+	
Elromlott berendezés javítása	-	-/+					+
Működési eszköz cseréje	-	-/+					+
Tőkeköltségek (CAPEX)							
Lemondott beruházás	-/+	(-)	(-)	(+)			-
Beruházási eszköz cseréje	-	(-/+)	(-)	(-/+)			+
Eszköz megsemmisülése	-						

Forrás: Saját szerkesztés

Magyarázat: - negatív következmény, + pozitív következmény, (-) lehetséges negatív következmény, (+) lehetséges pozitív következmény, (-/+) negatív vagy pozitív következmény is lehetséges

A táblázatban foglaltakra a következő gondolatsor ad magyarázatot. Az érintett szervezetet érintő elmaradt új értékesítések és korábbi megrendelések lemondása negatívan érinti az államot az elmaradó adóbevétel miatt, negatívan érintheti a beszállítókat kevesebb beszállítói megrendelés formájában és a vásárlókat a nem teljesített megrendelésből fakadó önnön kötelezettségeik nemteljesítése miatt. Ugyanakkor a versenytársakat pozitív hatás érheti a vásárlók átpártolása következtében, illetve negatív hatás az iparágra vonatkozóan kialakuló bizalomvesztésből fakadó csökkenő megrendelések miatt. Amennyiben az érintett szervezet rendelkezik kiberbiztonsági incidensre vonatkozó biztosítással, úgy a biztosításból befolyó összeg a negatív hatások csökkentésére hivatott, amely a biztosítók részéről kiadást jelent.

Amennyiben egy beszállító érintett az incidenselhárításban, az utólagos vizsgálatokban vagy az incidens miatt előálló PR tevékenységben, úgy a tevékenység számára negatív vagy pozitív

pénzáramot is jelenthet annak függvényében, hogy a saját költségek terhére vagy az érintett szervezet által finanszírozva végzi a feladatokat. Ezzel szemben, ha a bírság kifizetésében vagy a kártalanításban is érintett, úgy az számára egyértelműen negatív pénzáramot jelenthet. Az elromlott berendezés javítása vagy egy működési eszköz cseréje a szerződés függvényében negatív vagy pozitív pénzáramként jelenik meg számára. Az állam számára az incidenselhárításban és annak utólagos kivizsgálásában való feltételes szerep többletköltséget jelent. Másrészről a tevékenységekkel kapcsolatosan az érintett fél által esetlegesen kifizetett további tételek az állam számára adó formájában többletbevételt jelentenek.

Az értett szervezet által lemondott beruházás a szervezet számára érdekes módon jelenthet negatív és pozitív következményt is. Az előbbi a beruházásból elmaradó extra hatékonyságnövelésből, extra kapacitásból adódó további jövedelemből fakad, az utóbbi eshetőség pedig akkor áll fenn, ha a beruházás eredetileg is egy felesleges kiadás lett volna a szervezet részéről. A lemondott beruházás negatívan hathat a beszállítókra az elmaradó megrendelés miatt, a vevőkre az igényeik elmaradó teljesítéséből fakadóan, melyet a versenytársak akár ki is használhatnak a vevők elcsábítására. A beruházási eszköz meghibásodásából fakadó eszközcsere annyiban különbözik a lemondott beruházás esetétől, hogy a beszállítók számára az esetleges új megrendelés pozitív pénzáramot is jelenthet megrendelés formájában, továbbá a lemondott beruházás az állami bevétel elmaradását, míg a beruházási eszköz cseréje az állami bevételek növelését vonhatják magukkal. Végül egy eszköz megsemmisülése önmagában az érintett szervezet számára hordoz negatív hatást – amennyiben emiatt az érintett szervezet nem tudja teljesíteni az ügyféligényeket, úgy az elmaradó bevételek esetén felmerülő hatásmechanizmus lép életbe.

Ennek értelmében az érintett szervezetet ért kiberbiztonsági incidens a szervezet működési környezetében tovagyűrűző hatásmechanizmusban negatív és pozitív pénzáram formájában is megjelenik. E hatások összességére vonatkozóan a 11. ábra jelöléseit felhasználva a B időpontban előálló incidensre vonatkozó C időpontban végzett előzetes elemzés a következőképp adódik:

$$NPV_{Sum}^{I} = \sum_{E} NPV_{E}^{I} | \left(\forall E \in (érintett\ entitások) \wedge (I\ az\ adott\ incidens) \right) \qquad (15)$$

Míg a D időpontban végzett utólagos elemzés alapját az NFV számítás adja:

$$NFV_{Sum}^{I} = \sum_{E} NFV_{E}^{I} | \left(\forall E \in (érintett\ entitások) \wedge (I\ az\ adott\ incidens) \right) \qquad (16)$$

Az elemzés nagy kérdése, ahogy a 7. táblázat is mutatja, hogy kiket tekintünk az $érintett\ entitások$ halmaz részének, továbbá a pénzáramokat egy-egy $érintett\ entitás$ kapcsán külön is vizsgálhatjuk.

3.2.3 Kibertámadási kampányok mikroökonómiai hatása

Egy kibertámadási kampány során egy fenyegető tényező egy és ugyanazon tevékenysége generál incidenst több érintett szervezet működésében. Az előzőekhez hasonlatosan az érintett szervezeket ért kiberbiztonsági incidens a szervezetek működési környezetében tovagyűrűző hatásmechanizmusban negatív és pozitív pénzáram is megjelenik. E hatások összességére vonatkozóan a 11. ábra jelöléseit felhasználva a B időpontban előálló incidensre vonatkozó C időpontban végzett előzetes elemzés az egy szervezet környezetére vonatkozó hatások összessége:

$$NPV_{Sum}^{Kampány} = \sum_{E} NPV_{Sum}^{I} | \forall E \in (\text{közvetlenül érintett entitások}) \tag{17}$$

Hasonlóképp a D időpontban végzett utólagos elemzés:

$$NFV_{Sum}^{Kampány} = \sum_{E} NFV_{Sum}^{I} | \forall E \in (\text{közvetlenül érintett entitások}) \tag{18}$$

E megközelítés nem zárja ki, hogy egy-egy szervezet a kampányban közevetlenül érintett félként és egy másik szervezet működési környezetében is megjelenjen, valamint annak eshetőségét, hogy egy szervezet a kampányban közvetlenül érintett két vagy több szervezet működési környezetében is érdekelt legyen. E tekintetben azzal a feltételezéssel élek, hogy a különböző érintettségekből fakadó pénzáramok elkülöníthetők egymástól, így a számítás redundanciamentes. A módszer alkalmas egy botnet vagy egy fenyegető tényező tevékenységeinek összességére vonatkozó pénzáramok jelenértékének vagy jövőértékének vizsgálatára.

3.2.4 Makrogazdasági és nemzetközi pénzügyi hatások

Egy incidens hatással van a gazdasági szereplők pénzügyi és reálvagyoni helyezére, amely az incidensből fakadó tranzakciók, átértékelődések (pl. részvényárfolyam), valamint egyéb állományváltozások (pl. egyoldalú leírás) formájában a makrogazdasági mutatókban is megmutatkozik. Ráadásul egy adott incidens a nemzetközi gazdasági kapcsolatok tekintetében a belföld szempontjából ki- és beáramló pénzforgalomra (folyó fizetési mérlegre), valamint a nemzetközi befektetési pozícióra is hatással lehet [263]. A makrogazdasági statisztikai elszámolásokat összefüggéseket a nemzeti számlák rendszere (System of National Accounts – SNA) [264], illetve az Európai Unióban az azzal összhangban álló nemzeti számlák európai rendszere (European System of Accounts – ESA) (ESA 2010) [265], [266] szabályozza, melyet a 2. függelék részletesen tárgyal.

A makrogazdasági hatásokat a bruttó hazai termékre (gross domestic product – GDP) és a reálvagyonra, a folyó fizetési mérlegre, a nemzetközi befektetési pozícióra és a nemzeti vagyonra gyakorolt hatások alapján vizsgálom. A GDP és a folyó fizetési mérleg tranzakció szemléletű, míg a reálvagyon (azaz a reáleszközökben meglévő vagyon), a nemzeti vagyon és a nemzetközi befektetési

pozíció mérleg szemléletű, azaz két időpont közötti időszakra vonatkozóan a nettó vagyonváltozást vizsgálja, magában foglalva a tranzakciókat, átértékelődéseket és egyéb állományváltozásokat.

Az alábbiakban a korábban a számviteli szemlélet szerint meghatározott, a bevételt, működési költségeket és tőkeköltségeket befolyásoló vállalati események (7. táblázat) makroszintű és nemzetközi pénzügyikre gyakorolt hatásokat határozom meg. A hatások szemléltetésében két eshetőséget különböztetek meg: (1) az érintett szervezet belföldi és a tranzakcióban résztvevő fél is belföldi (rezidens – rezidens), (2) az érintett szervezet belföldi, de a tranzakcióban résztvevő másik fél külföldi illetékességű (rezidens – nem rezidens), illetve elmaradt tranzakció esetén olyan illetékességű lett volna. A bevételeket befolyásoló tranzakciók közül az elmaradt új értékesítések és a korábbi megrendelések lemondása, valamint a lemondott beruházás vizsgálata során két alesetet kell megkülönböztetni annak függvényében, hogy az eszköz vagy tőkejószág (az elmaradt értékesítés mellett) már előállításra került-e vagy sem. Továbbá az Eszköz megsemmisülése eseményt elkülönülten kell kezelni, tekintettel arra, hogy az nem tranzakciónak minősül.

A 8. táblázat a rezidensek közötti tranzakciók makrogazdasági mutatókra gyakorolt hatását foglalja össze. Az elmaradt új értékesítések és a korábbi megrendelések lemondása ellenére, amennyiben az adott tétel már létrehozásra került, a GDP, a reálvagyon és a nemzeti vagyon mutatókra az esemény növelő hatással bír, miközben az eszközöket a vállalat kénytelen készleten tartani. A lemondott beruházás esetében a saját vagy rezidens által végzett részteljesítés pozitívan hat a GDP és a nemzeti vagyon alakulására. Amennyiben az eszközök és tőkejószágok még nem kerültek létrehozásra, úgy az esemény az adott állapotot nem befolyásolja, feltételezve, hogy új eszköz, tőkejószág vagy szolgáltatás előállításának nem volt importvonzata. Importvonzat esetén a GDP és a nemzeti vagyon mutatókat az import értéke is befolyásolja, a reálvagyon növekedése mellett a folyó fizetési mérleg és a befektetési pozíció a külföld felé tartozás irányába mozdulnak el.

A biztosításból befolyó összeg, valamint a bírság és a kártalanítás a másodlagos jövedelem számlához tartozóan nem befolyásolja a GDP alakulását. A drágább hitelfinanszírozást az elsődleges jövedelemszámla tartalmazza, nincs hatással a GDP-re. Az incidenselhárítás következtében felmerülő extra költségek, az utólagos vizsgálatok többletköltségei és az extra PR költségek rezidensek közötti tranzakció esetén GDP és nemzeti vagyon növelő hatással vannak, míg a reálvagyont nem befolyásolják. Az elromlott berendezés javítása, a működési eszköz cseréje (feltéve, hogy az incidens nélkül nem lett volna az adott eszköz legyártva) és a beruházási eszköz cseréje (feltételezve a teljes megsemmisülést) rezidens-rezidens viszony esetében GDP növelő hatással bír, ugyanakkor a reálvagyon és a nemzeti vagyon alakulása a korábbi állapot és a jelenlegi állapotban képviselt eszközök értékeitől függ.

8. táblázat. Egy incidens makrogazdasági mutatókra gyakorolt hatásai – rezidensek közötti tranzakciók vizsgálata

Vizsgált hatás	GDP	Reálvagyon	Folyó fizetési mérleg	Befektetési pozíció	Nemzeti vagyon
Bevételek					
Elmaradt új értékesítések (nincs még létrehozva az eszköz)	➡	➡			➡
Elmaradt új értékesítések (eszköz már készleten)	↗	↗			↗
Elmaradt új értékesítések (eszköz már készleten) – IMPORT	?	↗	↘	↘	?
Korábbi megrendelések lemondása (nincs még létrehozva az eszköz)	➡	➡			➡
Korábbi megrendelések lemondása (eszköz már készleten)	↗	↗			↗
Korábbi megrendelések lemondása (eszköz már készleten) – IMPORT	?	↗	↘	↘	?
Biztosításból befolyó összeg					
Működési költségek (O/PEX)					
Az incidenselhárítás következtében felmerülő extra költségek	↗				↗
Az utólagos vizsgálatok többletköltségei	↗				↗
Bírság					
Kártalanítások					
Extra PR költségek	↗				↗
Drágább hitelfinanszírozás					
Elromlott berendezés javítása	↗	?			?
Működési eszköz cseréje	↗	?			?
Tőkeköltségek (CAPEX)					
Lemondott beruházás (a tőkejószág még nem került létrehozásra)	➡	➡			➡
Lemondott beruházás (a tőkejószág legalább részben létrehozásra került)	↗	↗			↗
Lemondott beruházás (a tőkejószág legalább részben létrehozásra került) – IMPORT	?	↗	↘	↘	?
Beruházási eszköz cseréje	↗	?			?

Forrás: Saját szerkesztés

Jelölés a vizsgálatok kapcsán az adott esetre vonatkozóan:

↗	Kedvező befolyás
↘	Kedvezőtlen befolyás
➡	Nincs befolyásoló hatás
?	Nem megállapítható befolyás

	Tranzakcióalapú mutató
	Mérlegalapú mutató

A rezidens, mint az incidensben érintett vállalat, valamint egy nem rezidens között fennálló vagy tervezett, de elmaradt tranzakcióalapú eseményeket a 9. táblázat foglalja össze. Az események vizsgálata során a rezidens vállalat esetén belföldi tulajdonosokat feltételezek. Az elmaradt új értékesítések és a korábbi megrendelések lemondása nincs hatással a vizsgált mutatókra, amennyiben az adott eszköz legalább részben nem került létrehozásra és feltéve, hogy az eseményhez nem kapcsolódott előlegfizetés és/vagy az előállításnak nem volt importvonzata. Importvonzat esetén a GDP és a nemzeti vagyon mutatókat az import értéke is befolyásolja, a reálvagyon növekedése mellett a folyó fizetési mérleg és a befektetési pozíció a külföld felé tartozás irányába mozdulnak el.

A lemondott tőkeberuházás nincs hatással a vizsgált mutatókra. Részbeni teljesítés esetén az eseményhez kapcsolódó importvonzat miatt a reálvagyon feltehető növekedése, valamint a folyó fizetési mérleg és a befektetési pozíció mutatók által jelzett külföldi tartozás mértékének növekedése mellett a GDP és a nemzeti vagyon mértéke az import értékétől és az előállított eszköz értékétől függ.

A biztosításból befolyó összeg, valamint a bírság és a kártalanítás a másodlagos jövedelem számlához tartozóan nem befolyásolja a GDP alakulását, ugyanakkor az események a nem rezidens érintettsége miatt a folyó fizetési mérleg, a befektetési pozíció és a nemzeti vagyon mutatókat a bevétel esetén pozitív, míg a költségek esetén negatívan befolyásolja. A drágább hitelfinanszírozás a GDP kivételével az összes vizsgált mutató értékét csökkenti. Az incidenselhárítás következtében felmerülő extra költségek, az utólagos vizsgálatok többletköltségei és az extra PR költségek események során a tranzakció az összes vizsgált mutatót értékét csökkenti.

Az elromlott berendezés javítása, a működési eszköz cseréje (feltéve, hogy az incidens nélkül nem lett volna az adott eszköz legyártva) és a beruházási eszköz cseréje (feltételezve a teljes megsemmisülést) a fennálló importvonzat miatt a folyó fizetési mérleg és a befektetési pozíció mutatókra negatív hatással van, azonban a GDP, a reálvagyon és a nemzeti vagyon mutatók alakulása a régi és az új eszköz értékelésének függvényében alakul.

9. táblázat. Egy incidens makrogazdasági mutatókra gyakorolt hatásai – rezidens és nem rezidens közötti tranzakciók vizsgálata

Vizsgált hatás	**GDP**	**Reálvagyon**	**Folyó fizetési mérleg**	**Befektetési pozíció**	**Nemzeti vagyon**
Bevételek					
Elmaradt új értékesítések (nincs még létrehozva az eszköz)	➡	➡	➡	➡	➡
Elmaradt új értékesítések (eszköz már készleten)	↗	↗	➡	➡	↗

Elmaradt új értékesítések (eszköz már készleten) – IMPORT	?	↗	↘	↘	?
Korábbi megrendelések lemondása (nincs még létrehozva az eszköz)	→	→	→	→	→
Korábbi megrendelések lemondása (eszköz már készleten)	↗	↗	→	→	↗
Korábbi megrendelések lemondása (eszköz már készleten) – IMPORT	?	↗	↘	↘	↗
Biztosításból befolyó összeg			↗	↗	↗
Működési költségek (OPEX)					
Az incidenselhárítás következtében felmerülő extra költségek	↘	↘	↘	↘	↘
Az utólagos vizsgálatok többletköltségei	↘	↘	↘	↘	↘
Bírság		↘	↘	↘	↘
Kártalanítások		↘	↘	↘	↘
Extra PR költségek	↘	↘	↘	↘	↘
Drágább hitelfinanszírozás			↘	↘	↘
Elromlott berendezés javítása – IMPORT	?	?	↘	↘	?
Működési eszköz cseréje – IMPORT	?	?	↘	↘	?
Tőkeköltségek (CAPEX)					
Lemondott beruházás (a tőkejószág még nem került létrehozásra)	→	→	→	→	→
Lemondott beruházás (a tőkejószág legalább részben létrehozásra került) – IMPORT	?	↗	↘	↘	?
Beruházási eszköz cseréje	?	?	↘	↘	?

Forrás: Saját szerkesztés

Jelölés a vizsgálatok kapcsán az adott esetre vonatkozóan:

↗	Kedvező befolyás
↘	Kedvezőtlen befolyás
→	Nincs befolyásoló hatás
?	Nem megállapítható befolyás

	Tranzakcióalapú mutató
	Mérlegalapú mutató

A 10. táblázat az Eszköz megsemmisülése eseményt elkülönülten tartalmazza, tekintettel arra, hogy a vizsgált eset a többi esettől eltérően nem tranzakcióalapú esemény. Az incidens közvetlenül az incidensben érintett vállalat reálvagyonára hat, abban sem rezidens, sem nem rezidens másik fél nem vesz részt, ennek értelmében az esemény egyéb volumenváltozást von maga után a nemzeti vagyonban, illetve egy nem rezidens finanszírozó fél esetén annak pénzügyi követeléseit befolyásolhatja.

10. táblázat. Egy incidens makrogazdasági mutatókra gyakorolt hatásai – eszköz megsemmisülése

Vizsgált hatás	GDP	Reálvagyon	Folyó fizetési mérleg	Befektetési pozíció	Nemzeti vagyon
Tőkeköltségek (CAPEX)					
Eszköz megsemmisülése		↘		↘	↘

Forrás: Saját szerkesztés

Jelölés a vizsgálatok kapcsán az adott esetre vonatkozóan:

↘ Kedvezőtlen befolyás

Tranzakcióalapú mutató

Mérlegalapú mutató

A vásárlóerő-paritáselméletet alapul véve a fizetési mérleg befolyásolja a nominális és reálárfolyamokat a valuták keresleti és kínálati erői révén [267]. Egyrészt a fizetési mérleg hiánya egybeesik a devizakínálattal szembeni devizakereslet-többletével. A keresleti nyomás a deviza árfolyamának felértékelődését és a hazai valuta devizához viszonyított árfolyamának leértékelődését eredményezi. Másrészt a fizetési mérleg többlete a devizakínálat többletét jelenti, ami a deviza leértékelődését, egyben a hazai valuta felértékelődését okozza. A fizetési mérleg és az árfolyam közötti összefüggés azonban nem egyértelmű, és az időtávlat is befolyásolja.

3.3 Incidensek elemzése esettanulmányok alapján

A 3.2 fejezetben ismertetett metodológiát öt különböző esetet vizsgálva alkalmazom vállalattulajdonosokra, a vállalat működésére, vállalat működési környezetére és a makrogazdasági hatásokra fókuszálva. Az esetek tárgyalása során a vizsgálat tárgyát a rendelkezésre álló adatok köre határozza meg, melyet szükség szerint az incidensleírás alapján meglévő vagy feltételezhető kvantitatív, másodsorban kvalitatív jellegű információval egészítem ki.

Az incidensek kiválasztása szubjektív módon valósult meg, a 1. fejezettel összefüggésben a NIS irányelvben és NIS 2 irányelvben meghatározott szektorok, az IT ellátási lánc és a közösségi média lefedését célozva történt, figyelembe véve az elemzésekhez szükséges adatok lehetőség szerinti rendelkezésre állását, valamint [BZs11], [BZs12], [BZs13] elemzéseket alapul véve. A lehetséges forrásokat nem korlátoztam be uniós entitásokra, hiszen a pénzügyi hatások általános jellegére keresem a választ, amely a globalizált világban javarészt függetleníthető a lokalizációtól.

Vizsgálom a Tesco Bank 2016-ban, a SolarWinds 2020-ban bekövetkezett egyedi incidenseit, a két kibertámadási kampányként viselkedő WannaCry és NotPetya ransomware támadás esetében több közvetlen érintett felet. Végül a Meta (Facebook) szolgáltatásokat 2014-2020 között ért incidensek

kapcsán részletesen elemzem a befektetői viselkedést is. Minden esettanulmány egy rövid esetleírásból és elemzés részből tevődik össze.

3.3.1 Tesco Bank incidens

2016. november 6-án brit újságok, köztük a BBC [268], arról számoltak be, hogy a Tesco PLC részeként az Egyesült Királyságban lakossági banki és biztosítási szolgáltatásokat nyújtó Tesco Bankot olyan kibertámadás érte, amelyben az ügyfelek számláiról eltérő nagyságú pénzösszegek tűntek el. Másnap a bank felfüggesztette az online tranzakciókat, és közölte, hogy akár 40 000 ügyfelet is érinthetett az incidens [269]. A bank lakossági csoport részvényei 3 százalékot estek a hírre, de a veszteség a nap közepére 1,1 százalékra csökkent [270]. Valójában 8 261 ügyfél folyószámlája kompromittálódott. A támadók megszerezték az ügyfelek betéti kártyaadatait, és több ezer jogosulatlan tranzakciót hajtottak végre, összesen 2,26 millió fontot (2,5 millió dollárt) eltulajdonítva a bankszámlákról. Továbbá a többi ügyfél az online banki felület elérhetetlensége miatt nem tudta elérni és kezelni a pénzeszközeit [271], amelyből másodlagos hatásként likviditási problémák és nem teljesített kötelezettségek származtak. A Tesco Bank ígéretet tett arra, hogy tíz napon belül új kártyákat bocsát ki az érintett ügyfelek számára. Két évvel később, 2018. október 1-jén a Pénzügyi Felügyelet (Financial Conduct Authority – FCA) [272] 16,4 millió GBP (körülbelül 21,4 millió USD) pénzbírságot szabott ki a Tesco Bankra a kibertámadás miatt.

A Tesco Bankot ért incidens a bank működési környezetére mért ismert és vélt hatását a 11. táblázat tartalmazza. A 12. táblázat a Tesco Bank az incidens kapcsán előálló ismert pénzáramainak 2018-ra vetített összértékére vonatkozó kalkulációt ismerteti.

11. táblázat. Az incidens valós és lehetséges hatásai (Tesco Bank)

	Tesco Bank	**8 261 ügyfél**	**A többi ügyfél**	**Egyesült Királyság**
OPEX				
Az incidenselhárítás következtében felmerülő extra költségek	Ismeretlen (beleértve az új kártyák kiadásának költségeit)	Átmeneti likviditási probléma	Nem elérhető webbank felület	
Az utólagos vizsgálatok többletköltségei	Feltételezhető			Feltételezhető
Bírság	-21,4$ (2018)			+21,4$ (2018)
Kártalanítások	-2,5$ (2016)	+2,5$ (2016)		

Forrás: Saját szerkesztés

12. táblázat. Az incidens a Tesco Bank vállalati költségeinek összértéke (millió)

	2016	2017	2018
OPEX	-2,5$		-21,4$
Az incidens éves pénzárama	**-2,5001$**		**-21,4023$**
r_{wacc}[a]	3,86%	3,94%	4,29%
$\boldsymbol{NFV^{I,2018}}$	**-24,1011$**		

Forrás: Saját szerkesztés
Magyarázat:
[a] [273] Europe, Banks (Regional) értékek alapján becsülve

3.3.2 SolarWinds incidens

2020-ban a SolarWinds rendszereit ért fejlett támadást fedeztek fel, amely az Orion IT hálózatkezelő eszközén keresztül komolyan érintette ügyfeleit [274]. A támadó fél valójában 2019 szeptemberében jogosulatlanul hozzáfértek a SolarWinds hálózathoz [275]. 2019 októberében tesztelték a kódinjektálás folyamatát a SolarWinds Orion szoftverének kódbázisába, míg a Sunburst rosszindulatú kódot 2020. február 20-án integrálták az Orionba. A SolarWinds Orion 2019.4 és 2020.2.1 HF1 közötti verziói kompromittálódtak a támadás következtében. Az első verzió, amely a kártékony kódbázist is tartalmazta, az ügyfelek számára 2020. március 26-án vált elérhetővé. Ebben az időben a SolarWinds 33 000 Orion-ügyfele volt szerte a világon, közülük körülbelül 18 000 ügyfél telepítette a rosszindulatú frissítéseket [276].

Az Egyesült Államokban az érintettek közé tartoztak (1) olyan állami szervek, mint a Pentagon, a Belbiztonsági Minisztérium (Department of Homeland Security), a Külügyminisztérium (State Department), az Energiaügyi Minisztérium (Department of Energy), a Nemzeti Nukleáris Biztonsági Igazgatóság (National Nuclear Security Administration) és az Egyesült Államok Pénzügyminisztériuma (Treasury of the United States), (2) olyan magánvállalkozások, mint a FireEye, a Microsoft, a Cisco, az Intel, az Nvidia és a VMware, valamint a Deloitte, és (3) más szervezetek, például a Kaliforniai Állami Kórházak Minisztériuma (California Department of State Hospitals) és a Kent Állami Egyetem (Kent State University) [277]. Az ismert információk alapján a 18 000 érintett ügyfélből 2021. január 12-ig körülbelül 40 vállalatot céloztak meg a támadók a kompromittált Orion telepítéseken keresztül. A BitSight adatai szerint az azonosított áldozatok 80 százaléka az Egyesült Államokban található, a fennmaradó 20 százalék pedig hét másik országra szóródik szét, köztük Kanada, Mexikó, Belgium, Spanyolország, az Egyesült Királyság, Izrael és az Egyesült Arab Emírségek [278]. Lehetséges azonban, hogy világszerte ismeretlen entitások, köztük az uniós OES és DSP szolgáltatók is közvetetten érintettek voltak a támadásban.

A SolarWinds pénzügyi jelentései szerint a vállalat az incidens kapcsán csak 2020 decemberében 3,5 millió dollárt költött [279], további 40 millió dollárt 2021 első kilenc hónapjában a vállalat negyedéves

jelentése [280] szerint, amelyből várakozás szerint 15 millió dollár visszanyerhető a kiberbiztonsági biztosítás alapján. A SolarWinds IKT rendszereit ért kibertámadás a vállalat működési környezetére mért ismert pénzügyi hatásait a 13. táblázat tartalmazza, amely kiegészül mind az érintett vállalat és az ügyfelek tekintetében a csökkent biztonsági szinttel és az állami szereplők érintettsége következtében a nemzetbiztonsági kockázattal, mely az USA esetében kiemelkedő mértékű volt tekintettel arra, hogy az azonosított áldozatok 80 százaléka az Egyesült Államokban volt. 2021 januárban végzett szakértői elemzések [281] szerint az érintett vállalatok és állami ügynökségek számára az incidens kezelése $NPV_{Sum}^{I,USA} > 100\ milliárd\ \$$. (Az utólagos elemzés megvalósulására nem találtam információt.)

A 14. táblázat a SolarWinds az incidens kapcsán előálló ismert pénzáramainak 2021-re vetített összértékére vonatkozó kalkulációt ismerteti.

13. táblázat. Az incidens valós és lehetséges hatásai (SolarWinds)

	SolarWinds	**Ügyfelek**	**USA**
OPEX			
Az incidenselhárítás következtében felmerülő extra költségek	-3,5 millió $ (2020) -40 millió $ (2021)	Feltételezhető	Feltételezhető
Az utólagos vizsgálatok többletköltségei			

Forrás: Saját szerkesztés

14. táblázat. Az incidens a SolarWinds vállalati költségeinek összértéke (millió)

	2020	**2021**
OPEX	-3,5$[a]	-40$[b]
Az incidens éves pénzárama	**-3,5$**	**-40,0062$**
r_{wacc}[c]	9,7%	6,15%
$\boldsymbol{NFV^{I,2021}}$	**-43,8457 $**	

Forrás: Saját szerkesztés

Magyarázat:

[a] A pénzáram az év végén került rögzítésre

[b] A pénzáram a harmadik negyedév végén került rögzítésre

[c] [273] US, Software (System & Application) értékek alapján becsülve

3.3.3 WannaCry ransomware támadás

2017-ben a WannaCry ransomware számos szektorban tevékenykedő áldozatot szedett, az Egyesült Államok Nemzetbiztonsági Ügynökségtől (National Security Agency – NSA) kiszivárgott az EternalBlue exploit felhasználásával, titkosítva a Windows-eszközök merevlemezein lévő fájlokat [282]. A támadók a fájlok visszaállításáért 300 és 600 dollár közötti váltságdíjat követelt bitcoinban. Az áldozatok azonban csak egy része kapott visszafejtési kulcsot, hiába fizetett érte. Az első támadás 2017. májusban történt, és a becslések szerint több mint 200 000 eszközt ért el mintegy 150 ország vonatkozásában [283],

beleértve a bristoli repülőtér, a Deutsche Bahn, valamint az angol és skót Nemzeti Egészségügyi Szolgálat (National Health Services – NHS) rendszereit. A mintegy 150 országra kiterjedő és 200 ezer eszközt érintő kampány a Symantec (amely immáron a Broadcom része) becslése szerint $NPV_{Sum}^{Kampány} = 4\ milliárd\ \$$, míg más szakértők szerint $NPV_{Sum}^{Kampány} = 8\ milliárd\ \$$ értékre tehető [284]. A számos érintett közül a továbbiakban a bristoli repülőtér, a Deutsche Bahn, valamint az NHS esetét tárgyalom.

A bristoli repülőtér utas információs rendszerét érintette az incidens. A két napos leállás alatt az utasok tájékoztatása az induló járatokról és a használatos kapukról papíralapú jegyzeteken történt, amely kisebb fennfordulást okozott a működésben. Ugyanakkor a ransomware nem érintette a repülőtér többi rendszerét, köztük a kritikus rendszereket sem. A reptér részéről az incidenselhárítás kapcsán extra költségek merülhettek fel, az utasok pedig némi kellemetlenséggel szembesültek [284].

Ezzel szemben a WannaCry a hétvégi forgalom közepette nem csak az utastájékoztató rendszereket érintette az incidens a mintegy négyszázhetven pályaudvaron több órán keresztül a Deutsche Bahn esetében, hanem a jegyautomaták sem működtek. A beszámolók szerint a vasúti közlekedési rendszereket nem érte behatás. Így a Deutsche Bahn működését ért hatáshoz a jegyautomaták kiesése által okozott bevételkisesés is hozzáadódik, amely az elmaradt jegyvásárlásokhoz mérten az állami adóbevételt is csökkentette [284].

Az angol és skót Nemzeti Egészségügyi Szolgálat (National Health Services – NHS) 2017. május 12-én délután már hivatalosan közzétette a WannaCry fertőzés tényét, amely számos kórházban napokig elérhetetlenné tette az IKT rendszereket. Ennek eredményként tervezett műtéteket kellett halasztani, továbbá mintegy 13 500 rendelést töröltek, köztük legalább 139 potenciális rákos beteg esetén, valamint sürgősségi ellátást igénylő betegeket kellet átirányítani az incidensben nem érintett kórházakba [285]. Összesen öt kórház sürgősségi osztályát kellett bezárni, hat százalékkal csökkentve a betegellátás kapacitását. A támadás pénzügyi hatását a kórházak működése kapcsán $NPV_{Sum}^{Kampány|NHS} = 5{,}9\ \text{millió}\ £$ értékre becsülték [286], mindamellett emberi életek kerültek veszélybe.

3.3.4 NotPetya ransomware támadás

A NotPetya kampány [287] 2017. június 27-én, az ukrán alkotmány ünneplése előtti napon indult. Az első fertőzések az Intellect Service MEDoc alkalmazás szoftverfrissítési mechanizmusán keresztül történtek, amely egy hivatalosan jóváhagyott, ukrán cégeket kiszolgáló adóbevallási program volt. A kártevő jellemzői hasonlóságot mutattak a jól ismert Petya zsarolóvírussal, de mindez egy álcázás volt, melyből a rosszindulatú kód NotPetya elnevezése is származik. Ukrajnában cégek ezrei estek áldozatul, köztük olyan kritikus infrastruktúrák, mint a Kijevi Boriszpol Repülőtér, bankok, valamint

energiavállalatok, például a Kyivenergo és az Ukrenergo. Járulékos kárként azonban számos további entitás is érintett volt, amelyek központja más országban, köztük Németországban, Franciaországban, Olaszországban, Lengyelországban, Dániában és az Egyesült Államokban található [318].

Az ukrán kiberbűnözés elleni egység meglehetős késedelemmel, mindössze 2017. július 4-én foglalta le az Intellect Service szervereit, és azt tanácsolta a MEDoc felhasználóknak, hogy hagyják abba a szoftver használatát. Az Intellect Service vállalat vezetését büntetőjogi felelősségre vonták a támadást elősegítő, hanyag módon karbantartott vállalati informatikai infrastruktúrája miatt. Az incidens elemzése során egyértelmű jel mutatkozott a kibertámadás orosz eredetére [288]. Az első becslések szerint a NotPetya által okozott károk várható összértéke $4\ milliárd\ \$ < NPV_{Sum}^{Kampány} < 8\ milliárd\ \$$, míg más szakértők szerint $NPV_{Sum}^{Kampány} > 10\ milliárd\ \$$ összegre tehető [289]. A NotPetya által okozott károk következményeként 2018 februárban Ausztrália, Észtország, Dánia, Litvánia, Ukrajna, az Egyesült Királyság és az Egyesült Államok közösen nyilatkozatot adott ki, amelyben a kezdeti kibertámadást és a kampányszerű hatását hivatalosan Oroszországnak és az orosz hadseregnek tulajdonítják. A nyilatkozatot Új-Zéland, Norvégia, Lettország, Svédország és Finnország is hivatalosan támogatta [287, p. 489]. A továbbiakban a dán Maersk és az egyesült államokbeli Merck esetét tárgyalom.

A Maersk, mint vezető hajózási vállalat, az ukrajnai Odessza városában is üzemeltetett irodát, ahol a kibertámadásban a közvetítő szerepet betöltő MEDoc könyvelőprogramot használták [289]. A fertőzés hamar túllépett az iroda virtuális határain, mely eredményeként 7 perc alatt átterjedt az egész vállalati IKT rendszerre, működésképtelenné téve 49 000 laptopot, 6 200 szerverből 3 500 szervert, a teljes nyomtatási képesség, fájlmegosztás és Enterprise Service Bus szolgáltatás megsemmisült, továbbá a DHCP (Dynamic Host Configuration Protocol) és az Active Directory rendszerek is súlyosan megsérültek, a vCenter felhőszolgáltatásokat kezelő rendszerek instabillá váltak, és mind az 1 200 alkalmazás elérhetetlenné vált, amelyekből körülbelül 1 000 alkalmazás meg is semmisült. Bár az adatokat a biztonsági mentés megőrizte, az alkalmazásokat nem lehetett visszaállítani a biztonsági másolatból, mivel azonnal újonnan megfertőződtek volna. A Deloitte segítségével sikerült a rosszindulatú program működési módját megismerni. Azonban több napba telt, mire 2 000 laptopot és az Active Directory szolgáltatást újjáépítették a szakemberek, mely lehetővé tette az alapvető üzleti folyamatok és rendszerek visszaállításának megkezdését. Két hét elteltével az összes globális alkalmazást visszaállították, négy hét múlva pedig az összes laptopot újratelepítették [290], [291].

Az incidens a Maersk működését épp csökkenő tendenciát mutató jövedelmezőség mellett érte, ami miatt a vállalat már a tevékenységei konszolidálására szánta rá magát, így a ransomware támadás épp egy vállalati transzformáció során történt. A számítások szerint az incidens elhárítása, elemzése, a visszaállítás, az elmaradt bevételt stb. együttesen 300-350 millió $ kárt okozott, hozzájárulva a 2017.

évi -1,9 milliárd $ működési veszteséghez. Továbbá egy év alatt a piaci kapitalizáció 27 százalékot csökkent [290], minthogy egyre több ügyfél a Maersk versenytársai szolgáltatását vette igénybe (15. táblázat). Mindez feltételezhetően negatívan befolyásolta a dán GDP adatokat és a nemzetközi számlát.

15. táblázat. Az incidens valós és lehetséges hatásai (Maersk)

	Maersk	**Ügyfelek**	**Versenytársak**	**Dánia**
OPEX	-300-350 millió $ (2017)	Feltételezhető	Bevétel növekedése feltételezhető	Feltételezhető

Forrás: Saját szerkesztés

A Merck gyógyszeripari óriáscég IKT rendszerei hasonlóképp az ukrajnai irodáján keresztül fertőződtek meg. Az incidens 30 000 számítógépet érintett, és fennakadást okozott a gyártási, a kutatási és az értékesítési tevékenységekben [292]. A Merck első nyilatkozata még arról szólt, hogy képes fenntartani a legkeresettebb és életmentő gyógyszereinek folyamatos ellátását, másfelől figyelmeztetett más termékekre vonatkozó szállítások átmeneti csúszására [293]. Ugyanakkor az egyik vakcinagyár leállását követően a vállalat kilenc adag Gardasil oltóanyagot kölcsönzött az Egyesült Államok stratégiai készletéből, hogy teljesítse megrendelését [292].

A Merck, az éves jelentése [294] szerint, még 2017-ben valóban nem tudta maradéktalanul az egyes termékekre vonatkozó megrendeléseket teljesíteni az általa lefedett összes piacon, amely -260 millió $ hatást gyakorolt a forgalomra, valamint -286 millió $ értékben károkat okozva az értékesítési, általános és adminisztratív költségek, valamint kutatási és fejlesztési költségek formájában. Az incidens még 2018-ban is éreztette a hatását, körülbelül -150 millió dollárral csökkentve az értékesítést.

2017-ben megközelítőleg 45 millió $ kártalanítási összeget kapott a vállalat. Bár a Merck nagyságrenddel nagyobb pénzügyi károkat szenvedett az incidens miatt, a biztosító szerint a NotPetya háborús cselekménynek minősül, ami a biztosítás esetén vis major eseménynek minősül [292]. Válaszreakcióként a Merck beperelte a biztosítót, mert véleménye szerint az 1,75 milliárd $ értékű biztosítási szerződése a szóban forgó kiberbiztonsági incidensre is vonatkozik. 2021. december 6-án a New Jersey-i Legfelsőbb Bíróság részleges gyorsítéletet hozott a Merck javára, és kijelentette, hogy a háborús vagy ellenséges cselekmények kizárása nem alkalmazható [295], így az 1,4 milliárd dollár kártalanítási összeghez a Merck némileg közelebb került.

A Merck IKT rendszereit ért kibertámadás a vállalat működési környezetére mért ismert és vélt hatását a 16. táblázat tartalmazza. Ezen túlmenően az incidensnek tulajdonítható az ellátási lánc végén a készlethiány és nem teljesített új értékesítésekből fakadó esetleges ellátatlan betegek globális szinten. Továbbá az új értékesítések elmaradása az USA GDP mutatójára, valamint az elmaradt export miatt a folyó fizetési mérlegre is kedvezőtlen hatással volt. A 17. táblázat a két nettó jövőbeni értéket határoz

meg: 2018-ra datálható az utolsó publikusan ismert tényleges pénzáram, másrészt a biztosítási díjra vonatkozó várakozás kapcsán az utolsó publikus információ 2021 év végén vált ismertté. Ez utóbbi a bizonytalan tétel miatt nem tartalmazza a biztosítás díját.

16. táblázat. Az incidens valós és lehetséges hatásai (Merck)

	Merck	**Ügyfelek**	**Biztosító**	**USA**
Bevétel				
Elmaradt új értékesítések	-260 millió $ (2017) -150 millió $ (2018)	Elmaradt disztribútori bevétel		Elmaradt adóbevétel
OPEX				
Értékesítési, általános és adminisztratív költségek, valamint kutatási és fejlesztési költségek	-285 millió $ (2017)	Elmaradt disztribútori bevétel		Elmaradt adóbevétel
Biztosítás	+1,4 milliárd $ (?)		-1,4 milliárd $ (?)	

Forrás: Saját szerkesztés

17. táblázat. Az incidens a Merck vállalati költségeinek összértéke (millió)

	2017	**2018**	**2019**	**2020**	**2021**
Bevétel	45$[a]				
OPEX	-545$[a]	-150$[a]			
Az incidens éves pénzárama	**-500$**	**-150$**			
r_{wacc}[b]	8,13%	10,49%	8,51%	4,75%	5,63%
$\boldsymbol{NFV^{I,2018}}$	**-763,0992$**				
$\boldsymbol{NFV^{I,2021}}$	**-916,2037$**				

Forrás: Saját szerkesztés

Magyarázat:

[a] A pénzáram az év végén került rögzítésre

[b] [273] által biztosított US, Software (System & Application) adatok alapján becsülve

3.3.5 Meta (Facebook) szolgáltatásokat ért incidensek

2014-ig a Cambridge Analytica Facebook felhasználói profilokat gyűjtött be nem etikus és nem is legális módon. Az első híresztelések szerint az incidens mintegy 50 millió felhasználót érintett [296], azonban későbbi lapértesülések szerint csak az Egyesült Államokban 87 millió fiók adata került illetéktelen kezekbe [297].

2015 évvégén a The Guardian arról számolt be, hogy a Cambridge Analytica segített Ted Cruz elnökválasztási kampányában. A jelentés azt sugallja, hogy a republikánus jelölt több tízmillió Facebook-felhasználót felölelő kutatáson alapuló pszichológiai adatokat használt fel, hogy előnyt szerezzen politikai riválisaival szemben. 2016-ban az amerikai elnökválasztás előtt Trump

kampánycsapata komoly befektetéseket kezdett a Facebook-hirdetésekbe. A lépés a Cambridge Analytica közreműködésével járt, és a cég ügyvezető igazgatója, Mark Turnbull a brit Channel 4 News-nak elmondta, hogy a cég a felelős a Facebookon található videókampányért [298]. Az incidens széleskörű publicitását követően a vállalat részvényárfolyama 2018 március 19-én megközelítőleg 7 százalékot esett, mellyel a piaci értéke több mint 36 milliárd dollárral csökkent [299].

2018. július 26-án a Facebook részvényárfolyama az elmaradó bevételeket ismertető piaci jelentés alapján 19 százalékkal esett vissza. A záró árfolyam $176,26 volt, ami azt jelenti, hogy az előző napi, szerdai piaci kapitalizációhoz képest ($630 milliárd) a csütörtöki kereskedési nap végére $510 milliárd értékre csökkent 170 millió kereskedési volumen mellett. Ez a változás mintegy $120 milliárd értékvesztést jelentett [300].

Ezt követően 2018. szeptember 28-án a vállalat bejelentette, hogy adatlopás következtében felhasználói adatok kerültek illetéktelen kézbe a szolgáltatásban rejlő logikai sérülékenység kihasználásával [301]. A támadó fél mintegy 29 millió Facebook felhasználó személyes adatait lopta el, úgymint születési dátum, telefonszám, keresési előzmények és a legutóbbi bejelentkezés lokalizációja. Továbbá a támadó fél hozzájutott a felhasználói access token-ekhez, így hozzáférést nyerhetett az érintett felhasználók Facebook-fiókjaihoz, illetve további más szolgáltatásokhoz (pl. Tinder, Spotify, Airbnb), amelyhez a felhasználó a Facebook-fiókját regisztrálta. A kibertámadás hírére már a hivatalos bejelentést megelőzően, 2018. szeptember 27-én a részvényárfolyam három százalékkal csökkent [301].

2019. március 18-i kereskedési nap végére a Facebook részvények a negyedik napja tartó csökkenés következtében 7,4 százalékkal alacsonyabban zártak a negatív tendenciát megelőző árfolyamhoz képest [302]. A rossz híreket a vállalat Chris Cox termékvezető és Chris Daniels WhatsApp alelnök távozása, valamint a Needham elemzői leminősítés szolgáltatta. Azonban még március 13-án többórás, minden szolgáltatást érintő szolgáltatáskiesés történt alkalmazáshiba miatt [303].

2019. március 24-én a Facebook egy, az Instagram szolgáltatást érintő biztonsági incidenst jelentett be, amelyet még januárban érzékeltek egy rutin biztonsági ellenőrzés során – belső munkatársak az Instagram felhasználók elmaszkolt jelszavaihoz férhettek hozzá. Az incidenssel összefüggésben a vállalat 2019. április 18-án frissítette a korábbi közleményét, miszerint a jelszavakat nem titkosított módon is eltárolták [304]. 2019. június 12-én, miután napvilágot látott Mark Zuckerberg vezérigazgató levele a „potenciálisan problematikus adatvédelmi gyakorlatokkal" kapcsolatos aggodalmairól, a Facebookrészvények 2,9 százalékkal estek vissza [305].

A Cambridge Analytica botrány és a botrányt okozó adatszivárgás kapcsán 2018. október 24-én az Egyesült Királyság Adatvédelmi Biztos Hivatala (Information Commissioner's Office – ICO) a vállalatot

mindössze £500 000 (kb. $643 000) pénzbírság megfizetésére kötelezte a Cambridge Analytica botrányban játszott szerepéért. (Ekkor még nem volt hatályos a GDPR [99] a maga egy adatvédelmi incidens kapcsán kiszabható €20 millió bírságával.) A Facebook 2018.11.21-én fellebbezett, 2019.06.14-én a Törvényszék közbenső határozatot hozott, amely eredményeként kötelezte az ICO-t a döntéshozatali folyamatához kapcsolódó anyagok nyilvánosságra hozatalára. 2019.09.02-én az ICO fellebbezett az ideiglenes határozat ellen, végül 2019. október 30-án a felek megegyeztek, amely eredményeként a Facebook kifizette a büntetést [306].

Az incidenssel összefüggésben a Szövetségi Kereskedelmi Bizottság (Federal Trade Commission – FTC) az Egyesült Államokban 2019. július 24-én $5 milliárd büntetést szabott ki a vállalatra [307]. Továbbá a vizsgálat eredményeként a SEC további $100 millió büntetést szabott ki a Facebookra [308]. A bírságok, illetve további biztonsági incidensek (pl. 2019 szeptemberben a Techcrunch több nem titkosított, 419 millió rekordot tartalmazó adatbázis miatt történt adatszivárgásról számolt be [309]) ellenére, a Facebook 2019 Q3 eredménye felülmúlta az elemzői és befektetői várakozásokat [310].

2020. május 19-én Kanadában az illetékes hatóság, a Competition Bureau Canada 9 millió CAD büntetést szabott ki a nem megfelelő adatvédelmi gyakorlat következtében, amelyhez az 500 000 CAD eljárási díj is hozzáadódott (együtt kb. 13 221 150 USD) [311]. Bár az uniós adatvédelmi hatóságok többféle témában aktívan felléptek a vállalattal szemben, ugyanakkor a Facebook mindössze Németországban a GDPR 37. cikkének nem teljesítése, azaz adatvédelmi tisztviselő kinevezésének hiánya miatt kapott €51 000 bírságot 2019-ben [312].

Az esetleírás alapján a Meta (Facebook) esetében öt incidenst ($|I| = 5$) azonosítottam az alábbiak szerint (az egyes incidenseket a felső indexben szereplő számozással megkülönböztetve) [BZs13]:

$$I = \left\{ \begin{array}{c} I^1 = Cambridge\ Analytica\ botrány \\ I^2 = Instagram\ sérülékenység\ és\ adatszivárgás \\ I^3 = 419\ millió\ adatrekord\ kiszivárgása \\ I^4 = 50\ millió\ felhasználót\ érintő\ adatlopás \\ I^5 = Minden\ szolgáltatást\ érintő\ alkalmazáskiesés \end{array} \right\}$$

Az egyes incidensekhez kapcsolódó befolyásoló tényezők (18. táblázat) alapján az incidensekhez hozzárendeltem az adott eseményhez tartozó első tőzsdei kereskedési napot. A 2019. június 12-i és 2020. május 19-i események a Meta az általános jelleggel tanúsított biztonsági magatartása miatt következtek be, amely szorosan nem köthető egyik incidenshez sem, ezért a velük összefüggésben felmerülő pénzáramokat az I^1, I^2, I^3 és I^4 események között egyenlő arányban osztom meg (az I^5 incidens bekövetkeztésre ezek az események nem voltak hatással).

18. táblázat. Meta (Facebook) szolgáltatásait érintő incidensekkel összefüggésbe hozható események (2018-2020)

Esemény	Incidens	Dátum	Megjegyzés
A Facebook felfüggeszti a Cambridge Analytics hozzáférését a felhasználói adatokkal való visszaélés miatt	I^1	2018.03.17.	A bejelentés szombaton történt, ennélfogva a befektetők asoron következő (hétfői) kereskedési napon tudják lereagálni az információt.
19 százalékos csökkenés a bevételkiesést leíró piaci jelentés alapján	I^1	2018.07.25.	A bejelentés délután történt, így a befektetői reakció a következő kereskedési napra várható.
A Techcrunch 419 millió rekordot érintő adatszivárgásról számol be	I^3	2018.09.04.	
50 millió felhasználót érintő adatlopás	I^4	2018.09.27.	Az adatlopás felfedézése
	I^4	2018.09.28.	A bejelentést a péntek délelőtti konferenciabeszélgetés keretében ismertették az újságírókkal
Az ICO $643 000 értékű büntetést szab ki a Cambridge Analytica adatszivárgása miatt	I^1	2018.10.24.	
A realizált negyedéves bevétel nem éri el az előzetes elvárást	I^1	2018.10.30.	
A Facebook az elsőfokú bírósághoz fordult az ICO bírsága kapcsán	I^1	2018.11.21.	
Minden szolgáltatást érintő leállás	I^5	2019.03.13.	
	I^5	2019.03.14.	Széles körben ismertté vált a kimaradás ténye
Értesítés üzleti és személyi változásokról		2019.03.18.	Nem az eseményekre vonatkozik, de befolyásolja az elemzést
Instagram adatvédelmi incidens bejelentése	I^2	2019.03.25.	
A vállalat további információkat közöl, amelyek súlyosbítják az adatvédelmi incidenst	I^2	2019.04.18.	
Mark Zuckerberg vezérigazgató levele a „potenciálisan problémás adatvédelmi gyakorlatokkal” kapcsolatos aggályokról	I^1,I^2, I^3,I^4	2019.06.12.	
A Törvényszék közbenső ítéletében kötelezi az ICO-t, hogy hozza nyilvánosságra döntéshozatali anyagát	I^1	2019.06.14.	
Az FTC 5 milliárd dolláros büntetést szab ki a Cambridge Analytica adatszivárogtatásáért	I^1	2019.06.24.	
	I^1	2019.06.25.	Az információ széles körben történő elterjedése

Az ICO fellebbez az ideiglenes határozat ellen	I^1	2019.19.03.	
A Meta (Facebook) kifizeti a büntetést	I^1	2019.10.30.	
A Competition Bureau Canada 9 millió CAD bírságot szabott ki helytelen adatvédelmi gyakorlatok miatt	I^1, I^2, I^3, I^4	2020.05.19.	

Forrás: Saját szerkesztés

A Cambridge Analytica botrány következtében a Meta részvények árfolyama meredeken csökkent a 2018 márciusát követő hónapokban a vállalatot arra kényszerítve, hogy emelje a biztonsági törekvéseit [BZs14]. A vállalati beszámoló [313] szerint 2018 második negyedévében a bevétel 13,73 milliárd dollár volt, amely ugyan elmaradt a kezdeti várakozásoktól -92,44 millió dollár értékben. 2018 harmadik negyedévében a Meta 13,23 milliárd dollár bevételt ért el, ami szintén elmaradt az elemzői várakozásoktól -115,24 millió dollár eltéréssel. Ezek az eltéréseket az incidens nem kívánt hatásaként azonosítom, mint elmaradt bevétel. Mindezek ellenére a Meta mindkét évben nyereséges volt, mivel éves bevétele 2018-ban 55 838 milliárd dollár, 2019-ben 70 697 milliárd dollár volt, míg a teljes működési költsége 2018-ban 30 925 milliárd dollár, 2019-ben pedig 46 711 milliárd dollár volt. Ezen felüli pénzáramokat az esetleírás tartalmazza. Az ennek megfelelő vállalati többletköltségeket rendeli az egyes incidensekhez hozzárendelt módon, megadva az adott pénzáram realizálásának dátumát a 19. táblázat tartalmazza. A táblázat adatait alapján megállapítom, hogy az incidensekkel összefüggésben azonosított események 2018-2020 években zajlottak. Bár az incidensekhez kapcsolódóan az incidens hatását éreztető események 2018-ban kezdődtek, maga az incidens azt megelőzően valósult meg. Az illetéktelen adathozzáférések és adatfelhasználások talán a legjelentősebb a 2016-ban előálló Egyesült Államok elnökválasztással kapcsolatosan felmerülő incidens, ezért a Cambridge Analytica botránnyal összefüggésben az incidensvizsgálathoz a 2016-2020 időszakra vonatkozóan végzem a számításokat.

19. táblázat. Az eseményekhez rendelhető nyilvános vállalati többletköltségek

	I_A^1	I_A^2	I_A^3	I_A^4	I_A^5
2018. július 26.	-92 550 000$				
2018. október 30.	-115 240 000$				
2019. március 13.					-96 845 205,48$
2019. június 24.	-5 100 000 000$				
2019. október 30.	-643 000$				
2020. május 19.	-3 305 288$	-3 305 288$	-3 305 288$	-3 305 288$	

Forrás: Saját szerkesztés

A 18. táblázat a számításokhoz alkalmazott tőkeköltségek kalkulációját és annak eredményét ismerteti, felhasználva a vállalati éves jelentések [313], [314], [315], [316], [317] adatait. A jelentések szerint a

Meta nem dolgozott hosszú lejáratú adóssággal a vizsgált időszakban, azonban a kötelezettségek folyamatosan fennálltak (újratermelődtek), így az r_{wacc} tőkeköltség alkalmazása indokolt.

20. táblázat. Meta vállalati pénzügyi adatok

	2016	**2017**	**2018**	**2019**	**2020**
Éves bevételek és költségek (millió)					
Bevétel[a]	27 638$	40 653$	55 838$	70 697$	85 96$
Teljes költség[a]	-15 211$	-20 450$	-30 925$	-46 711$	-53 294$
Részvények száma (millió)					
Class A[a]	2 354	2 397	2 385	2 407	2 406
Class B[a]	538	509	469	445	443
Összesen	2 892	2 906	2 854	2 852	2 849
Tőke (E), eszköz (A) és hitel (D) értéke (millió)					
A=[a]	64 961$	84 524$	97 334$	133 376$	159 316$
E=[a]	59 194$	74 347$	84 127$	101 054$	128 29$
D=[a]	5 767$	10 177$	13 207$	32 322$	31 026$
Számított éves tőkeköltségek					
r_{wacc}=[b]	0,0473	0,2029	-0,1665	0,2739	0,2237
r_E=[c]	0,0494	0,2259	-0,2000	0,3520	0,2733
r_D=[d]	0,0316	0,0448	0,0538	0,0398	0,0210

Forrás: Saját szerkesztés

Magyarázat:

[a] A vállalati beszámolókban [313], [314], [315], [316], [317] ismertetett adatok szerint

[b] (26) egyenlet alapján

[c] (24) egyenlet alapján, ahol r_f az USA T Bond éves reálhozama [318], r_M az MSCI ACWI Index (USD) [319], $r_{f,nom}$ USA reálkamatból [320] és USA inflációs rátából [321] került kiszámításra, β a Meta részvényárfolyamok [322] S&P500 index [323] alapján került kiszámításra

[d] r_D értékét tökéletes hitelpiacot [324] feltételezve $r_{f,nom}$ értékével becsültem spread felár nélkül

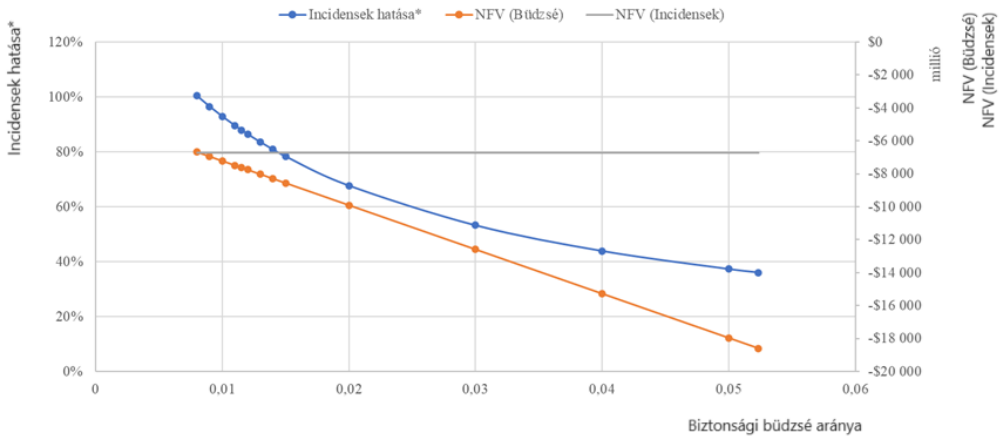
A 21. táblázat a Meta becsült IT biztonsági költségvetését, valamint a büdzsé és az incidensekkel összefüggésben felmerült vállalati pénzáramok 2020-ra vetített nettó jövőértékét, valamint az általuk determinált Incidensek hatása mérőszám értékét tartalmazza. A költségvetés becsléséhez a [325], [326], [327] források felhasználásával az IT büdzsé és IT biztonsági büdzsé százalékos arányok alapján szubjektív módon az IT büdzsé bevételhez képest viszonyított arányát 11,4 százalékban, az IT biztonsági büdzsé az IT büdzséhez képest viszonyított arányát 10,1 százalékban határozom meg. (A becslés jellege miatt a későbbiekben érzékenységi vizsgálatokat hajtok végre.) Ezek az arányok azt eredményezik, hogy az IT biztonsági büdzsé átlagosan a bevételek 1,1514 százalékát teszik ki. Ugyanakkor a Meta vezérigazgatójának nyilatkozata [328] szerint a 2019-es IT biztonsági költségvetés 3,7 milliárd dollár összegben került meghatározásra. A szubjektivitást kompenzálva az elemzés során szükség szerint a projektvizsgálatok során alkalmazott szokványos érzékenységvizsgálat módszerét alkalmazom.

21. táblázat. Az incidensek vállalati nettó jövőbeli értékének és az incidens hatásának kiszámítása

	2016	2017	2018	2019	2020
Incidensekhez kapcsolódó IT biztonsági büdzsé az adott év végén (millió)					
Becsült biztonsági büdzsé	-318,22$	-468,08$	-642,92$	-3 700,00$	-989,80$
Incidensekhez kapcsolódó vállalati változások értéke az adott év végén (millió)					
$\boldsymbol{I^1}$			-207,67$	-5 107,98$	-3,31$
$\boldsymbol{I^2}$					-3,31$
$\boldsymbol{I^3}$					-3,31$
$\boldsymbol{I^4}$					-3,31$
$\boldsymbol{I^5}$				-97,19$	
Elemzés					
			$\boldsymbol{NFV^{\text{Büdzsé},2020}}$		-7 625,22$
			$\boldsymbol{NFV^{I,2020}}$		-6 706,27$
			$Incidensek\ hatása = +87{,}95\%$		

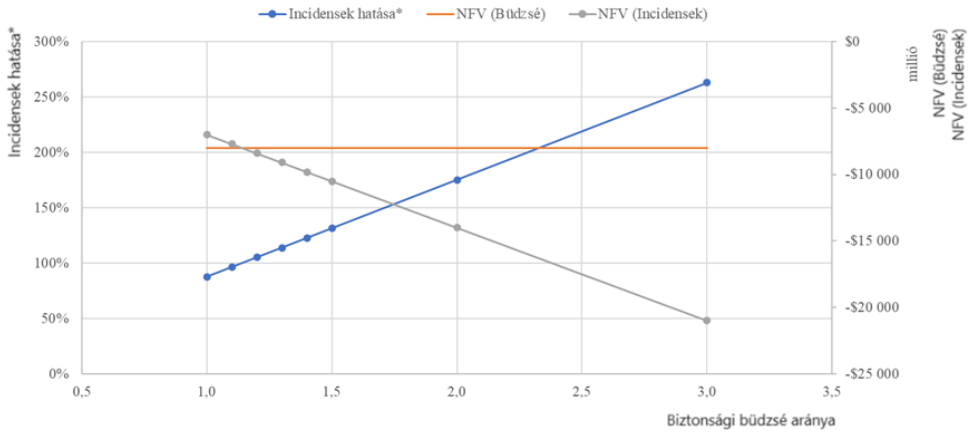
Forrás: Saját szerkesztés

Az incidensekhez rendelt pénzáramok a becsült IT biztonsági büdzsét a számítások szerint 87,95 százalékkal növelték meg. A ***13***. ábra az éves IT büdzsé a bevételhez viszonyított változásának hatását szemlélteti, változatlanul hagyva az incidensek által okozott hatásokat, azaz azt vizsgálja, hogy az NFV (Incidensek) (másként $NFV^{I,2020}$) érték megfelelősségét feltételezve a Biztonsági büdzsé változása (amelyet a Biztonsági büdzsé aránya szabályoz) milyen hatással van az $Incidensek\ hatása^*$ mérőszámra. A biztonsági büdzsé arányának maximumát a 2019-ben a publikusan elérhető információk alapján számított 5,23 százalékban határoztam meg. Minél magasabb az éves költségvetés, annál kisebb az Incidensek hatása.



13. ábra. Az Incidensek hatása* mérőszám érzékenysége az IT biztonsági büdzsére
Forrás: Saját szerkesztés

A ***14***. ábra az incidensek által okozott pénzáramok változásának hatását mutatja az éves IT biztonsági büdzsé összegeit változatlanul hagyva, mely szerint minél magasabbak az incidensek vállalati költségei, annál nagyobb az Incidensek hatása. Az ábra azt vizsgálja, hogy az NFV (Büdzsé) érték megfelelősségét feltételezve az Incidensek által okozott pénzáramok változása (amelyet a Biztonsági incidens multiplikátor szabályoz) milyen hatással van az $Incidensek\ hatása^*$ mérőszámra.



14. ábra. Az Incidensek hatása mérőszám érzékenysége az incidensek pénzáramaira
Forrás: Saját szerkesztés

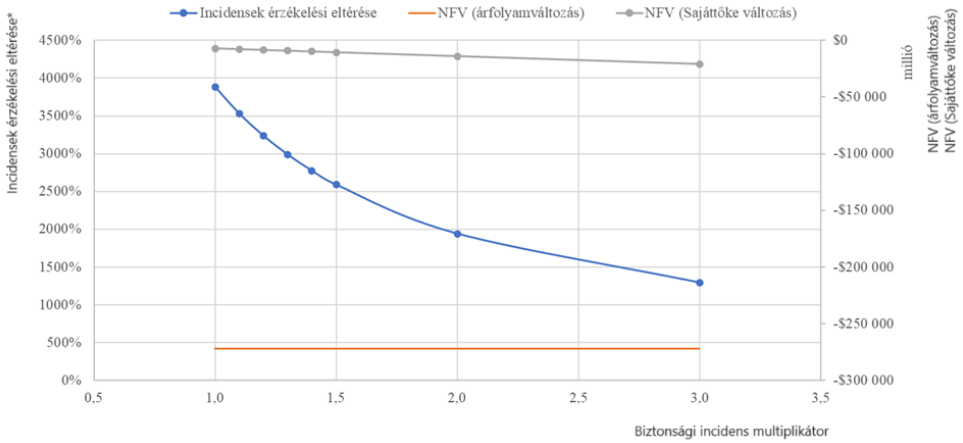
Az Incidensek érzékelési eltérése mérőszám meghatározásához meg szükséges vizsgálni a részvényárfolyamok kapcsán előálló abnormális hozamokat, melyhez az eseményvizsgálat (event study) módszerét [329] alkalmazom a 3. függelékben meghatározott módszertan szerint. Az abnormális hozamok értékét a részvények mennyiségével összeszorozva adódik az abnormális hozamok összértéke. Ennek az adott év végére vetített összegét, valamint a tulajdonosi értékben bekövetkezett változások év végére vetített összértékét a 22. táblázat tartalmazza. Az adatok alapján adódik, hogy az árfolyamok abnormális hozamok alapján azonosított változása a tulajdonosi értékben bekövetkezett tulajdonosi érték ~39-szerese.

22. táblázat. Az incidensek részvényárakra és részvényekre gyakorolt hatásának összehasonlítása

	2016	**2017**	**2018**	**2019**	**2020**
Az eseményekkel összefüggő részvényárfolyam értékváltozásai az adott év végen (millió)					
I^P_{Sum}			-166,90$	12 151,90$	
Incidensekhez kapcsolódó tőkeváltozások értéke az adott év végén (millió)					
I^E_{Sum}			-207 67$	-5 207,12$	-13,24$
Elemzés					
				I^P_{Sum}	I^E_{Sum}
			NFV^{2020}	1 672,81$	-7 001,12$
			$Incidensek\ érzékelési\ eltérése = 3\ 883{,}19\%$		

Forrás: Saját szerkesztés

A ***15***. ábra az Incidensek érzékelési eltérése mérőszám az incidensek hatására vállalat értékeiben bekövetkezett változásokból levezetett tulajdonosi értékekben bekövetkezett változásokra való érzékenységét szemlélteti változatlan abnormális hozam mellett. Az ábra azt vizsgálja, hogy az NFV (Sajáttőke változás) érték megfelelősségét feltételezve az NFV (árfolyamváltozás) módosulása (amelyet a Biztonsági incidens multiplikátor szabályoz) milyen hatással van az $Incidensek\ érzékelési\ eltérése^*$ mérőszámra. Minél magasabb az incidens tulajdonosi értékre vetített hatása, annál kisebb a tulajdonosi érték és az árfolyamok között eltérés mértéke.



15. ábra. Az Incidensek érzékelési eltérése mérőszám érzékenysége az incidensek pénzáramaira
Forrás: Saját szerkesztés

A fejezetben felhasznált részletes adatok és alkalmazott kalkuláció az Open Science Foundation oldalán [BZs15] érhető el.

3.4 Összefoglalás és következtetések

A fejezetben a kiberbiztonság pénzügyi tervezés összefüggéseire alapozva az incidensek ex post elemezésének metodológiáját kialakítva öt esettanulmány részleteit tárgyaltam. Az incidenseket szubjektív módon választottam ki a vállalati, vállalattulajdonosi, a vállalat mikroökonómiai környezetét ért hatások, valamint a makrogazdasági következmények vizsgálatához. Ennek megfelelően a nem tervezett incidensek, illetve a tervezett incidensek nem várt hatásainak vizsgálatához a metodológiát (1) a szervezetre és tulajdonosaira gyakorolt hatások, (2) a vállalat működési környezetét ért hatások, valamint (3) a makrogazdasági és nemzetközi pénzügyi hatások tekintetében alakítottam ki.

Szervezetre gyakorolt hatások elemzéséhez megadtam az $Incidens\ hatása$ és az $Incidensek\ hatása$ mérőszámokat és azok több évre szóló változatait, amelyek megadják, hogy az adott incidens hány százalékkal módosította a költségvetéstervezetet a megadott időintervallumon vizsgálva. A szervezet (kifejezetten a nyilvánosan működő részvénytársaságok esetén) tulajdonosaira gyakorolt hatások vizsgálatához meghatároztam az $Incidensek\ érzékelési\ eltérése$

mérőszámot, amely összehasonlítja az incidensekből fakadóan előálló részvényárfolyam változást és a tulajdonosi érték változását.

A vállalat működésére és működési környezetét ért hatások a (1) bevételeket módosító tételek, (2) az OPEX növelő tételek és (3) a CAPEX növelő tételek kategóriákban különböző eseményeket (szcenáriókat) határoztam meg, amelyek hatását a közvetlenül érintett szervezet működéséből fakadó tipikus üzleti és gazdasági kapcsolatain keresztüli lehetséges hatásokat is vizsgáltam, amelyet a kibertámadási kampányok vizsgáltára is kiterjesztettem.

Az ex post elemzésre való tekintettel a pénzügyi számításokhoz a nettó jövőértéket (NFV) vettem alapul, amely – a nettó jelenértékhez (NPV) hasonlatosan – érzékeny a kamatlábak és a pénzáramok minél pontosabb meghatározására. Előbbi gazdasági vállalatok esetében az adott entitás kockázatosságára figyelemmel a CAPM alapú becslést alkalmaztam. Makrogazdasági és nemzetközi pénzügyi hatásokat a nemzeti számlák európai rendszere (ESA2010) szerint vizsgáltam, amely során a vállalatra gyakorolt hatásokat a makrogazdasági mutatószám rendszerében helyeztem el.

Bár a módszertan végrehajtását a kiválasztott esettanulmányokon több esetben a publikusan elérhető adatok hiánya meggátolta, ugyanakkor a megvalósított részleges vagy teljes értékű elemzések alapján az alábbi következtetéseket vonom le:

1) A Tesco Bank, SolarWinds, Merck, Meta (Facebook) incidensek alapján egy incidens több éven át is kifejtheti a hatását.
2) A Meta (Facebook) incidens alapján egy incidens hatása és az incidens bekövetkezte eltérő naptári és pénzügyi évben is megvalósulhat.
3) Egy incidens a vállalatra, ügyfeleire (beleértve a magánszemélyeket), a vállalat üzleti partnereire, tulajdonosaira, az államra és összességében a makrogazdaság teljesítményére és a nemzetközi pénzügyekre is hatással lehet.
4) A vállalatra és vállalattulajdonosokra gyakorolt hatás részeként egy incidens a vállalat kockázatosságára is hatással lehet. Ezzel összefüggésben sejtésként fogalmazom meg, egy incidens a kockázatosság mértékére gyakorolt hatása a vállalatra jellemző lokáció, iparág, szervezeti méret, a digitalizációtól való függőség mértéke, az érintett adatok függvénye. Ennek megállapítása további kutatást igényel.
5) A részvényesek, mint vállalattulajdonosok, hajlamosak lehetnek a kiberbiztonsági incidensek által okozott hatás mértékét túlreagálni. Ennek megállapítása további kutatást igényel.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A technológiai fejlődés, a digitalizáció mértéke, azaz az IKT szolgáltatások penetrációjából és a különböző ágazatok IKT infrastruktúrától és szolgáltatásoktól való függőségéből fakadón az IKT már nem minősül külön ágazatnak, hanem a modern, innovatív gazdasági rendszerek alapját képezi. A fokozódó társadalmi függőség következtében felmerülő vélt-valós hatások kezelése pedig a kiberbiztonság és kibervédelem erősítését igényli.

A KC1 kutatási céllal összefüggésben az 1. fejezetben áttekintettem a jelentős, Észtországot 2007-ben ért kibertámadási kampány utáni időszakra vonatkozóan az uniós politikai elköteleződés fejlődését, illetve az ennek következtében manifesztálódott jogszabályokat. Az aktuális uniós jogszabályok egyértelműen befolyásolják a szupranacionális és nemzeti kiberbiztonsági és kibervédelmi képességeket, valamint determinálják az érdekelt feleket és azok kötelezettségeit. Ez a meghatározás a NIS 2 irányelv által „kellő mértékben" bonyolult módon valósult meg, alapozva a hatályba tartozás jellegére (az ágazat/alágazat, a szervezet mérete, a kockázati besorolás stb. függvénye) vagy a joghatóság megvalósítására. Továbbá a NIS 2 irányelv megteremti a lehetőséget a tagállamok számára, hogy a gazdasági szempontból fontos szereplőket az irányelv hatálya alá helyezze. Azonban az irányelv nem határozza meg a vizsgálandó gazdasági szempontok jellegét, így a tagállamokra hagyva a módszertan meghatározását (ezzel fokozva a tagállami eltérések mértékét).

A jogalanyok számára a NIS 2 irányelv és további jogszabályok (pl. DORA) tételesen előírják egyes kiberbiztonsági kontrollok kialakítását és fenntartását. A jogszabályok továbbá kijelölik a felügyeleti hatóságot, illetve hatóságokat és meghatározzák a kapcsolódó feladatokat és felügyeleti lehetőségeket, amely a bírságolást is magában foglalja. Mindez azt jelenti, hogy a szervezeti és vállalati szintű szereplők számára jelentős elvárások jelentkeznek.

További nyomást jelent a jogalanyok irányában, hogy a megnövekedett IKT penetráció és függőség a különböző (külső és belső) humán eredetű fenyegető tényezők számára a motiváció függvényében pénzszerzés, információszerzés vagy épp szabotálás végrehajtását jelentheti. Mindemellett a szerkezeti és környezeti fenyegetések is jelentős problémát okozhatnak. Ennek folyományaként, a KC2 kutatási céllal összefüggésben azonosítottam azokat a megközelítéseket, amelyek elősegíthetik a fenyegetések szisztematikus azonosítását és elemzését. Ide soroltam például az általános kockázati kereteket és módszereket (NIST SP 800-39, ISO/IEC 27005), (2) a fenyegetés modellezési keretrendszereket (Attack tree modelling) és az eszközök, taktikák, folyamatok (TTP) alapú modellezéseket (MITRE ATT&CK, MITRE CAPEC). Az elemzés részeként a kibertérbeli műveletekre és képességekre alapozva azonosítottam és analizáltam a kiberfenyegetések, különösképp a humán eredetű fenyegető tényezők jellemzőit, illetve elemeztem a kiberfenyegetésekhez kapcsolódó TTP és IoC információk megosztási lehetőségeit. A rendszerezett információkat felhasználva megalkottam „A

fenyegetések és az érintettek attribútumainak és kapcsolatának modelljét", illetve arra alapozva vizualizáltam „A fenyegetések és az érintettek modellezési lehetőségeit". A modellt felhasználva vizsgáltam a STIX 2.1 képességeivel, amelyet az Európai Unió által támogatott MISP platform is implementál. Megállapítottam, hogy a STIX, valamint a MISP platform szerves részét képezi az incidensekről szóló információk disszeminációja is. Ugyanakkor az incidensek kezelése jelenleg nem a hatósági bejelentésekre vonatkozó elvárások szerint valósul meg. Azonban ahogy a MISP platform a pénzügyi csalásokkal kapcsolatos információk és a terrorizmusellenes információk megosztására alkalmassá vált, úgy a hatósági bejelentések kezelésére is képessé tehető.

A jogalanyok számára következő fájó pontként jelentkezik a fenyegető tényezők által a bekövetkezésük esetén okozott közvetlen és közvetett hatások, amelyek jelentős mértékben pénzben is kifejezhetőek. A KC3 kutatási céllal összefüggésben meghatároztam a kiberbiztonsági incidensek pénzügyi elemzésének egy lehetséges módszertanát, amely alapján megmutattam, hogy egy kiberbiztonsági incidens vállalatra (és a vállalat kockázatosságának megítélésére), ügyfeleire (beleértve a magánszemélyeket), a vállalat üzleti partnereire, tulajdonosaira, az államra és összességében a makrogazdaság teljesítményére és a nemzetközi pénzügyekre is hatással lehet. A szervezetre gyakorolt hatások elemzéséhez meghatároztam az $Incidens\ hatása$ és az $Incidensek\ hatása$, valamint az $Incidensek\ érzékelési\ eltérése^*$ mérőszámokat. A vizsgált esetek alapján megállapítottam, hogy egy incidens hatása és az incidens bekövetkezte eltérő naptári és pénzügyi évben is megvalósulhat, a hatás több éven át is jelentkezhet. Továbbá hipotetikus jelleggel azt a következtetést vontam le, hogy a vállalatra és vállalattulajdonosokra gyakorolt hatás részeként egy incidens a vállalat kockázatosságára is hatással lehet, valamint a részvényesek, mint vállalattulajdonosok, hajlamosak lehetnek a kiberbiztonsági incidensek által okozott hatás mértékét túlreagálni. Mindezek tényszerű megállapítása további kutatást igényel.

Új tudományos eredmények

A kutatásom során az Európai Unió kiberbiztonságának vizsgálatához a jogszabályi, a fenyegetettségek és a pénzügyi-gazdasági jellegű összefüggések elemzéséhez meghatározott hipotézisekre vonatkozóan az alábbi téziseket fogalmazom meg. A H2 és a H3 hipotézisek két részből álló összetett hipotézisek, ennélfogva a kapcsolódó téziseket ketté bontva kezelem.

T1: Igazoltam, hogy léteznek olyan szervezetek, illetve profitorientált vállalkozások, amelyek bár jelentős társadalmi vagy gazdasági funkciót töltenek be, nem vonatkoznak rájuk az uniós jogszabályokban előírt kiberbiztonsági elvárások. [BZs2] [BZs3] [BZs4] [BZs5] [BZs6] [BZs7]

T2.1: Igazoltam, hogy a kiberbiztonsági incidensek menedzselése kapcsán az Európai Unió hatályos jogszabályai átfedésben határozzák meg a vonatkozó szabályokat. [BZs1] [BZs2] [BZs3] [BZs6]

T2.2: Az elemzés során megállapítottam, hogy a kiberfenyegetettségre vonatkozó információk megosztását szolgáló célrendszerek az incidensek hatósági bejelentési kötelezettség támogatására is alkalmasak. [BZs1] [BZs7] [BZs8] [BZs9]

T3.1: Igazoltam, hogy egy szervezet esetén egy kiberbiztonsági incidens gazdasági hatásának vizsgálata többféle szempont alapján is lehetséges. [BZs10] [BZs11] [BZs12] [BZs13] [BZs14] [BZs15]

T3.2: A Magyarországon hatályos jogszabályokra korlátozódva igazoltam, hogy a hatályos jogszabályok helytelenül határozzák meg a kiberbiztonsági incidensek pénzügyi jellegű üzleti hatások vizsgálatára vonatkozó elvárásokat, amelyet a kockázatok elemzésekor figyelembe kell venni. [BZs10] [BZs11] [BZs12] [BZs13] [BZs14]

Ajánlások

A kutatásom eredményeképp a következő ajánlásokat fogalmazom meg:

A1.1: Javaslom a későbbiekben a NIS 2 irányelv utódja esetén („NIS 3 irányelv") a kiberbiztonságban érintettek körének további szélesítését.

A1.2: Javaslom a gazdasági érintettség alapján történő kijelölés feltételeinek szabályozását egy Európai Unióban egységes szempontrendszer alkalmazása mellett.

A2: Javaslom az Európai Unió jogszabályaiban a hatósági incidensbejelentési kötelezettség szabályozásának felülvizsgálatát, valamint az incidensbejelentési kötelezettség technikai támogatásának (pl. MISP platform alapon történő) kialakítását.

A3.1: Javaslom az üzleti hatások vizsgálati szempontjait az Európai Unió egészére vonatkozóan egységes jelleggel kezelését, minimálisan vizsgálandó szempontok és értékintervallumok megadása mellett. Ezzel összefüggésben az incidensek pénzügyi hatásainak időbelisége, a több évben jelentkező negatív pénzáramok, a bekövetkezés és a jelentkező hatás közötti időbeli differencia kezelése elengedhetetlen.

A3.2: Javaslom a vállalatok kockázatosságának (beta) többfaktor modell alapú számítása során a kiberbiztonsági és adatvédelmi incidensek hatásainak figyelembevételét. E javaslat egyben meghatározza a későbbi kutatásaim alapjait.

IRODALOMJEGYZÉK

[1] Karvalics L., ‘Információs társadalom – mi az? Egy kifejezés jelentése, története és fogalomkörnyezete’, in Az információs társadalom. Az elmélettõl a politikai gyakorlatig, L. Pintér, Ed., Budapest: Gondolat Kiadó, 2007, pp. 29–46.

[2] F. Webster, ‘What information society?’, Information Society, vol. 10, no. 1, pp. 1–23, 1994, doi: 10.1080/01972243.1994.9960154.

[3] R. Kurzweil, ‘The Law of Accelerating Returns’, in Alan Turing: Life and Legacy of a Great Thinker, C. Teuscher, Ed., Berlin, Heidelberg: Springer, 2004, pp. 381–416. doi: 10.1007/978-3-662-05642-4_16.

[4] Molnár Sz., Kollányi B. és Székely L., ‘Társadalmi hálózatok, hálózati társadalom’, in Az információs társadalom. Az elmélettõl a politikai gyakorlatig, Pintér L., Ed., Budapest: Gondolat Kiadó, 2007, pp. 64–81.

[5] D. Bell, ‘The Coming of the Post-Industrial Society’, Educ Forum, vol. 40, no. 4, pp. 574–579, 1976, doi: 10.1080/00131727609336501.

[6] European Union, ‘Information society’. Hozzáférés: 2020.12.09. [Online]. Elérhető: https://eur-lex.europa.eu/summary/glossary/information_society.html

[7] S. Micossi, ‘30 Years of the Single European Market’, Bruges European Economic Policy Briefings, vol. 41, pp. 1–36, 2016, Hozzáférés: 2023.02.26. [Online]. Elérhető: https://www.coleurope.eu/sites/default/files/research-paper/beep41_0.pdf

[8] Európai Bizottság, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Európai digitális egységes piaci stratégia. 2015. Hozzáférés: 2022.10.16. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52015DC0192

[9] Munk S., ‘A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései’, Hadtudomány, vol. 28, no. 1, pp. 113–131, 2018, doi: 10.17047/HADTUD.2018.28.1.113.

[10] ENISA, ‘ENISA overview of cybersecurity and related terminology’. Hozzáférés: 2019.02.17. [Online]. Elérhető: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

[11] D. T. Kuehl, ‘From Cyberspace to Cyberpower: Defining the Problem’, in Cyberpower and National Security, Potomac Books and National Defense University, 2009, pp. 24–42. doi: 10.2307/j.ctt1djmhj1.7.

[12] Kovács L., A kibertér védelme. Budapest: Dialóg Campus Kiadó, 2018. [Online]. Elérhető: https://www.uni-nke.hu/document/uni-nke-hu/Kovács László.pdf

[13] Haig Zs., Információs műveletek a kibertérben. Budapest: Dialóg Campus Kiadó, 2018. Hozzáférés: 2023.02.26. [Online]. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12651/web_PDF_Informacios_muveletek_a_kiberterben.pdf

[14] Munk S., 'Információs színtér, információs környezet, információs infrastruktúra', Nemzetvédelmi egyetemi közlemények, vol. VI, no. 2, pp. 133–154, 2002, doi: 20.500.12944/1083.

[15] Berzsenyi D., 'Globális kihívás, regionális válaszok: kiberbiztonság Kelet-Közép-Európában', Nemzet és Biztonság, no. 3, pp. 69–79, 2017, Hozzáférés: 2022.12.04. [Online]. Elérhető: https://folyoirat.ludovika.hu/index.php/neb/article/view/3721/2999

[16] Szörényi A., 'A nem-állami szereplők befolyásának növekedése a nemzetközi kapcsolatok különböző területein', Corvinus University of Budapest, Budapest, 2014. doi: 10.14267/phd.2014080.

[17] Haig Zs., Hajnal B., Kovács L., Muha L. és Sik Z. N., A kritikus információs infrastruktúrák meghatározásának módszertana. ENO Advisory Kft., 2009. Hozzáférés: 2022.07.23. [Online]. Elérhető: https://nki.gov.hu/wp-content/uploads/2009/10/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf

[18] Haig Zs. és Kovács L., Kritikus infrastruktúrák és kritikus információs infrastruktúrák. Nemzeti Közszolgálati Egyetem, 2012. [Online]. Elérhető: https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf

[19] M. Ryba, 'The role of ICT components in the functioning of critical infrastructure', in Critical Infrastructure Security - the ICT Dimension, J. Świątkowska, Ed., Kraków: The Kosciuszko Institute, 2014, pp. 59–62.

[20] S. Kumar, A. K. Singh és M. A. Kalam, 'Intelligent electronic device functionality and interfacing: An experimental examination of smart grid', International Journal of Recent Technology and Engineering, vol. 8, no. 2 Special Issue 11, 2019, doi: 10.35940/ijrte.B1523.0982S1119.

[21] Y. Maleh, 'IT/OT convergence and cyber security', Computer Fraud & Security, vol. 2021, no. 12, pp. 13–16, 2021, doi: https://doi.org/10.1016/S1361-3723(21)00129-9.

[22] Muha L. és Krasznay Cs., Az elektronikus információs rendszerek biztonságának menedzselése. Nemzeti Közszolgálati Egyetem, 2018. Hozzáférés: 2023.02.26. [Online]. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/7135/Az%20elektronikus%20inform%C3%A1ci%C3%B3s%20rendszerek%20biztons%C3%A1g%C3%A1nak%20menedzsel%C3%A9sej%C3%B3.pdf

[23] M. Dunn Cavelty és M. Suter, 'The Art of CIIP Strategy: Tacking Stock of Content and Processes', in Critical Infrastructure Protection, J. Lopez, R. Setola, and S. D. Wolthusen, Eds., Springer, 2012, pp. 15–38. doi: 10.1007/978-3-642-28920-0_2.

[24] A. Sarri és K. Moulinos, Stocktaking, Analysis and Recommendations on the Protection of CIIs. ENISA, 2016. doi: 10.2824/534303.

[25] D. Štrucl, 'Comparative study on the cyber defence of NATO Member States', NATO CCDCOE. Hozzáférés: 2022.07.27. [Online]. Elérhető: https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf

[26] A. Ekelhart, S. Fenz, M. D. Klemen és E. R. Weippl, 'Security ontology: Simulating threats to corporate assets', in Information Systems Security, A. Bagchi and V. Atluri, Eds., Kolkata, India: Springer, 2006. doi: 10.1007/11961635_17.

[27] R. von Solms és J. van Niekerk, 'From information security to cyber security', Comput Secur, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[28] Európai Tanács és Az Európai Unió Tanácsa, 'Információvédelem'. Hozzáférés: 2022.08.14. [Online]. Elérhető: https://www.consilium.europa.eu/hu/general-secretariat/corporate-policies/classified-information/information-assurance/

[29] International Organization for Standardization, ISO/IEC 27000:2018, 5th ed. 2018.

[30] Európai Központi Bank, 'What is cyber resilience?' Hozzáférés: 2022.08.14. [Online]. Elérhető: https://www.ecb.europa.eu/paym/cyber-resilience/html/index.hu.html

[31] International Organization for Standardization, ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements. 2019.

[32] T. Bonnyai, 'Kritikus infrastruktúrák védelme', in Kritikus információs infrastruktúrák védelme, V. Deák, Ed., Budapest: Nemzeti Közszolgálati Egyetem, 2019, pp. 56–83.

[33] L. Robert M., 'The Sliding Scale of Cyber Security', SANS Institute. Hozzáférés: 2022.08.16. [Online]. Elérhető: https://sansorg.egnyte.com/dl/GJEumszLQX

[34] R. M. von Roessing, The Business Model for Information Security. ISACA, 2010.

[35] International Organization for Standardization, 'ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements', 2013.

[36] International Organization for Standardization, ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls. 2022.

[37] National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1', Gaithersburg, MD, 2018. doi: 10.6028/NIST.CSWP.04162018.

[38] National Institute of Standards and Technology, 'NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations', Gaithersburg, MD, 2020. doi: 10.6028/NIST.SP.800-53r5.

[39] Wimmer Á., 'Üzleti teljesítménymérés az értékteremtés szolgálatában', Vezetéstudomány - Budapest Management Review, vol. 35, no. 9, pp. 2–11, 2004.

[40] National Institute of Standards and Technology, 'NIST Special Publication 800-207 - Zero Trust Architecture', 2020. doi: https://doi.org/10.6028/NIST.SP.800-207.

[41] International Organization for Standardization, 'ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model'. 2022.

[42] A Bizottság (EU) 2024/482 végrehajtási rendelete a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról. 2024. Hozzáférés: 2024.03.03. [Online]. Elérhető: http://data.europa.eu/eli/reg_impl/2024/482/oj

[43] OWASP, 'Application Security Verification Standard 4.0.3'. Hozzáférés: 2022.08.27. [Online]. Elérhető: https://raw.githubusercontent.com/OWASP/ASVS/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf

[44] American Psychological Association, 'APA Dictionary of Psychology'. Hozzáférés: 2022.09.15. [Online]. Elérhető: https://dictionary.apa.org

[45] ISACA Magyarországi Egyesület, ISACA magyar szakkifejezés-gyűjtemény. 2014. Hozzáférés: 2023.02.26. [Online]. Elérhető: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/isaca-glossary-english-hungarian_1213.pdf

[46] A. Tversky és D. Kahneman, ‘The framing of decisions and the psychology of choice’, Science (1979), vol. 211, no. 4481, pp. 453–458, 1981, doi: 10.1126/science.7455683.

[47] D. Kahneman, Thinking, Fast and Slow. New York: Farrar, Straus and Giroux, 2011.

[48] A. Chariri, ‘Cognitive Limitations and Decision Making’, Jurnal Bisnis Strategi, vol. 3, pp. 21–28, 1999.

[49] Barabási A. L., The Formula: The Universal Laws of Success. New York: Little, Brown and Company, 2018.

[50] A. Anastasios, ‘The 2019 SANS Security Awareness Report: Awareness Training Is Rising’. Hozzáférés: 27, 2022.02.27. [Online]. Elérhető: https://www.tripwire.com/state-of-security/sans-security-awareness-training-rising

[51] L. Spitzner, ‘Applying Security Awareness to the Cyber Kill Chain | SANS Security Awareness’, SANS Institute. Hozzáférés: 2020.02.01. [Online]. Elérhető: https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain

[52] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. 2013. Hozzáférés: 2024.03.11. [Online]. Elérhető: https://njt.hu/jogszabaly/2013-50-00-00

[53] Michelberger P. és Horváth Z., ‘Biztonságorientált folyamatmenedzsment’, International Journal of Engineering and Management Sciences, vol. 2, no. 4, 2017, doi: 10.21791/ijems.2017.4.28.

[54] A. Schmidt, ‘The Estonian Cyberattacks’, in A Fierce Domain: Conflict in Cyberspace, 1986 to 2012, J. Healey, Ed., Vienna: Cyber Conflict Studies Association, 2013, pp. 174–193.

[55] D. K. Bohl, B. B. Hughes, M. T. Irfan, E. S. Margolese-Malin és J. R. Solórzano, ‘Cyber Benefits and Risks: Quantitatively Understanding and Forecasting the Balance’, University of Denver, Zurich Insurance and Atlantic Council, 2015. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://korbel.du.edu/pardee/resources/cyber-benefits-and-risks-quantitatively-understanding-and-forecasting-balance

[56] Trading Economics, ‘Estonia - Credit Rating’. Hozzáférés: 2020.10.15. [Online]. Elérhető: https://tradingeconomics.com/estonia/rating

[57] The Baltic Times, ‘S&P’s slams Estonia with negative outlooks’, 2007.07.04. [Online]. Elérhető: https://www.baltictimes.com/news/articles/18203/

[58] Republic of Estonia, ‘Estonian National Strategic Reference Framework 2007-2013’. Hozzáférés: 2023.02.16. [Online]. Elérhető:

https://vana.struktuurifondid.ee/sites/default/files/estonian_national_strategic_reference_framework_2007-2013.pdf

[59] Ministry of Defence - Estonia, 'Cyber Security Strategy'. [Online]. Elérhető: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en

[60] S. Herzog, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses', Journal of Strategic Security, vol. 4, no. 2, pp. 49–60, 2011, doi: 10.5038/1944-0472.4.2.3.

[61] Paráda I., 'A NATO kibervédelmi irányelveinek fejlődése', Honvédségi Szemle – Hungarian Defence Review, vol. 146, no. 3, pp. 3–13, 2018, Hozzáférés: 2023.02.27. [Online]. Elérhető: https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/373

[62] Európai Tanács Főtitkársága, Európai biztonsági stratégia - Biztonságos Európa egy jobb világban. Luxembourg: Az Európai Unió Kiadóhivatala, 2009. doi: 10.2860/15719.

[63] Ármás J. és Nagy L., 'Hibrid hadviselés: a befolyás megtartásának-megszerzésének új eszköze a posztszovjet térségben?', Honvédségi Szemle – Hungarian Defence Review, vol. 148, no. 2, pp. 74–88, 2020, doi: 10.35926/hsz.2020.2.8.

[64] Az Európai Parlament és a Tanács 1007/2008/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendeletnek az Ügynökség megbízatási ideje tekintetében történő módosításáról. 2008. Hozzáférés: 2022.10.05. [Online]. Elérhető: http://data.europa.eu/eli/reg/2008/1007/oj

[65] Az Európai Közösségek Bizottsága, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről. 2009. Hozzáférés: 2022.10.07. [Online]. Elérhető: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:hu:PDF

[66] Európai Bizottság, EURÓPA 2020 Az intelligens, fenntartható és inkluzív növekedés stratégiája. 2010. Hozzáférés: 2022.10.07. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/hu/ALL/?uri=CELEX%3A52010DC2020

[67] Európai Bizottság, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Az európai digitális menetrend. 2010. Hozzáférés: 2022.10.07. [Online]. Elérhető: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:HU:PDF

[68] Megállapodás az Európai Parlament, az Európai Tanács, az Európai Unió Tanácsa, az Európai Bizottság, az Európai Unió Bírósága, az Európai Központi Bank, az Európai Számvevőszék, az Európai Külügyi Szolgálat, az Európai Gazdasági és Szociális Bizottság, a Régiók Európai Bizottsága és az Európai Beruházási Bank között az uniós intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportjának (CERT-EU) szervezetéről és működéséről. 2018. Hozzáférés: 2022.10.08. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX:32018Q0113(01)

[69] Az Európai Parlament és a Tanács 580/2011/EU rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendeletnek az ügynökség megbízatási ideje tekintetében történő módosításáról. 2011. Hozzáférés: 2022.10.05. [Online]. Elérhető: http://data.europa.eu/eli/reg/2011/580/oj

[70] Az Európai Parlament és a Tanács 526/2013/EU rendelete az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről. 2013. Hozzáférés: 2022.10.08. [Online]. Elérhető: http://data.europa.eu/eli/reg/2013/526/oj

[71] Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér. 2013. Hozzáférés: 2022.10.08. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX:52013JC0001

[72] L. Dupré, EP3R 2010-2013 - Four Years of Pan-European Public Private Cooperation. ENISA, 2014. doi: 10.2824/565581.

[73] Európai Unió, ‘Számítástechnikai Bűnözés Elleni Európai Központ az Europolon belül’. Hozzáférés: 2022.10.10. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM:230806_1

[74] Európai Bizottság, A Bizottság közleménye a Tanácsnak és az Európai Parlamentnek - Küzdelem digitális korunk bűnözésével: Számítástechnikai Bűnözés Elleni Európai Központ létrehozása. 2012. Hozzáférés: 2022.10.10. [Online]. Elérhető: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:HU:PDF

[75] Az Európai Unió Tanácsa, Uniós kibervédelmi szakpolitikai keret. 2014. [Online]. Elérhető: http://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/hu/pdf

[76] Európai Bizottság, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának - Az európai biztonsági

stratégia. 2015. Hozzáférés: 2022.10.09. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52015DC0185

[77] Európai Külügyi Szolgálat, Közös jövőkép, közös fellépés: Erősebb Európa - Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan. Luxembourg: Az Európai Unió Kiadóhivatala, 2016. doi: 10.2871/695883.

[78] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. 2016. Hozzáférés: 2022.10.08. [Online]. Elérhető: http://data.europa.eu/eli/dir/2016/1148/oj

[79] Európai Bizottság, Közös közlemény az Európai Parlamentnek és a Tanácsnak - Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése. 2017. Hozzáférés: 2022.10.10. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450

[80] D. E. Sanger, 'As Russian Hackers Probe, NATO Has No Clear Cyberwar Strategy', The New York Times, 2016.06.17. [Online]. Elérhető: https://www.nytimes.com/2016/06/17/world/europe/nato-russia-cyberwarfare.html

[81] Molnár A., 'Az Európai Unió kiberbiztonsággal kapcsolatos tevékenysége', in Kritikus információs infrastruktúrák védelme, Deák V., Ed., Budapest: Nemzeti Közszolgálati Egyetem, 2019, pp. 35–55.

[82] Az Európai Unió Tanácsa, Uniós kibervédelmi szakpolitikai keret (2018. évi naprakésszé tett változat). 2018. [Online]. Elérhető: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hu/pdf

[83] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály). 2019. Hozzáférés: 2022.10.12. [Online]. Elérhető: http://data.europa.eu/eli/reg/2019/881/oj

[84] A Tanács (EU) 2019/796 rendelete az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről. 2019. Hozzáférés: 2022.10.12. [Online]. Elérhető: http://data.europa.eu/eli/reg/2019/796/oj

[85] Az Európai Unió Tanácsa, ‘Az első uniós szankciók kibertámadások elkövetőivel szemben’. Hozzáférés: 2022.10.12. [Online]. Elérhető: https://www.consilium.europa.eu/hu/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/pdf

[86] Európai Tanács, ‘A Tanács következtetéseket fogadott el a csatlakoztatott eszközök kiberbiztonságáról’. Hozzáférés: 2022.10.13. [Online]. Elérhető: https://www.consilium.europa.eu/hu/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/pdf

[87] Közös közlemény az Európai Parlamentnek és a Tanácsnak - Az EU kiberbiztonsági stratégiája a digitális évtizedre. 2020. Hozzáférés: 2022.10.14. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX:52020JC0018

[88] Az Európai Parlament és a Tanács (EU) 2021/887 rendelete az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak és a nemzeti koordinációs központok hálózatának a létrehozásáról. 2021. Hozzáférés: 2022.10.14. [Online]. Elérhető: http://data.europa.eu/eli/reg/2021/887/oj

[89] Európai Bizottság, Javaslat – Az Európai Parlament és a Tanács irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről. 2020. Hozzáférés: 2022.10.15. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=COM:2020:823:FIN

[90] Az Európai Unió Tanácsa, Javaslat – Az Európai Parlament és a Tanács irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről – Általános megközelítés. 2021. Hozzáférés: 2022.10.15. [Online]. Elérhető: https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/hu/pdf

[91] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv). 2022. Hozzáférés: 2023.01.12. [Online]. Elérhető: http://data.europa.eu/eli/dir/2022/2555/oj

[92] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának - Digitális iránytű 2030-ig: a digitális évtized megvalósításának európai módja. 2021. Hozzáférés: 2022.10.15. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52021DC0118

[93] S. Backman, ‘Risk vs. threat-based cybersecurity: the case of the EU’, European Security, vol. 32, no. 1, pp. 85–103, 2022.05., doi: 10.1080/09662839.2022.2069464.

[94] A Tanács 2008/114/EK irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. 2008. Hozzáférés: 2022.09.30. [Online]. Elérhető: http://data.europa.eu/eli/dir/2008/114/oj

[95] Európai Bizottság, Javaslat Az Európai Parlament és a Tanács irányelve a kritikus fontosságú szervezetek rezilienciájáról. 2020. Hozzáférés: 2022.10.15. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52020PC0829

[96] Európai Bizottság, Javaslat – Az Európai Parlament és a Tanács rendelete a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK rendelet, a 648/2012/EU rendelet, a 600/2014/EU rendelet, valamint a 909/2014/EU rendelet módosításáról. 2020. Hozzáférés: 2022.10.15. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52020PC0595

[97] Az Európai Parlament és a Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről. 2014. Hozzáférés: 2022.11.02. [Online]. Elérhető: http://data.europa.eu/eli/reg/2014/910/oj

[98] Európai Bizottság, Javaslat az Európai Parlament és a Tanács rendelete a 910/2014/EU rendeletnek az európai digitális személyazonosság keretének létrehozása tekintetében történő módosításáról. 2021. Hozzáférés: 2022.10.17. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52021PC0281

[99] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). 2016. Hozzáférés: 2022.09.16. [Online]. Elérhető: http://data.europa.eu/eli/reg/2016/679/oj

[100] Az Európai Parlament és a Tanács 575/2013/EU rendelete a hitelintézetekre és befektetési vállalkozásokra vonatkozó prudenciális követelményekről és a 648/2012/EU rendelet módosításáról. 2013. Hozzáférés: 2024.05.09. [Online]. Elérhető: http://data.europa.eu/eli/reg/2013/575/oj

[101] Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU

rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről. 2015. Hozzáférés: 2022.11.02. [Online]. Elérhető: http://data.europa.eu/eli/dir/2015/2366/oj

[102] 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról. 2013. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2013-237-00-00

[103] 42/2015. (III. 12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről. 2015. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2015-42-20-22

[104] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2012-166-00-00

[105] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól. 2015. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2015-222-00-00

[106] 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól. 2023. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2023-103-00-00

[107] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról jogszabály tartalmazza. 2011. Hozzáférés: 2023.03.27. [Online]. Elérhető: https://njt.hu/jogszabaly/2011-112-00-00

[108] 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről. 2023. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2023-23-00-00

[109] 2013. évi CCXXXV. törvény az egyes fizetési szolgáltatókról. 2013. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2013-235-00-00

[110] Centre for Cybersecurity Belgium, 'The NIS 2 Directive: what does it mean for my organization?' Hozzáférés: 2024.03.12. [Online]. Elérhető: https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization

[111] Európai Parlament, Jelentés a 2016–2020-as időszakra vonatkozó uniós e-kormányzati cselekvési tervről. 2017. Hozzáférés: 2022.10.12. [Online]. Elérhető: https://www.europarl.europa.eu/doceo/document/A-8-2017-0178_HU.pdf

[112] Anomali, ‘APT28 Timeline of Malicious Activity’. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://www.anomali.com/blog/a-timeline-of-apt28-activity

[113] J. Orr, ‘Incident Of The Week: 4 Million Bulgarian Citizens Affected By Tax Agency Data Breach’, CYBER Security Hub, 2019.07.26. [Online]. Elérhető: https://www.cshub.com/attacks/articles/incident-of-the-week-4-million-bulgarian-citizens-affected-by-tax-agency-data-breach

[114] A Tanács 904/2010/EU rendelete a hozzáadottérték-adó területén történő közigazgatási együttműködésről és csalás elleni küzdelemről (átdolgozás). 2010. Hozzáférés: 2022.10.11. [Online]. Elérhető: http://data.europa.eu/eli/reg/2010/904/oj

[115] 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. 2015. Hozzáférés: 2024.03.11. [Online]. Elérhető: https://njt.hu/jogszabaly/2015-187-20-22

[116] 2013. évi CXXXIX. törvény a Magyar Nemzeti Bankról. 2013. Hozzáférés: 2024.03.11. [Online]. Elérhető: https://njt.hu/jogszabaly/2013-139-00-00.62

[117] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről. 2018. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://njt.hu/jogszabaly/2015-41-20-0A

[118] National Institute of Standards and Technology, NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. 2013. doi: 10.6028/NIST.SP.800-53Ar4.

[119] Miniszterelnöki Kabinetirodát vezető miniszter, A Miniszterelnöki Kabinetirodát vezető miniszter ---------- MK rendelete a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről. 2024. Hozzáférés: 2024.03.11. [Online]. Elérhető: https://cdn.kormany.hu/uploads/document/2/25/25e/25e5d729f900acc21babb2d22da8cc03aa810a71.pdf

[120] Decreto del Presidente del Consiglio dei Ministri 14 aprile 2021, n. 81. Hozzáférés: 2022.10.29. [Online]. Elérhető: https://www.normattiva.it/uri-

res/N2Ls?urn:nir:stato:decreto.del.presidente.del.consiglio.dei.ministri:2021-04-14;81!vig=2021-06-30

[121] S. Schmitz-Berndt and P. G. Chiara, ‘One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive’, International Cybersecurity Law Review, vol. 3, pp. 289–311, 2022. doi: 10.1365/s43439-022-00058-7.

[122] BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist. Hozzáférés: 2022.10.29. [Online]. Elérhető: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

[123] ENISA, ‘Best practices for cyber crisis management’, 2024. doi: 10.2824/767828.

[124] J. De Muynck and S. Portesi, ‘Strategies for Incident Response and Cyber Crisis Cooperation’, 2016. doi: 10.2824/967546.

[125] NIS Cooperation Group, ‘Synergies in Cybersecurity Incident Reporting’. 2020.12. Hozzáférés: 2023.01.19. [Online]. Elérhető: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72147

[126] C. Lambrinoudakis et al., Interoperable EU risk management framework. ENISA, 2022. doi: 10.2824/07253.

[127] D. J. Bodeau, C. D. McCollum, and D. B. Fox, ‘Cyber Threat Modeling: Survey, Assessment, and Representative Framework’, 2018.04. Hozzáférés: 2022.11.23. [Online]. Elérhető: https://www.mitre.org/sites/default/files/2021-11/prs-18-1174-ngci-cyber-threat-modeling.pdf

[128] Joint Task Force Transformation Initiative, NIST SP 800-39 Managing Information Security Risk. National Institute of Standards and Technology, 2011. doi: 10.6028/NIST.SP.800-39.

[129] ‘ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks’, 2022.

[130] National Institute of Standards and Technology, NIST SP 800-30 R1 - Guide for conducting risk assessments. 2012. doi: 10.6028/NIST.SP.800-30r1.

[131] Office of the Director of National Intelligence, ‘Building Blocks of Cyber Intelligence’. Hozzáférés: 2023.02.23. [Online]. Elérhető: https://www.dni.gov/index.php/cyber-threat-framework

[132] B. Schneier, ‘Attack trees: Modeling security threats’, Dr. Dobb’s Journal, 1999.12., Hozzáférés: 2022.11.23. [Online]. Elérhető: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

[133] L. Zhang, A. Taal, R. Cushing, C. de Laat, and P. Grosso, ‘A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces’, Int J Inf Secur, vol. 21, pp. 509–525, 2021, doi: 10.1007/s10207-021-00566-3.

[134] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, ‘MITRE ATT&CK: Design and Philosophy’. Hozzáférés: 2021.12.11. [Online]. Elérhető: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

[135] MITRE, ‘Common Attack Pattern Enumeration and Classification’. Hozzáférés: 2022.11.24. [Online]. Elérhető: https://capec.mitre.org/index.html

[136] T. Ucedavélez and M. M. Morana, Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. John Wiley & Sons, Inc, 2015. doi: 10.1002/9781118988374.

[137] ENISA, ‘Cyber Security and Resilience of smart cars’, 2016. doi: 10.2824/87614.

[138] ENISA, ‘Glossary’. Hozzáférés: 2022.11.29. [Online]. Elérhető: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary

[139] National Institute of Standards and Technology, FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems. 2006, doi: 10.6028/NIST.FIPS.200.

[140] ENISA, ‘Threat Taxonomy’. Hozzáférés: 2023.01.16. [Online]. Elérhető: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

[141] NIS Cooperation Group, ‘Cybersecurity Incident Taxonomy’. 2018. Hozzáférés: 2023.01.17. [Online]. Elérhető: https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

[142] M. Theocharidou, A. Malatras, I. Lella, and E. Tsekmezoglou, ‘Threat Landscape 2021’. ENISA, 2021. doi: 10.2824/324797.

[143] G. Alblas és E. Wijsman, Organisational Behaviour, 2nd Edition. London: Routledge, 2021. doi: 10.4324/9781003194736.

[144] D. Gervasi, G. Faldetta, M. M. Pellegrini és J. Maley, ‘Reciprocity in organizational behavior studies: A systematic literature review of contents, types, and directions’, European Management Journal, vol. 40, no. 3, pp. 441–457, 2022, doi: 10.1016/j.emj.2021.07.008.

[145] R. A. Gandhi, Anup Sharma, W. Mahoney, W. Sousan, Q. Zhu és P. A. Laplante, 'Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political', IEEE Technology and Society Magazine, vol. 30, no. 1, pp. 28–38, 2011, doi: 10.1109/MTS.2011.940293.

[146] Verizon, 'Data Breach Investigations Report 2020'. Hozzáférés: 2021.03.23. [Online]. Elérhető: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

[147] M. Lee, 'Russia Is Losing a War Against Hackers Stealing Huge Amounts of Data', The Intercept. Hozzáférés: 2022.12.09. [Online]. Elérhető: https://theintercept.com/2022/04/22/russia-hackers-leaked-data-ukraine-war/

[148] W. Chang, A. Mohaisen, A. Wang, and S. Chen, 'Measuring botnets in the wild: Some new trends', in ASIACCS 2015 - Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, 2015, pp. 645–650. doi: 10.1145/2714576.2714637.

[149] C. Cimpanu, 'Hacker takes over 29 IoT botnets', ZDNet. Hozzáférés: 2020.03.10. [Online]. Elérhető: https://www.zdnet.com/article/hacker-takes-over-29-iot-botnets/

[150] IBM Corporation, 'The inside story on botnets'. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://securityintelligence.com/inside-story-on-botnets/

[151] K.-L. Hui and J. Zhou, 'The Economics of Hacking', Oxford Research Encyclopedia of Business and Management, 2020, doi: 10.2139/ssrn.3695381.

[152] D. Manky, 'Cybercrime as a service: A very modern business', Computer Fraud and Security, vol. 2013, no. 6, pp. 9–13, 2013, doi: 10.1016/S1361-3723(13)70053-8.

[153] Szőr P., The Art of Computer Virus Research and Defense. New Jersey: Pearson Education (US), 2005.

[154] C. G. J. Putman, A. Abhishta és L. J. M. Nieuwenhuis, 'Business Model of a Botnet', in Proceedings - 26th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, PDP 2018, 2018, pp. 441–445. doi: 10.1109/PDP2018.2018.00077.

[155] MITRE, 'Develop Capabilities'. Hozzáférés: 2023.01.05. [Online]. Elérhető: https://attack.mitre.org/techniques/T1587/

[156] MITRE, 'Obtain Capabilities'. Hozzáférés: 2023.01.05. [Online]. Elérhető: https://attack.mitre.org/techniques/T1588/

[157] CERT-FR, 'The malware-as-a-service Emotet', 2021.02. Hozzáférés: 2023.01.27. [Online]. Elérhető: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-003.pdf

[158] R. M. Ryan és E. L. Deci, ‘Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions’, Contemp Educ Psychol, vol. 25, no. 1, pp. 54–67, 2000, doi: 10.1006/ceps.1999.1020.

[159] H. Rhee, ‘Comparison of Process Theories to Content Theories in Motivating Workforces’, International Journal of Human Resource Studies, vol. 9, no. 4, pp. 267–274, 2019, doi: 10.5296/ijhrs.v9i4.15620.

[160] M. F. Washburn, ‘Dynamic Psychology . By Robert Sessions Woodworth. New York, Columbia University Press. 1918. Pp. 210.’, Science (1979), vol. 48, no. 1241, 1918, doi: 10.1126/science.48.1241.372.

[161] S. B. Klein, Motivation: Biosocial Approaches. McGraw-Hill, 1982.

[162] E. N. és C. L. Hull, ‘Principles of Behavior. An Introduction to Behavior Theory’, J Philos, vol. 40, no. 20, pp. 558–559, 1943, doi: 10.2307/2019960.

[163] O. Guy-Evans, ‘Drive-Reduction Theory and Human Behavior’, SimplyPschichology. Hozzáférés: 2022.12.12. [Online]. Elérhető: https://www.simplypsychology.org/drive-reduction-theory.html

[164] A. H. Maslow, ‘A theory of human motivation’, Psychol Rev, vol. 50, no. 4, pp. 370–396, 1943, doi: 10.1037/h0054346.

[165] A. H. Maslow, Motivation and Personality, 2nd Edition. Harper & Row, 1970.

[166] A. H. Maslow, ‘New Introduction: Religions, Values, and Peak-Experiences’, Journal of Transpersonal Psychology, vol. 2, no. 2, pp. 83–90, 1970.

[167] A. H. Maslow, Motivation és personality, 3rd Edition. Delhi, India: Pearson Education, 1987.

[168] C. Miller, ‘Kim Jong-il and me: How to build a cyber army to attack the U.S.’, in DEF CON 18, 2010. Hozzáférés: 2022.12.21. [Online]. Elérhető: https://defcon.org/images/defcon-18/dc-18-presentations/Miller/DEFCON-18-Miller-Cyberwar.pdf

[169] E. Hutchins, M. Cloppert és R. Amin, ‘Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains’, Leading Issues in Information Warfare & Security Research, vol. 1, no. 1, pp. 1–14, 2011, Hozzáférés: 2023.02.27. [Online]. Elérhető: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[170] MITRE, ‘MITRE ATT&CK - Enterprise Matrix’. Hozzáférés: 2021.12.11. [Online]. Elérhető: https://attack.mitre.org/matrices/enterprise/

[171] MITRE, ‘MITRE ATT&CK - Mobile Matrix’. Hozzáférés: 2022.12.23. [Online]. Elérhető: https://attack.mitre.org/matrices/mobile/

[172] MITRE, ‘MITRE ATT&CK - ICS Matrix’. Hozzáférés: 2022.12.23. [Online]. Elérhető: https://attack.mitre.org/matrices/ics/

[173] MITRE, ‘Common Weakness Enumeration’. Hozzáférés: 2023.01.04. [Online]. Elérhető: https://cwe.mitre.org/

[174] MITRE, ‘Common Vulnerabilities and Exposures’. Hozzáférés: 2023.01.04. [Online]. Elérhető: https://cve.mitre.org/

[175] N. Y. Conteh és P. J. Schmick, ‘Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks’, International Journal of Advanced Computer Research (IJACR), vol. 6, no. 23, pp. 31–38, 2016, doi: 10.19101/IJACR.2016.623006.

[176] ENISA, ‘ENISA Threat Landscape Report 2018’, 2019. doi: 10.2824/622757.

[177] ENISA, ‘Threat Landscape 2022’, 2022. doi: 10.2824/764318.

[178] J. Aycock, Spyware and adware. New York, NY: Springer, 2011. doi: 10.1007/978-0-387-77741-2.

[179] S. Eskandari, A. Leoutsarakos, T. Mursch és J. Clark, ‘A First Look at Browser-Based Cryptojacking’, in Proceedings - 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018, 2018. doi: 10.1109/EuroSPW.2018.00014.

[180] J. R. Youngblood, ‘Ransomware’, in Business Theft and Fraud, 1st Edition., J. R. Youngblood, Ed., Boca Raton, FL: Taylor & Francis Group, 2016, pp. 307–310. doi: 10.1201/9781315380780.

[181] P. Brichant, Ryan; Eftekhari, ‘The rise of disruptionware’, ICIT & Forescout. Hozzáférés: 2019.09.29. [Online]. Elérhető: https://icitech.org/wp-content/uploads/2019/09/ICIT-Brief-The-Rise-of-Disruptionware.pdf

[182] P. Ravali, ‘A Comparative Evaluation of OSI and TCP/IP Models’, International Journal of Science and Research, vol. 4, no. 7, pp. 514–521, 2013.

[183] S. M. Specht és R. B. Lee, ‘Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures’, in Proceedings of the International Workshop on Security in Parallel and

Distributed Systems, San Francisco, 2004, pp. 543–550. Hozzáférés: 2023.02.27. [Online]. Elérhető: http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf

[184] E. C. Tandoc, Z. W. Lim és R. Ling, 'Defining "Fake News": A typology of scholarly definitions', Digital Journalism, vol. 6, no. 2. pp. 137–153, 2018. doi: 10.1080/21670811.2017.1360143.

[185] H. Siddiqui, E. Healy és A. Olmsted, 'Bot or not', in 2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017, Cambridge, UK, 2018, pp. 462–463. doi: 10.23919/ICITST.2017.8356448.

[186] M. Khonji, Y. Iraqi és A. Jones, 'Phishing Detection: A Literature Survey', IEEE Communications Surveys and Tutorials, vol. 15, no. 4. pp. 2091–2121, 2013. doi: 10.1109/SURV.2013.032213.00009.

[187] Object Management Group, OMG Unified Modeling Language. 2017. Hozzáférés: 2023.01.10. [Online]. Elérhető: https://www.omg.org/spec/UML/2.5.1/PDF

[188] E. Hemberg et al., 'Linking Threat Tactics, Techniques, and Patterns with Defensive Weaknesses, Vulnerabilities and Affected Platform Configurations for Cyber Hunting'. 2020. doi: 10.48550/arXiv.2010.00533.

[189] R. McMillan, 'Definition: Threat Intelligence', Gartner Research. 2013. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://www.gartner.com/en/documents/2487216

[190] K. Baker, 'What is Cyber Threat Intelligence?', Crowdstrike. Hozzáférés: 2022.12.01. [Online]. Elérhető: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

[191] W. Tounsi és H. Rais, 'A survey on technical threat intelligence in the age of sophisticated cyber attacks', Comput Secur, vol. 72, pp. 212–233, 2018, doi: 10.1016/j.cose.2017.09.001.

[192] D. Chismon és M. Ruks, Threat Intelligence: Collecting, Analysing, Evaluating. MWR Infosecurity & CERT-UK, 2015. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf

[193] M. E. Korstanje, Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities. IGI Global, 2016. doi: 10.4018/978-1-5225-1938-6.

[194] G. Manco, 'Threat Intelligence Platforms', in The European Network for Cybersecurity (NeCS) PhD School, Trento, 2022. Hozzáférés: 2022.12.03. [Online]. Elérhető: https://gmanco.github.io/talk_trento_gen22.pdf

[195] Gartner, ‘CrowdStrike Reviews’. Hozzáférés: 2022.12.04. [Online]. Elérhető: https://www.gartner.com/reviews/market/endpoint-protection-platforms/vendor/crowdstrike

[196] Gartner, ‘Check Point Software Technologies Reviews’. Hozzáférés: 2022.12.04. [Online]. Elérhető: https://www.gartner.com/reviews/market/network-firewalls/vendor/check-point-software-tech

[197] Gartner, ‘Recorded Future Reviews’. Hozzáférés: 2022.12.04. [Online]. Elérhető: https://www.gartner.com/reviews/market/security-threat-intelligence-services/vendor/recorded-future

[198] Check Point, ‘What is Cyber Threat Intelligence?’ Hozzáférés: 2022.12.04. [Online]. Elérhető: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-threat-intelligence/

[199] Recorded Future, ‘What is Threat Intelligence?’ Hozzáférés: 2022.12.04. [Online]. Elérhető: https://www.recordedfuture.com/threat-intelligence

[200] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder és C. Skorupka, Guide to Cyber Threat Information Sharing. Gaithersburg, MD: National Institute of Standards and Technology, 2016. doi: 10.6028/NIST.SP.800-150.

[201] T. D. Wagner, K. Mahbub, E. Palomar és A. E. Abdallah, ‘Cyber threat intelligence sharing: Survey and research directions’, Comput Secur, vol. 87, p. 101589, Nov. 2019, doi: 10.1016/j.cose.2019.101589.

[202] MISP Project, ‘MISP Threat Sharing’. Hozzáférés: 2023.10.20. [Online]. Elérhető: https://www.misp-project.org/

[203] ETSI, ETSI TR 103 456 V1.1.1 (2017-10) CYBER; Implementation of the Network and Information Security (NIS) Directive. 2017. Hozzáférés: 2023.01.20. [Online]. Elérhető: https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf

[204] G. Settanni et al., ‘A collaborative cyber incident management system for European interconnected critical infrastructures’, Journal of Information Security and Applications, vol. 34, no. 2, pp. 166–182, 2017.06., doi: 10.1016/j.jisa.2016.05.005.

[205] K. Satlas, ‘CTI-EU event’, in Cyber Threat Intelligence CERT-EU vision, Róma: CERT-EU, 2017.10. Hozzáférés: 2023.01.20. [Online]. Elérhető: https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/cert-eu-presentation/

[206] B. Stojkovski, G. Lenzini, V. Koenig és S. Rivas, ‘What’s in a Cyber Threat Intelligence sharing platform?’, in Annual Computer Security Applications Conference, New York, NY, USA: ACM, Dec. 2021, pp. 385–398. doi: 10.1145/3485832.3488030.

[207] A. Michota, A. Mitrakas, C. Patsakis és V. Stupka, ‘Technical aspects of cooperation between CSIRTS and LE’. ENISA, Dec. 2019. doi: 10.2824/28206.

[208] MISP Project, ‘How MISP enables stakeholders identified by the NISD to perform key activities’. Hozzáférés: 2023.01.20. [Online]. Elérhető: https://www.misp-project.org/compliance/NISD/

[209] FIRST, ‘TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0’. Hozzáférés: 2023.01.22. [Online]. Elérhető: https://www.first.org/tlp/

[210] ENISA, ‘Considerations on the Traffic Light Protocol’. Hozzáférés: 2023.01.22. [Online]. Elérhető: https://www.enisa.europa.eu/topics/incident-response/glossary/considerations-on-the-traffic-light-protocol

[211] FireEye, ‘OpenIOC_1.1’. Hozzáférés: 2023.01.16. [Online]. Elérhető: https://github.com/fireeye/OpenIOC_1.1

[212] Internet Engineering Task Force (IETF), ‘The Incident Object Description Exchange Format Version 2’. Hozzáférés: 2023.01.16. [Online]. Elérhető: https://www.rfc-editor.org/rfc/rfc7970

[213] Verizon, ‘Vocabulary for Event Recording and Incident Sharing (VERIS)’. Hozzáférés: 2023.01.16. [Online]. Elérhető: https://github.com/vz-risk/veris

[214] MITRE, ‘STIX Release Archive’. Hozzáférés: 2023.01.17. [Online]. Elérhető: https://stixproject.github.io/releases/archive/

[215] MITRE, ‘Cyber Observable eXpression (CybOXTM) Archive Website’. Hozzáférés: 2023.01.17. [Online]. Elérhető: https://cyboxproject.github.io/

[216] OASIS, ‘OASIS Cyber Threat Intelligence (CTI) TC’. Hozzáférés: 2023.01.17. [Online]. Elérhető: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

[217] OASIS Open, ‘STIX Best Practices Guide Version 1.0.0’. 2022.09.15. Hozzáférés: 2023.01.18. [Online]. Elérhető: https://docs.oasis-open.org/cti/stix-bp/v1.0.0/stix-bp-v1.0.0.pdf

[218] MITRE, ‘Malware Attribute Enumeration and Characterization (MAEC)’. Hozzáférés: 2023.01.18. [Online]. Elérhető: https://maecproject.github.io/

[219] OASIS, ‘TAXII Version 2.1’. 2021.06.10. Hozzáférés: 2023.01.18. [Online]. Elérhető: https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html

[220] A. Ramsdale, S. Shiaeles és N. Kolokotronis, ‘A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages’, Electronics (Basel), vol. 9, no. 5, p. 824, 2020, doi: 10.3390/electronics9050824.

[221] ENISA, ‘Gaps in NIS standardisation Recommendations for improving NIS in EU standardisation policy’. 2016. doi: 10.2824/975760.

[222] Európai Bizottság, A Bizottság (EU) 2017/2288 végrehajtási határozata a közbeszerzésben hivatkozható IKT műszaki előírások azonosításáról. 2017. Hozzáférés: 2023.01.18. [Online]. Elérhető: http://data.europa.eu/eli/dec_impl/2017/2288/oj

[223] DIGITALEUROPE, ‘The EU-US Trade & Technology Council: from ambitious work plans to concrete outcomes’. 2022. Hozzáférés: 2023.01.18. [Online]. Elérhető: https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2022/09/TTC_from_ambition_to_outcome.pdf

[224] A. Malatras, E. Tsekmezoglou, M. Theocharidou és R. Naydenov, Cybersecurity Threat Landscape Methodology. ENISA, 2022. doi: 10.2824/339396.

[225] MISP Project, ‘MISP Published Standards’. Hozzáférés: 2023.01.22. [Online]. Elérhető: https://www.misp-standard.org/standards/

[226] OASIS, ‘STIX Version 2.1’. Hozzáférés: 2023.01.17. [Online]. Elérhető: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html

[227] C. Oral és G. CenkAkkaya, ‘Cash Flow at Risk: A Tool for Financial Planning’, Procedia Economics and Finance, vol. 23, pp. 262–266, 2015, doi: 10.1016/s2212-5671(15)00358-5.

[228] IFRS, ‘IAS 7 Statement of Cash Flows’. 2022. Hozzáférés: 2023.02.28. [Online]. Elérhető: https://www.ifrs.org/content/dam/ifrs/publications/pdf-standards/english/2022/issued/part-a/ias-7-statement-of-cash-flows.pdf?bypass=on

[229] O. Žižlavský, ‘Net Present Value Approach: Method for Economic Assessment of Innovation Projects’, Procedia Soc Behav Sci, vol. 156, pp. 506–512, 2014, doi: 10.1016/j.sbspro.2014.11.230.

[230] I. Fisher, The theory of interest. New York: Macmillan, 1930.

[231] F. Modigliani és M. H. Miller, ‘The Cost of Capital, Corporation Finance and the Theory of Investment’, Am Econ Rev, vol. 48, no. 3, pp. 261–297, 1958.

[232] F. Modigliani és M. H. Miller, ‘Corporate Income Taxes and the Cost of Capital: A Correction’, Am Econ Rev, vol. 53, no. 3, pp. 433–443, 1963.

[233] S. C. Myers, ‘Interactions of Corporate Financing and Investment Decisions-Implications for Capital Budgeting’, J Finance, vol. 29, no. 1, pp. 1–25, 1974, doi: 10.2307/2978211.

[234] P. Fernández, ‘Valuing companies by cash flow discounting: ten methods and nine theories’, Managerial Finance, vol. 33, no. 11, pp. 853–876, 2007, doi: 10.1108/03074350710823827.

[235] A. Beccarini, ‘Investment sensitivity to interest rates in an uncertain context: is a positive relationship possible?’, Economic Change and Restructuring, vol. 40, pp. 223–234, 2007.09., doi: 10.1007/s10644-007-9025-1.

[236] M. Rossi, ‘The capital asset pricing model: A critical literature review’, Global Business and Economics Review, vol. 18, no. 5, pp. 604–617, 2016, doi: 10.1504/GBER.2016.078682.

[237] M. A. Elbannan, ‘The Capital Asset Pricing Model: An Overview of the Theory’, Int J Econ Finance, vol. 7, no. 1, pp. 216–228, 2014, doi: 10.5539/ijef.v7n1p216.

[238] A. Damodaran, Investment Valuation: Tools and Techniques for Determining the Value of Any Asset, 3rd edition. John Wiley & Sons, 2012.

[239] P. Fernández, ‘WACC: Definition, Misconceptions, and Errors’, Business Valuation Review, vol. 29, no. 4, pp. 138–144, 2010, doi: 10.5791/0897-1781-29.4.138.

[240] E. F. FAMA and K. R. FRENCH, ‘The Cross-Section of Expected Stock Returns’, J Finance, vol. 47, no. 2, pp. 427–465, 1992, doi: 10.1111/j.1540-6261.1992.tb04398.x.

[241] M. M. Carhart, ‘On Persistence in Mutual Fund Performance’, J Finance, vol. 52, no. 1, pp. 57–82, 1997, doi: 10.1111/j.1540-6261.1997.tb03808.x.

[242] Ľ. Pástor és R. F. Stambaugh, ‘Liquidity Risk and Expected Stock Returns’, Journal of Political Economy, vol. 111, no. 3, pp. 642–685, 2003, doi: 10.1086/374184.

[243] E. F. Fama és K. R. French, ‘A five-factor asset pricing model’, J financ econ, vol. 116, no. 1, pp. 1–22, 2015, doi: 10.1016/j.jfineco.2014.10.010.

[244] F. P. Ramsey, ‘A Mathematical Theory of Saving’, The Economic Journal, vol. 38, no. 152, pp. 543–559, 1928, doi: 10.2307/2224098.

[245] V. Kazlauskienė, ‘Application of Social Discount Rate for Assessment of Public Investment Projects’, Procedia Soc Behav Sci, vol. 213, pp. 461–467, 2015, doi: 10.1016/j.sbspro.2015.11.434.

[246] M. A. Moore, A. E. Boardman, A. R. Vining, D. L. Weimer és D. H. Greenberg, '"Just give me a number!" Practical values for the social discount rate', Journal of Policy Analysis and Management, vol. 23, no. 4, pp. 789–812, 2004, doi: 10.1002/pam.20047.

[247] J. Zhuang, Z. Liang, T. Lin és F. D. xDe Guzman, 'Theory and practice in the choice of social discount rate for cost-benefit analysis: a survey', 2007. Hozzáférés: 2023.01.26. [Online]. Elérhető: http://hdl.handle.net/11540/1853

[248] N. Sklavos és P. Souras, 'Economic models and approaches in information security for computer networks', International Journal of Network Security, vol. 2, no. 1, pp. 14–20, 2006, Hozzáférés: 2023.02.01. [Online]. Elérhető: ijns.jalaxy.com.tw/download_paper.jsp?PaperID=IJNS-2005-07-08-1&PaperName=ijns-v2-n1/ijns-2006-v2-n1-p14-20.pdf

[249] L. A. Gordon és Martin P. Loeb, 'The economics of information security investment', ACM Transactions on Information and System Security, vol. 5, no. 4, pp. 438–457, 2002, doi: 10.1145/581271.581274.

[250] Z. Bederna és T. Szadeczky, 'Industry 4.0-based critical infrastructure and the NIS Directive', in Central and Eastern European eDem and eGov Days, New York, NY, USA: ACM, 2022, pp. 93–99. doi: 10.1145/3551504.3551546.

[251] T. Szádeczky és Z. Bederna, 'The Economic Measurement of Cyber Incidents', Periodica Polytechnica Social and Management Sciences, 2023, doi: 10.3311/PPso.22150.

[252] T. Olovsson, 'A structured approach to computer security', Chalmers University of Technology, Gothenburg, 1992. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://research.chalmers.se/en/publication/166411

[253] K. Ruan, 'Introducing cybernomics: A unifying economic framework for measuring cyber risk', Comput Secur, vol. 65, pp. 77–89, 2017, doi: 10.1016/j.cose.2016.10.009.

[254] J. Freund és J. Jones, Measuring and Managing Information Risk. Elsevier, Butterworth-Heinemann, 2015. doi: 10.1016/C2013-0-09966-5.

[255] A. Erola, I. Agrafiotis, J. R. C. Nurse, L. Axon, M. Goldsmith és S. Creese, 'A system to calculate Cyber Value-at-Risk', Comput Secur, vol. 113, p. 102545, 2022, doi: 10.1016/j.cose.2021.102545.

[256] M. Talabis és J. Martin, 'Information Security Risk Assessments', in Information Security Risk Assessments, Elsevier, 2013, pp. 1–26. doi: 10.1016/B978-1-59-749735-0.00001-4.

[257] W. K. Brotby, Information Security Management Metrics, 1st Edition. New York: Auerbach Publications, 2009.

[258] EY, ‘Applying IFRS Accounting for the financial impact of natural disasters’. Hozzáférés: 2023.02.17. [Online]. Elérhető: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/ifrs/ey-applying-ifrs-natural-disasters.pdf

[259] M. Rabin, ‘Psychology and Economics’, J Econ Lit, vol. 36, no. 1, pp. 11–46, 1998, Hozzáférés: 2023.02.28. [Online]. Elérhető: https://www.jstor.org/stable/2564950

[260] A. Tversky és D. Kahneman, ‘Judgment under uncertainty: Heuristics and biases’, Science (1979), vol. 185, no. 4157, pp. 1124–1131, 1974, doi: 10.1126/science.185.4157.1124.

[261] N. Ambady és R. Rosenthal, ‘Thin slices of expressive behavior as predictors of interpersonal consequences: A meta-analysis’, Psychol Bull, vol. 111, no. 2, pp. 256–274, 1992, doi: 10.1037/0033-2909.111.2.256.

[262] B. Schwartz, The Paradox of Choice. New York, USA: HarperCollins Publishers Inc, 2004.

[263] International Monetary Fund, Balance of Payments and International Investment Position Manual, 6th Edition. Washington, D.C: International Monetary Fund, 2009. Hozzáférés: 2023.02.28. [Online]. Elérhető: https://www.imf.org/external/pubs/ft/bop/2007/pdf/bpm6.pdf

[264] United Nations, System of National Accounts 2008. New York, [Brussels/Luxembourg], [Washington, D.C.], [Paris], [Washington, D.C.]: United Nations; Commission of the European Communities; International Monetary Fund; Organisation for Economic Co-operation and Development; World Bank, 2010. doi: 10.18356/4fa11624-en.

[265] European Commission, European system of accounts ESA 2010. Luxembourg: Publications Office of the European Union, 2010. doi: 10.2785/16644.

[266] Az Európai Parlament és a Tanács 549/2013/EU rendelete az Európai Unió-beli nemzeti és regionális számlák európai rendszeréről. 2013. Hozzáférés: 2023.02.06. [Online]. Elérhető: http://data.europa.eu/eli/reg/2013/549/oj

[267] S. Suranovic, International Finance: Theory and Policy. Saylor Foundation 2010, 2010.

[268] BBC, ‘Tesco Bank attack: What do we know?’, 2016.11.07. Hozzáférés: 2022.04.25. [Online]. Elérhető: https://www.bbc.com/news/technology-37896273

[269] Tesco PLC, ‘Tesco PLC Annual Report and Financial Statements 2017’. Hozzáférés: 2022.04.28. [Online]. Elérhető: https://www.tescoplc.com/media/474467/16-tesco-annual-report-2017.pdf

[270] L. Botter, ‘Tesco Shares Fall After Cyber Attack at its Online Banking Group Hits 40,000 Customers’, TheStreet, 2016.11.07. Hozzáférés: 2022.04.25. [Online]. Elérhető: https://www.thestreet.com/investing/tesco-shares-drop-on-bank-hack-13882530

[271] M. Kumar, ‘Tesco Bank Hacked — Cyber Fraudsters Stole Money From 20,000 Accounts’, The Hacker News, 2016.11.07. Hozzáférés: 2022.04.25. [Online]. Elérhető: https://thehackernews.com/2016/11/tesco-bank-hack.html

[272] Financial Conduct Authority, ‘FCA fines Tesco Bank £16.4m for failures in 2016 cyber attack’. Hozzáférés: 2022.04.25. [Online]. Elérhető: https://www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack

[273] A. Damodaran, ‘Data:Archives, Discount Rate Estimation’. Hozzáférés: 2022.06.12. [Online]. Elérhető: https://pages.stern.nyu.edu/~adamodar/New_Home_Page/dataarchived.html#discrate

[274] D. Wolpoff, ‘After the FireEye and SolarWinds breaches, what’s your failsafe?’, TechCrunch, 2020.12.21. [Online]. Elérhető: https://techcrunch.com/2020/12/21/after-the-fireeye-and-solarwinds-breaches-whats-your-failsafe

[275] S. Oladimeji és S. M. Kerner, ‘SolarWinds hack explained: Everything you need to know’, TechTarget, 2021.06.16. Hozzáférés: 2022.05.02. [Online]. Elérhető: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[276] SolarWinds, ‘Form 10-K 2019’. Hozzáférés: 2022.05.02. [Online]. Elérhető: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm

[277] I. Jibilian és K. Canales, ‘The US is readying sanctions against Russia over the SolarWinds cyber attack. Here’s a simple explanation of how the massive hack happened and why it’s such a big deal’, Insider, 2021.04.15. Hozzáférés: 2022.05.02. [Online]. Elérhető: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

[278] S. Shah, ‘The Financial Impact of SolarWinds Breach’, BitSight, 2021.01.12. Hozzáférés: 2022.06.11. [Online]. Elérhető: https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided

[279] SolarWinds, ‘Form 10-K 2020’. Hozzáférés: 2022.06.11. [Online]. Elérhető: https://www.sec.gov/Archives/edgar/data/1739942/000173994221000043/swi-20201231.htm

[280] SolarWinds, ‘Form 10-Q’, 2021.09. Hozzáférés: 2022.06.11. [Online]. Elérhető: https://www.sec.gov/Archives/edgar/data/0001739942/000173994221000154/swi-20210930.htm

[281] G. Ratnam, ‘Cleaning up SolarWinds hack may cost as much as $100 billion’, Roll Call, 2021.01.11. Hozzáférés: 2022.06.11. [Online]. Elérhető: https://rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/

[282] M. Akbanov, V. G. Vassilakis és M. D. Logothetis, ‘WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms’, Journal of Telecommunications and Information Technology, vol. 1, no. 2019, pp. 113–124, 2019.04., doi: 10.26636/jtit.2019.130218.

[283] L. Rosencrance, ‘WannaCry ransomware’, TechTarget, 2021.09. Hozzáférés: 2022.06.16. [Online]. Elérhető: https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware

[284] S. Barlyn, ‘Global cyber attack could spur $53 billion in losses: Lloyd’s of London’, Reuters, 2017.07.17. Hozzáférés: 2022.06.16. [Online]. Elérhető: https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB

[285] National Audit Office, ‘Investigation: WannaCry cyber attack and the NHS’, 2018.04. Hozzáférés: 2019.03.15. [Online]. Elérhető: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

[286] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi és P. Aylin, ‘A retrospective impact analysis of the WannaCry cyberattack on the NHS’, NPJ Digit Med, vol. 2, no. 1, p. 98, 2019.12., doi: 10.1038/s41746-019-0161-6.

[287] Krasznay Cs., ‘Case Study: The NotPetya Campaign’, in Információ- és kiberbiztonság, T. Bernát, Ed., Ludovika Egyetemi Kiadó, 2020, pp. 485–499. Hozzáférés: 2022.06.17. [Online]. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf

[288] A. Hern, ‘Hackers who targeted Ukraine clean out bitcoin ransom wallet’, The Guardian, 2017.07.05. Hozzáférés: 2022.06.17. [Online]. Elérhető: https://www.theguardian.com/technology/2017/jul/05/notpetya-ransomware-hackers-ukraine-bitcoin-ransom-wallet-motives

[289] A. Greenburg, ‘The Untold Story of NotPetya, the Most Devastating Cyberattack in History’, Wired, 2018.08.22. Hozzáférés: 2022.06.17. [Online]. Elérhető: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[290] C. Pownall, ‘The Context and Impact of Maerk’s NotPetya cyber attack’. Hozzáférés: 2022.06.17. [Online]. Elérhető: https://www.researchgate.net/publication/346080185_The_Context_and_Impact_of_Maerk’s_NotPetya_cyber_attack

[291] M. van Hees, ‘The 2017 MAERSK Cyber Incident’. Hozzáférés: 2022.07.17. [Online]. Elérhető: https://fhi.nl/app/uploads/sites/75/2020/10/201029-FHI_Maersk.pdf

[292] E. Sagonowsky, ‘Merck, insurers fight over $1.3B in damages from cyberattack: Bloomberg’, Fierce Pharma. Hozzáférés: 2022.06.18. [Online]. Elérhető: https://www.fiercepharma.com/pharma/merck-insurers-fight-over-1-3-billion-damages-from-cyberattack-bloomberg

[293] M. Erman és J. Finkle, ‘Merck says cyber attack halted production, will hurt profits’, Reuters, 2017.07.28. Hozzáférés: 2022.06.18. [Online]. Elérhető: https://www.reuters.com/article/us-merck-co-results/merck-says-cyber-attack-halted-production-will-hurt-profits-idUSKBN1AD1AO

[294] Merck, ‘Form 10-K’. Hozzáférés: 2022.06.18. [Online]. Elérhető: https://www.sec.gov/Archives/edgar/data/310158/000031015819000014/mrk1231201810k.htm

[295] Merck & Co. Inc. v. ACE American Ins. Co., UNN-L-002682-18. US: N.J. Super. Ct. Law Div., 2022. Hozzáférés: 2023.02.28. [Online]. Elérhető: https://www.documentcloud.org/documents/21183337-merck-v-ace-american

[296] The Guardian, ‘Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach’, 2018.03.17. [Online]. Elérhető: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[297] Business Insider, ‘Facebook understood how dangerous the Trump-linked data firm Cambridge Analytica could be much earlier than it previously said. Here’s everything that’s happened up until now.’, 2019. Hozzáférés: 2023.02.22. [Online]. Elérhető:

https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3

[298] S. Meredith, 'Facebook-Cambridge Analytica: A timeline of the data hijacking scandal', CNBC, 2018.04.10. Hozzáférés: 2023.03.01. [Online]. Elérhető: https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

[299] CNBC, 'Here are the scandals and other incidents that have sent Facebook's share price tanking in 2018', 2018.10.20. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://www.cnbc.com/2018/11/20/facebooks-scandals-in-2018-effect-on-stock.html

[300] MarketWatch, 'Facebook stock drops roughly 20%, loses $120 billion in value after warning that revenue growth will take a hit', 2018. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://www.marketwatch.com/story/facebook-stock-crushed-after-revenue-user-growth-miss-2018-07-25

[301] Business Insider, 'Facebook just announced it was hacked, and almost 50 million users have been affected'. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://www.businessinsider.com.au/facebook-security-attack-affecting-50-million-users-2018-9

[302] International Business Times, 'Facebook Stock Suffers Biggest Drop Of 2019, Loses $37B In 4 Trading Days', 2019.03.18. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://www.ibtimes.com/facebook-stock-suffers-biggest-drop-2019-loses-37b-4-trading-days-2776826

[303] Liao Shannon, 'Facebook, Instagram, and WhatsApp are still down for some users around the world', The Verge, 2019.03.13. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://www.theverge.com/2019/3/13/18264092/facebook-instagram-down-partially-post-messages-profile-loading

[304] Facebook, 'Keeping Passwords Secure'. Hozzáférés: 2020.08.10. [Online]. Elérhető: https://about.fb.com/news/2019/03/keeping-passwords-secure/

[305] Markets Insider, 'Facebook shares drop sharply after unearthed emails reportedly show Mark Zuckerberg is aware of "problematic privacy practices"', 2019.06.12. Hozzáférés: 2021.03.01. [Online]. Elérhető: https://markets.businessinsider.com/news/stocks/facebook-stock-price-reaction-to-zuckerberg-reportedly-aware-privacy-issues-2019-6-1028274446

[306] Information Commissioner's Office, 'Statement on an agreement reached between Facebook and the ICO'. Hozzáférés: 2023.02.28. [Online]. Elérhető: https://www.wired-

gov.net/wg/news.nsf/articles/Statement+on+an+agreement+reached+between+Facebook+and+the+ICO+30102019151000?open

[307] Federal Trade Commission, 'FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook'. Hozzáférés: 2020.08.10. [Online]. Elérhető: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

[308] Facebook, 'FTC Agreement Brings Rigorous New Standards for Protecting Your Privacy'. Hozzáférés: 2020.11.08. [Online]. Elérhető: https://about.fb.com/news/2019/07/ftc-agreement/

[309] Techcrunch, 'A huge database of Facebook users' phone numbers found online', 2019.09.04. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/

[310] CNBC, 'Facebook stock rises on better-than-expected revenue and earnings', 2019.10.30. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://www.cnbc.com/2019/10/30/facebook-fb-q3-2019-earnings.html

[311] Competition Bureau Canada, 'Facebook to pay $9 million penalty to settle Competition Bureau concerns about misleading privacy claims'. Hozzáférés: 2021.01.08. [Online]. Elérhető: https://www.canada.ca/en/competition-bureau/news/2020/05/facebook-to-pay-9-million-penalty-to-settle-competition-bureau-concerns-about-misleading-privacy-claims.html

[312] HmbBfDI, 'Tätigkeitsbericht datenschutz 2019'. Hozzáférés: 2021.03.06. [Online]. Elérhető: https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf

[313] Facebook, 'Form 10-K 2019'. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://s21.q4cdn.com/399680738/files/doc_financials/2019/ar/2019-Annual-Report.pdf

[314] Facebook, 'Form 10-K 2016'. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2016_FINAL.pdf

[315] Facebook, 'Form 10-K 2017'. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2017_FINAL.pdf

[316] Facebook, 'Form 10-K 2018'. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/2018-Annual-Report.pdf

[317] Facebook, 'Form 10-K 2020'. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://s21.q4cdn.com/399680738/files/doc_financials/2020/ar/2020-Annual-Report.pdf

[318] A. Damodaran, ‘Historical Returns on Stocks, Bonds and Bills: 1928-2020’. Hozzáférés: 2021.07.09. [Online]. Elérhető: https://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/histretSP.html

[319] MSCI, ‘MSCI ACWI Index (USD)’. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://www.msci.com/documents/10199/8d97d244-4685-4200-a24c-3e2942e3adeb

[320] International Monetary Fund, ‘Interest Rates, Government Securities, Government Bonds for United States’. Hozzáférés: 2023.02.01. [Online]. Elérhető: https://fred.stlouisfed.org/series/INTGSBUSM193N#

[321] Coin News, ‘Current US Inflation Rates: 2000-2021’. Hozzáférés: 2021.03.06. [Online]. Elérhető: https://www.usinflationcalculator.com/inflation/current-inflation-rates/

[322] Yahoo! Finance, ‘Meta Platforms, Inc. (META)’. Hozzáférés: 2023.01.07. [Online]. Elérhető: https://finance.yahoo.com/quote/FB/history

[323] Yahoo! Finance, ‘S&P 500 (^GSPC)’. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://finance.yahoo.com/quote/%5EGSPC/history?p=%5EGSPC%0A

[324] J. H. Ahn, ‘The impact of the banking competition in funding and lending markets on lending technology’, Revue Economique, vol. 67, no. 6, pp. 1117–1139, 2016, doi: 10.3917/reco.pr2.0069.

[325] Statista, ‘IT budgets & investments’. Hozzáférés: 2021.01.28. [Online]. Elérhető: https://www.statista.com/study/71560/it-budgets-and-investments/

[326] Flexera, ‘State of tech spend report’. Hozzáférés: 2021.03.14. [Online]. Elérhető: https://info.flexera.com/SLO-REPORT-State-of-Tech-Spend

[327] J. Bernard, D. Golden és M. Nicholson, ‘Reshaping the cybersecurity landscape’, Deloitte Insights. Hozzáférés: 2021.03.20. [Online]. Elérhető: https://www.fsisac.com/hubfs/DI_2020-FS-ISAC-Cybersecurity.pdf

[328] J. Roettgers, ‘Mark Zuckerberg Says Facebook Will Spend More Than $3.7 Billion on Safety, Security in 2019’, Variety, 2019.02.05. Hozzáférés: 2021.03.06. [Online]. Elérhető: https://variety.com/2019/digital/news/facebook-2019-safety-speding-1203128797/

[329] S. Armitage, ‘Event study methods and evidence on their performance’, J Econ Surv, vol. 9, no. 1, pp. 25–52, 1995, doi: 10.1111/j.1467-6419.1995.tb00109.x.

[330] T. S. Breusch és A. R. Pagan, ‘A Simple Test for Heteroscedasticity and Random Coefficient Variation’, Econometrica, vol. 47, no. 5, pp. 1287–1294, Sep. 1979, doi: 10.2307/1911963.

[331] E. I. Obilor és E. C. Amadi, ‘Test for significance of Pearson’s correlation coefficient’, International Journal of Innovative Mathematics, Statistics & Energy Policies, vol. 6, no. 1, pp. 11–23, 2018.

A tézispontokhoz kapcsolódó tudományos közlemények

[BZs1] Bederna Zs., ‘Bizalom és megbízhatóság’, Katonai Nemzetbiztonsági Szoglálat, vol. XVII., no. 1., pp. 135–149, 2019, [Online]. Elérhető: https://www.knbsz.gov.hu/hu/letoltes/szsz/2019_1_szam.pdf

[BZs2] Bederna Zs., ‘Critical Information and Communications Technology protection’, in Kiberbiztonság-Cybersecurity 2, Rajnai Z., Ed., Biztonságtudományi Doktori Iskola, 2019, pp. 137–146. [Online]. Elérhető: https://bdi.uni-obuda.hu/sites/default/files/oldal/csatolmany/kiadvany-2019.pdf

[BZs3] Bederna Zs., Rajnai Z. és Szádeczky T., ‘Further Strategy Analysis of Cybersecurity Incidents’, Land Forces Academy Review, vol. 26, no. 3, pp. 251–260, 2021, doi: 10.2478/raft-2021-0032.

[BZs4] Bederna Zs. és Rajnai Z., ‘Review of the advancement of critical information infrastructures and their structural analysis’, National Security Review, pp. 166–175, 2020.

[BZs5] Bederna Zs., ‘Az Általános adatvédelmi rendelet és az információbiztonság kapcsolódási pontjai’, Szakmai Szemle, vol. XVI., no. 3., pp. 76–103, 2018.

[BZs6] Bederna Zs. és Rajnai Z., ‘Analysis of the cybersecurity ecosystem in the European Union’, International Cybersecurity Law Review, vol. 3, pp. 35–49, 2022, doi: 10.1365/s43439-022-00048-9.

[BZs7] Bederna Zs. és Szádeczky T., ‘Cyber espionage through Botnets’, Security Journal, vol. 33, pp. 43–62, 2019, doi: 10.1057/s41284-019-00194-6.

[BZs8] Bederna Zs. és Rajnai Z., ‘Analysis of static and dynamic parameters of players in cyberspace’, in Eighth International Scientific Web-conference of Scientists and PhD. students or candidates, in Trends and Innovations in E-business, Education and Security. Budapest: Obuda University, 2020, pp. 65–80.

[BZs9] Bederna Zs. és Szádeczky T., ‘Effects of botnets – a human-organisational approach’, Security and Defence Quarterly, vol. 35, no. 3, pp. 25–44, 2021, doi: 10.35467/sdq/138588.

[BZs10] Bederna Zs. és Szadeczky T., ‘Industry 4.0-based critical infrastructure and the NIS Directive’, in Central and Eastern European eDem and eGov Days, New York, NY, USA: ACM, 2022, pp. 93–99. doi: 10.1145/3551504.3551546.

[BZ11]Szádeczky T. és Bederna Zs., ‘The Economic Measurement of Cyber Incidents’, Periodica Polytechnica Social and Management Sciences, 2023, doi: 10.3311/PPso.22150.

[BZs12] Bederna Zs., Rajnai Z. és Szádeczky T., ‘Attacks against energy, water and other critical infrastructure in the EU’, in 2020 IEEE 3rd International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE), IEEE, 2021, pp. 000125–000130. doi: 10.1109/cando-epe51100.2020.9337751.

[BZs13] Bederna Zs. és Szádeczky T., ‘Managing the financial impact of cybersecurity incidents’, Security and Defence Quarterly, vol. 41, no. 1, 2023, doi: 10.35467/sdq/159625.

[BZs14] Bederna Zs., Rajnai Z. és Szadeczky T., ‘Business Strategy analysis of Cybersecurity Incidents’, Land Forces Academy Review, vol. 26, no. 2, pp. 139–148, 2021, doi: 10.2478/raft-2021-0020.

[BZs15] Bederna Zs., ‘Analysing the Financial Impact of Cybersecurity Incidents’, Open Science Foundation. 2023. doi: 10.17605/OSF.IO/ZEM8Y.

További tudományos közlemények

[BZs16] Bederna Zs. és Szádeczky T., ‘Modelling computer networks for further security research’, Security and Defence Quarterly, vol. 36, no. 4, pp. 51–66, 2021, doi: 10.35467/sdq/141572.

[BZs17] Bederna Zs., ‘Fuzzy-based intrusion detection’, Hadmérnök, vol. 10, no. 1, pp. 147–160, 2015, Hozzáférés: 2024.03.11. [Online]. Elérhető: http://hadmernok.hu/151_14_bedernazs.pdf

[BZs18] Bederna Zs., ‘Az informatikai eszközök használatával kapcsolatos attitűdök az egyetemi hallgatók körében ma Magyarországon’, Információs Társadalom, vol. 12, no. 4, p. 106, 2012, doi: 10.22503/inftars.XII.2012.4.4.

[BZs19] Bederna Zs., Váczi D., Pollner P. és Szádeczky T., ‘Támadás hálózatba szervezve’, in Hálózatok a közszolgálatban, Auer Á. és Joó T., Eds., Budapest: Dialóg Campus Kiadó, 2019, pp. 223–247.

[BZs20] Váczi D., Bederna Zs., Szalánczi-Orbán V. és Szádeczky T., ‘Az incidenskezelés szervezeti háttere’, in Hálózatok a közszolgálatban, Auer Á. és Joó T., Eds., Budapest: Dialóg Campus Kiadó, 2019, pp. 205–222.

RÖVIDÍTÉSJEGYZÉK

Rövidítés	Magyarnyelvű feloldás	Idegen nyelvi feloldás
APT	fejlett perzisztens fenyegetés	advanced persistent threat
ATT&CK		Adversarial Tactics, Techniques and Common Knowledge
BSI	Német Szövetségi Információbiztonsági Hivatal	Bundesamt für Sicherheit in der Informationstechnik
C&C		Command and Control
CEPOL	Európai Unió Bűnüldözési Képzési Ügynöksége	The European Union Agency for Law Enforcement Training
CER	a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv	resilience of critical entities
CERT-EU		Computer Emergency Response Team for the EU institutions, bodies and agencies
CIRAS		Cybersecurity Incident Reporting and Analysis System
CKC		Cyber Kill Chain
CPS	kiber-fizikai rendszerek	Cyber-Physical Systems
DESI	Digitális Gazdaság és Társadalom Index	Digital Economy and Society Index
DHCP		Dynamic Host Configuration Protocol
DNC	Egyesült Államok Demokrata Nemzeti Bizottsága	Democratic National Committee
DORA	a pénzügyi ágazat digitális működési rezilienciájáról szóló rendelet	digital operational resilience for the financial sector
DoS	túlterheléses támadás	denial of service
DREAD		Damage Potential, Reproducibility, Exploitability, Affected Users and Discoverability
DSP	digitális szolgáltatók	digital service provider
EC3	az Európai Unió bűnüldöző ügynökségének szervezetén belül létrejött Számítástechnikai Bűnözés Elleni Európai Központ	European Cybercrime Centre
ECCC	Európai Elektronikus Hírközlési Kódex	European Electronic Communications Code
ECCC	Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont	European Cybersecurity Competence Centre
EDA	Európai Védelmi Ügynökség	European Defence Agency
EEAS	Európai Külügyi Szolgálat	European External Action Service
EGT	Európai Gazdasági Térség	European Economic Area (EEA)

eIDAS	elektronikus tranzakciókhoz kapcsolódó elektronikus azonosítás és bizalmi szolgáltatások	electronic identification and trust services
ENISA	Európai Uniós Kiberbiztonsági Ügynökség	European Union Agency for Cybersecurity
	Európai Uniós Hálózat- és Információbiztonsági Ügynökség	European Network and Information Security Agency
EP3R	Európai köz- és magánszféra együttműködés az ellenállóképességért	European Public-Private Partnership for Resilience
ETSI	Európai Távközlési Szabványügyi Intézet	European Telecommunications Standards Institute
EU	Európai Unió	European Union
Eurofisc	Európai Unió tagállamainak együttműködését támogató nemzetközi adatcsere mechanizmus	A multilateral warning system of the Member States for combating VAT fraud
Eurojust	Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége	European Union Agency for Criminal Justice Cooperation
Europol	Európai Rendőrségi Hivatal	European Police Office
EU-CyCLONe	Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata	European cyber crisis liaison organisation network
GDPR	Általános adatvédelmi rendelet (Az Európai Parlament és a Tanács (EU) 2016/679 rendelete)	General Data Protecion Regulation
Kibertan. tv.	2023. évi XXIII. törvény	
Ibtv.	2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról	
IDPS	behatolás detektáló és megelőző rendszer	Intrusion Detection and Prevention System
IETF		Internet Engineering Task Force
IODEF		Incident Object Description Exchange Format
IVBB	Berlin és Bonn között szövetségi hálózatban	Informationsverbund Berlin-Bonn
JIT	éppen-időben	just in time
JSON		JavaScript Object Notation
KBVP	közös biztonság- és védelempolitika	Common Security and Defence Policy (CSDP)
KKBP	Európai Unió közös kül- és biztonságpolitikájára	common foreign and security policy (CFSP)
MAEC		Malware Attribute Enumeration and Characterization
MISP		Malware Information Sharing Platform

NATO	Észak-atlanti Szerződés Szervezete	North Atlantic Treaty Organisation
NATO CCDCOE	NATO Kooperatív Kibervédelmi Kiválósági Központ	NATO Cooperative Cyber Defence Centre of Excellence
NCCs	koordinációs központok hálózat	Network of National Coordination Centres
NHS	Angol és skót Nemzeti Egészségügyi Szolgálat	National Health Services
NIST	Nemzeti Szabványügyi és Technológiai Intézet, Egyesült Államok	National Institute of Standards and Technology
NIST SP		NIST Special Publication
OES	alapvető szolgáltatásokat nyújtó szereplő	operator of essential services
OpenIOC		Open Indicators of Compromise
OpenTPX		Open Threat Partner Exchange
PASTA		Process for Attack Simulation and Threat Analysis
PESCO	állandó strukturált együttműködés	Permanent Structured Cooperation
PSD2	Megjegyzés: Európai Parlament és a Tanács (EU) 2015/2366 irányelve	Second Payment Services Directive
SIEM	biztonsági információs és eseménykezelő rendszer	Security Information and Event Management
SOAR	Kibertámadások elhárítása automatizált megoldásokkal	Security Orchestration, Automation and Response
SOC	biztonsági műveleti központ	Security Operation Centre
STIX		Structured Threat Information eXpression
STRIDE		Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege
TAXII		Trusted Automated eXchange of Indicator Information
TC		Technical Committee
TIP	fenyegetés intelligencia platformon	Threat Intelligence Platform
TTP	taktikák, technikák és folyamatok	tactics, techniques, and procedures
UEBA	felhasználói és entitás-viselkedéselemzési elemzés	User and Entity Behaviour Analytics
UML		Unified Modeling Language
VERIS		Vocabulary for Event Recoding and Incident Sharing
Vhr.	végrehajtási rendelet	
XML		Extensible Markup Language

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

FÜGGELÉK

1. függelék A gazdasági elemzések alapvető eszközei

A vállalkozások számára a pénzáramok (cash flow – CF) [227] megléte jelenti a pénzügyi funkcióik egyik alapját, amely az adott szervezet szempontjából tekintett be- vagy kiáramló készpénz vagy készpénz-egyenértékes összeget jelent. Az elemzés tárgya egy vállalat, egy üzleti funkció vagy egy projekt is lehet. A vizsgált időszakra vonatkozó pénzáramot a záró egyenlegből és a nyitó egyenleg különbsége reprezentálja. A pénzáram pozitív, ha a különbség eredménye nagyobb nullánál, ekkor a beáramló összeg nagyobb, mint a kiáramló összeg, illetve a pénzáram negatív, ha a kiáramló összeg nagyobb a befolyó összeghez képest. A negatív pénzáramok likviditási problémákat okozhatnak, megakadályozva a szervezetet abban, hogy az esedékes pénzügyi kötelezettségeit teljesítse. Minél kisebb időegység kerül vizsgálatra, annál pontosabb lehet a likviditáselemzés.

A nettó jelenérték (net present value – NPV) [229] a különböző időpontokban előforduló pénzáramok sorozatára vonatkozóan határozza meg azok jelenértékét, amely a jövőbeni pénzáramoktól, valamint a diszkontrátától függ. Az NPV a pénzügyi tevékenységek (projektek, vállalatok) értékelésének egyik alapvető eszköze, amely a következőképp számítandó:

$$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+r)^t} \tag{19}$$

ahol CF_t az adott pénzáram, r a kamatláb. A fenti megközelítés az évenként megegyező kamatláb esetén alkalmazandó, ellenkező esetben az egyszerűsített összegzést szét kell bontani a tagokra:

$$NPV = \frac{CF_1}{(1+r_1)} + \frac{CF_2}{(1+r_1)(1+r_2)} + \cdots \frac{CF_t}{(1+r_1)(1+r_2)\cdots(1+r_t)} \tag{20}$$

A nevező tagokat az összegzésen belüli szorzatként megadva adódik a következő formula:

$$NPV = \sum_{t=1}^{n} \frac{CF_t}{\prod_{i=1}^{t}(1+r_i)} \tag{21}$$

A képlet a pénzáramok éves bontású vizsgálatát szemlélteti. Az egy éven belüli vizsgálatok során a pontosabb eredmény elérése végett az e^{ri} effektív kamatlábat szükséges alkalmazni, ahol i az eltelt napok számának és az év napjainak hányadosa.

A pénzáramok jövőben értékét, ennek megfelelően múltbeli pénzáramok jelenértékét a nettó jövőbeli érték (net future value – NFV) mutató alapján lehetséges meghatározni az alábbi formula alkalmazásával évvégi pénzáramok feltételezése mellett, ahol a vizsgálat időpontja az utolsó év vége (az utolsó pénzáram megtörténte):

$$NFV = \text{NPV} * (1+r)^n = \sum_{t=1}^{n} \left(\frac{CF_t}{(1+r)^t} \right) * (1+r)^n$$
$$= \sum_{t=1}^{n-1} (CF_t * (1+r)^{n-t}) + CF_n \quad (22)$$

Az éves kamatlábak eltérése esetén a fenti egyszerűsített képletből a következő formula adódik:

$$NFV = \sum_{t=1}^{n-1} \left(CF_t * \prod_{i=t}^{n-1} (1 + r_{i+1}) \right) + CF_n \quad (23)$$

Bár az NPV és NFV számítások a pénzügyi elemzések elengedhetetlen eszközei, rendelkeznek hátrányokkal is. A mutatók igen érzékenyek a pénzáramok és a kamatlábak minél pontosabb meghatározására [235].

Pénzáram meghatározása során a számviteli alapelvekre érdemes építeni, így az ügylet jellegétől függően a működési, befektetési vagy finanszírozási tevékenységek szerint többféle pénzáramot kell megkülönböztetni [228]. A működési cash flow a vállalkozás fő bevételteremtő tevékenységeiből adódik, a nettó árbevételt meghatározó kapcsolódó tevékenységekből adódik, beleértve a bevételeket és kiadásokat, mint például az áruk értékesítéséből származó vagy az áruért kifizetett pénzeszköz. A befektetési cash flow a befektetett eszközökkel kapcsolatos pénzforgalmi tevékenységeket takarja, beleértve a hosszú távú befektetéseket, az ingatlanokat, gépeket és berendezéseket és a más gazdálkodó egységeknek nyújtott hitelek tőkeösszegét vagy épp a kapott osztalékot. A finanszírozási cash flow a fő változásokat mutatja a tőkében, hitelekben a pénzáramok és összetétel tekintetében egyaránt. A finanszírozási tevékenységek magukban foglalják a hosszú lejáratú kötelezettségeket és a saját tőkével kapcsolatos készpénzes tevékenységeket, beleértve például a hosszú lejáratú adósság tőkeösszegét, a részvénykibocsátásokat és -visszavásárlásokat.

A vállalati (asset – A), a részvényesek (equity – E) és a hitelezői (debt – D) pénzáramok értéke különbözik, amelyek megkülönböztetést igényelnek a tőkeköltségen alapuló kamatszámítás pénzügyi hatásainak vizsgálatakor. A részvényesek tőkeköltségének kiszámítására több lehetőség is kínálkozik, amelyekből a Capital Asset Pricing Model (CAPM) [236] egy prominens megoldás, melyet Elbannan [237] részletesen tárgyal. A CAPM alapján a tőkeköltség a következő formula alapján adódik:

$$r_E = r_f + \beta(r_M - r_f) \quad (24)$$

ahol r_E tulajdonosi kamatláb, r_f a kockázatmenetes kamatláb, r_M piaci portfólió kamatláb, $r_{f,nom}$ nominális kockázatmentes kamatláb, β (béta) az adott részvények volatilitásának mértéke a teljes piac szisztematikus kockázatához viszonyítva. A fenti egyenletben a $\beta(r_M - r_{f,nom})$ szorzat azt a kockázati prémiumot jelenti, amelyet a befektetők egy adott részvény vagy portfólió birtoklásától

elvárnak a kockázatmentes eszközök hozamán felül. Ugyanakkor egy, a tőzsdén nem jegyzett vállalat magasabb kockázattal működik a tőzsdén működő ugyanolyan vagy hasonló vállalathoz képest, amelyet a teljes béta (total beta) [238] reprezentál:

$$\beta_T = \beta_M * p_{jM} \tag{25}$$

ahol β_T a totál béta, β_M piaci portfólió béta, p_{jM} a részvény és a piaci portfólió közötti korreláció.

A faktormodellek olyan statisztikai modellek, amelyek a tőkeköltség alakulását megmagyarázni több tényező alkalmazásával a CAPM egyváltozós modelljével szemben, amelyek például piaci anomáliák vagy makroökonómiai tényezőkre reagálnak. Neves faktormodell Fama-Franch 3 faktor modell [240], Carhart 4 faktor modell [241], Pastor-Stambaugh 5 faktor modell [242], Fama-French 5 faktoros modell [243].

A tőkeköltség meghatározása során további figyelembe veendő szempont, hogy egy vállalat a saját tőkén (E) kívül hitelt (D) is igénybe vehet. Adósság nélkül ($D = 0$) egy szervezetet tőkeáttétel nélkülinek (unlevereged) kell tekinteni, egyébként tőkeáttételes (levereged). Egy tőkeáttételes társaságnál a súlyozott átlagos tőkeköltséget (weighted-average cost of capital – WACC) kell figyelembe venni [239], amelyet a következőképp kell meghatározni:

$$r_{wacc} = \frac{E}{E+D} * \mathrm{E}(r_E) + (1 - t_c) * \frac{D}{E+D} * E(r_D) \tag{26}$$

ahol r_{wacc} a tőkeáttételes kamatláb (WACC), $E(\cdot)$ a várható érték (expected value), E a tulajdonosi érték, D a hitelezői érték, r_E a tulajdonosi kamatláb (mint korábban), r_D a hitelezői kamatláb, t_c a társasági adó.

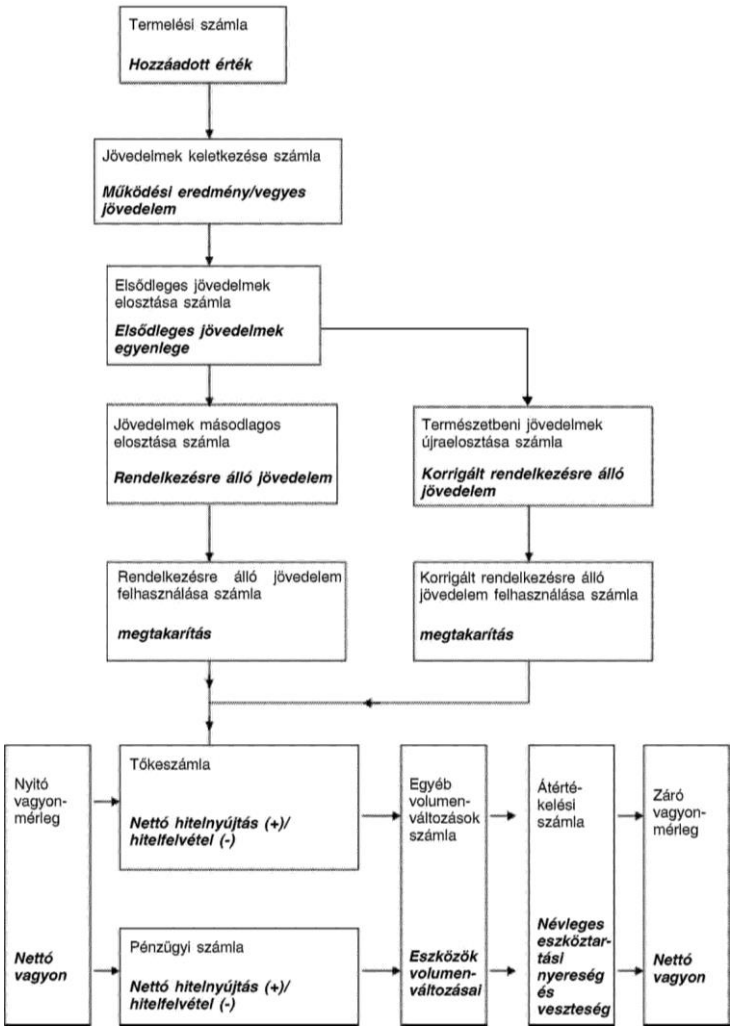
A kormányzati projektekkel összefüggésben a kamatlábak meghatározására két számítási modell áll rendelkezésre, ezek a társadalmi időpreferencia (social rate of time preference – SRTP) és a társadalmi lehetőségköltség (social opportunity cost of capital – SOC) [245]. Az SRTP kiszámításának általánosan elfogadott módszere a Ramsey-képlet [244], amely két komponensből áll:

$$S = p + eg \tag{27}$$

ahol S a társadalmi diszkontráta, p a hasznosság diszkontrátája, e a fogyasztás határhasznának rugalmassága, g az egy főre jutó növekedés várható üteme. A SOC modell a magán- és állami projektek erőforrásokért történő versenyeztetésén alapul annak érdekében, hogy az állami projektek hozama ne essen a konkurens magánprojektek hozama alá, különben a közösségi jólét a források átcsoportosítását igényelné [245]. A SOC értékére több becslés is létezik, például a kiváló minőségű vállalati kötvények [246] és a kockázatmentes magánbefektetések adózás előtti marginális megtérülési rátája [247].

2. függelék Nemzeti számlák európai rendszere

A nemzeti számlák európai rendszere (European System of Accounts – ESA) 2010, azaz ESA 2010 [265] rendszer az egymással összefüggő számlák sorozatára, a nemzetgazdaság integrált számláira épül (***16***. ábra), melyek folyó számlákból, felhalmozási számlákból és vagyonmérlegekből tevődnek össze. A folyó számlák a jövedelem termelésével, keletkezésével, elosztásával és újraelosztásával, valamint a jövedelemnek a végső fogyasztás formájában történő felhasználásával foglalkoznak. A felhalmozási számlák az eszközök és kötelezettségek, továbbá a gazdasági egységnél vagy egységcsoportnál az eszközök és kötelezettségek különbségének, azaz a nettó vagyon változását tartalmazzák. A vagyonmérlegek az eszközök és kötelezettségek, valamint a nettó vagyon állományát reprezentálják. A sorozat fontos eleme az egyes számlák egyenlegező tétele, amely a számla egyik oldalán lévő tételek összértékéből és a számla másik oldalán szereplő összérték különbsége.



16. ábra. ESA 2010 számlák sorozata
Forrás: [266]

Az ESA 2010 első számlája a termelési folyamat kibocsátását és ráfordításait elszámoló termelési számla egyenlegező tételként a hozzáadott értéket eredményezve. A második a jövedelmek keletkezése számla, amely a termelési folyamat során keletkező munkavállalói jövedelmeket és a termelés miatt a kormányzatnak fizetendő adókat számolja el, aminek eredményeként a szektoronkénti működési eredmény vagy a háztartási szektor önálló vállalkozóinak vegyes jövedelme egyenlegező tétel áll elő. Ezt követően a hozzáadott értéket munkavállalói jövedelem, adók és működési eredmény, illetve vegyes jövedelem lebontásban az elsődleges jövedelmek eloszlása számla dolgozza fel, egyenlegező tételként a szektorba beáramló elsődleges jövedelem egyenlegét megadva. A jövedelmek másodlagos eloszlása számla a jövedelmek transzferek útján megvalósított újraelosztását tartja nyilván, a rendelkezésre álló jövedelem egyenlegező tételt eredményezve. A rendelkezésre álló jövedelem felhasználása számla a háztartási szektor esetében a háztartások végső kiadását számolja el, megadva a háztartások megtakarításai egyenlegező tételt. Ezzel párhuzamosan a természetbeni jövedelmek újraelosztása számla az államháztartásból a háztartási szektornak juttatott természetbeni társadalmi juttatásokat tartalmazza, amelyet a korrigált rendelkezésre álló jövedelem felhasználása számla dolgozza fel a megtakarítás egyenlegező tételt megadásával. Ez azonos a számlák fő sorozatában szereplő megtakarítással.

A megtakarításokat a tőkeszámla dolgozza fel, lehetővé téve a szektorokból kiáramló, illetve szektorokba beáramló tőketranszfereket, nyilvántartva a megtakarításhoz viszonyított alulköltekezést vagy túlköltekezést, amely az egyenlegező tételben megjelenő nettó hitelnyújtáshoz vagy hitelfelvételhez vezet. Végül a pénzügyi számlákban minden egyes szektor részletes hitelnyújtása és hitelfelvétele jelenik meg, a nettó hitelnyújtást vagy hitelfelvételt egyenlegező tételt eredményezve, amely alapvetően megegyezik a tőkeszámla nettó hitelnyújtás/hitelfelvétel egyenlegező tételével.

A nyitó vagyonmérleg az összes eszköz és kötelezettség szintjét mutatja egy meghatározott időszak kezdetén, amely az eszközök és kötelezettségek egyenlegével megadja az adott gazdaság nettó vagyonát. Az eszközöknek és kötelezettségeknek az elszámolási időszak alatt történő különböző változásai a nyitó vagyonmérleg alapján a tőkeszámlán, illetve a pénzügyi számlán kerülnek elszámolásra. A tőkeszámla a reáleszközöket és -kötelezettségeket, a pénzügyi számla pedig a pénzügyi eszközöket és kötelezettségeket érintő gazdasági műveletek miatt bekövetkezett változásokat mutatja ki. Az eszközök nem gazdasági cseretranzakciók vagy transzferek (pl. természeti katasztrófa) miatti volumenváltozás kapcsán a veszteséget az „eszközök egyéb volumenváltozásai” számlán kell elszámolni. Továbbá az eszközök és kötelezettségek értékében gazdasági műveletek eredményeként bekövetkező változástól eltérő változást okozhat az árváltozás, amely az eszközállomány tekintetében eszköztartási nyereséget és veszteséget eredményez. Ezt a változást az

átértékelési számlákban kell elszámolni. Mindezek együttesen teszik lehetővé a záró vagyonmérleg értékeinek megbecslését.

A számlák által biztosított nyilvántartások alapján az aggregátumok a teljes gazdaság tevékenységének eredményét mérik: (1) közvetlenül a gazdasági műveletekre utaló aggregátumok (pl. javak és szolgáltatások kibocsátása, végső fogyasztás, bruttó állóeszköz-felhalmozás, munkavállalói jövedelmek stb.), (2) a számlákban egyenlegező tételeket jelentő aggregátumok (pl. bruttó hazai termék piaci áron, teljes gazdaság működési eredménye, bruttó nemzeti jövedelem, rendelkezésre álló nemzeti jövedelem, megtakarítás, folyó külső egyenleg, teljes gazdaság nettó vagyona).

A teljes gazdaság nettó vagyona (nemzeti vagyon) egy meghatározott időpontban mért nem pénzügyi eszközök és a külfölddel szembeni nettó pénzügyi eszközök összértéke. A bruttó hazai termék (gross domestic product – GDP), mint kiemelt aggregátum, egy gazdasági területen belül a teljes gazdasági tevékenységet méri, mely a gazdaság eredeti keresletét kielégítő kibocsátást biztosítja. Mérésére három módszer adódik.

Egy nemzet gazdasági tevékenységéhez nem csak a belföldi illetékességű (rezidens), hanem a külföldi illetékességű (nem rezidens) gazdasági egységek is hozzájárulnak. Egy nemzet nemzetközi számlája a fizetési mérleget és a nemzetközi befektetési pozíciót tartalmazza [263]. A fizetési mérleg egy statisztikai kimutatás, amely összegzi a rezidensek és nem rezidensek közötti tranzakciókat egy adott időszakra vonatkozóan. Ez az áruk és szolgáltatások számlájából, az elsődleges jövedelem számlájából, a másodlagos jövedelmi számlából, a tőkeszámlából és a pénzügyi számlából áll. Minden tranzakció megfelel egy jóváírási és terhelési bejegyzésnek: (1) áruk és szolgáltatások exportja, a kapott bevétel, az eszközök csökkenése vagy a kötelezettségek növekedése a hitelekkel összefüggésben, valamint (2) az áruk és szolgáltatások importja, a fizetendő jövedelem, az eszközök növekedése, vagy a kötelezettségek csökkenése a hitelek kapcsán. A kettős könyvvitel szerint a fizetési mérleg minden egyes tranzakciója legalább két különböző számlára kerül: egy terhelési és egy jóváírási számlára.

A fizetési mérleg részeként a folyó fizetési mérleg az áruk, szolgáltatások, elsődleges jövedelmek és másodlagos jövedelmek áramlását tartalmazza a rezidensek és nem rezidensek között az alábbiak szerint: (1) Az áruk és szolgáltatások számla a termelési tevékenységekből származó tételekkel kapcsolatos tranzakciókat képviseli. (2) Az elsődleges jövedelem a rezidens és nem rezidens intézményi egységek közötti pénzáramlást jelenti; és két altípust foglal magában: (a) a termelési folyamathoz kapcsolódó jövedelem, beleértve a munkaerő termelési folyamathoz való hozzájárulását, az adókat és a termékekre és a termelésre kivetett támogatásokat, valamint (b) a pénzügyi és egyéb eszközök kapcsán a tulajdonjoggal kapcsolatos bevételeket. (3) A másodlagos jövedelem számla a

rezidensek és nem rezidensek közötti folyó transzfereket, például személyes transzfereket vagy társadalombiztosítási hozzájárulásokat képvisel.

A fizetési mérleg tőkeszámlája tartalmazza (1) a nem termelt, nem pénzügyi eszközök rezidensek és nem rezidensek közötti beszerzését és elidegenítését, valamint (2) rezidensek és nem rezidensek között kapott és fizetendő tőketranszfereket. A pénzügyi számla a rezidensek és nem rezidensek között lebonyolított pénzügyi eszközöket és kötelezettségeket magában foglaló tranzakciókat rögzíti, amelyekre öt funkcionális befektetési kategória adódik: (1) közvetlen befektetés, (2) portfólióbefektetés, (3) származékos pénzügyi eszközök (a tartalékok kivételével) és munkavállalói részvényopciók, (4) egyéb befektetések és (5) tartalékeszközök. A pénzügyi számlán a „pénzügyi eszközök nettó beszerzése" és a „nettó kötelezettségvállalás" szerepel, amelyek a pénzügyi eszközökkel és kötelezettségekkel kapcsolatos tranzakciókat jelentik.

A nemzetközi számlák [263] második része a nemzetközi befektetési pozíciót részletezi, amely egy olyan statisztikai kimutatás, amely egy adott időpontban megmutatja (a) egy gazdaság rezidenseinek pénzügyi eszközei, amelyek nem rezidensekkel szembeni követelések vagy tartalékeszközként tartott aranyrúd, valamint (b) egy gazdaság rezidenseinek nem rezidensekkel szembeni kötelezettségei. Tehát a nemzetközi befektetési pozíció nettó követelést vagy nettó kötelezettséget jelent más nemzeti számlákkal szemben a pénzügyi számla tranzakciók, pénzügyi eszközök és kötelezettségek pénzáramainak megfelelő nyitó és záró értékének egyeztetésével. A nemzetközi befektetési pozíció értékelése az eszközök mindenkori piaci ára és az egyes időszakok végén érvényes árfolyamok alapján történik.

3. függelék Abnormális hozam vizsgálata

Eseményvizsgálat (event study) módszere [329] az események kapcsán felmerülő abnormális hozam (abnormal return – AR) gazdasági hatásának számszerűsítésére szolgál. A piaci modell (market modell – MM) egy referenciapiac tényleges hozamaira és az adott cég részvényeinek a referenciapiaccal való korrelációjára épít, amelyhez a legkisebb négyzeteket módszerét (ordinary least squares – OLS) alkalmazza.

A MM alkalmazásával a várható abnormális hozam kiszámítása a következő egyenlet szerint történik:

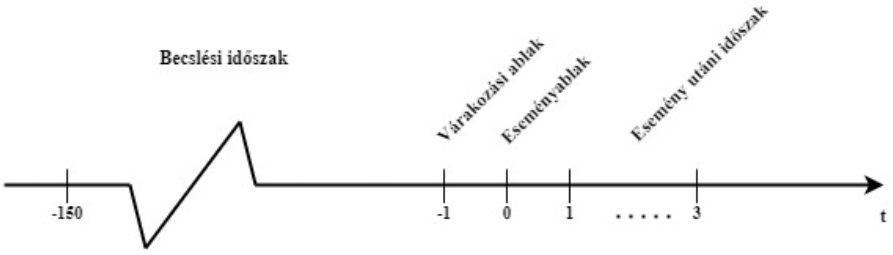
$$AR_t = R_t - (\alpha + \beta R_{M,t}) \tag{28}$$

ahol AR_t a részvény abnormális hozama, R_t a részvény *t* periódus tényleges hozama, $R_{M,t}$ a piaci portfólió *t* periódus hozama, α a regressziós modellből becsülendő illeszkedést segítő paraméter, β a regressziós modellből becsülendő együttható megmutatva a vizsgált részvény érzékenységét a piaci portfólióra.

A normál hozam kiszámításához az S&P500 indexet veszem alapul a piac hozam ($R_{M,t}$) meghatározásához. Az R_t és az $R_{M,t}$ a log-normalizált hozamok alapján kerül kiszámításra az alábbi képlettel:

$$R_t = ln\left(\frac{P_t}{P_{t-1}}\right) \tag{29}$$

ahol P_t az aznapi záró árfolyam, P_{t-1} az előző napi záró árfolyam. Az eseményvizsgálat során becslési időszakként (observation period) a $[-150, -2]$ intervallumot, az eseményt megelőző várakozási ablak a $]-2, -1]$ terjedelmű intervallumot, eseményablakként (event day) a $]-1,1[$ terjedelmű intervallumot és az esemény utáni időszakként (adjustment window) az $[1,3]$ terjedelmű intervallumot veszek alapul (***17***. ábra).



17. ábra. Egy eseményvizsgálat időrendje
Forrás: Saját szerkesztés

Az abnormális hozam szignifikanciájának mérésére a t-próbát alkalmazom, ahol a nullhipotézis állítása a vizsgált napon az abnormális hozam átlaga nulla ($H_0: \mu = 0$), az alternatív hipotézis pedig ennek az ellenkezője ($H_1: \mu \neq 0$). A t-próba a következőképp számítandó:

$$t_{AR_t} = \frac{AR_t}{S_{AR}} S_{AR} \tag{30}$$

ahol t_{AR_t} az a *t* időszakra vonatkozó t-próba, S_{AR} a minta szórását jelöli a becslési ablakban. A minta szórása a szórásnégyzetből adódik, amelyet a következő egyenlet határoz meg:

$$S_{AR}^2 = \frac{1}{M-2} \sum_{t=T_0}^{T_1} (AR_t)^2 \tag{31}$$

ahol S_{AR}^2 a szórásnégyzet, P_{t-1} az előző napi záró árfolyam, T_0 a becslési ablak legkorábbi napja, T_1 a becslési ablak legkésőbbi napja, M a nem hiányzó (azaz párosítható) hozamok számát jelöli.

A modell feltételezi, hogy a reziduumok normális eloszlásúak nulla átlaggal állandó variancia (homoszkedaszticitás) mellett, nincs autokorreláció, és a magyarázott változó nem korrelál a magyarázó változókkal. Annak tesztelésére, hogy a heteroszkedaszticitás negatívan befolyásolja-e a becslést, Breusch-Pagan tesztet [330] alkalmazom, a részvényárfolyam és a piaci index hozamát jellemző autokorreláció, valamint ezek keresztkorrelációjának mérésére a Pearson féle korrelációs együtthatóra alapuló tesztet [331] használom. Az abnormális hozam, valamint a Breusch-Pagan teszt és a Pearson teszt esetén egységesen 95 százalékos szignifikanciaszintet alkalmazok a számítások során. A Meta (Facebook) incidensek kapcsán a részvények abnormális hozamának a fentebb meghatározott metodológia szerinti vizsgálatát a 23. táblázat tartalmazza.

23. táblázat. Meta (Facebook) részvények abnormális hozamának vizsgálata

Események	Megfigyelés	Abnormális hozam	Paraméterek***	t stat	p érték
A Facebook felfüggeszti a Cambridge Analytics szolgáltatást a felhasználói adatokkal való visszaélés miatt (2018. március 19.)	AR (-1)	0,55%	$\alpha = -0{,}00093$	0,4655	0,64246
	AR (0)	-5,15%	β =1,23583	-4,3639	**0,00003***
	AR (1)	-2,68%	$p_{BP} = 0{,}25248$	-2,2706	**0,02498***
	AR (2)	1,06%	$p_{P_S} = 0{,}5298$	0,8947	0,37279
	AR (3)	0,55%	$p_{P_M} = 0{,}4105$ $p_{Corr} = 0{,}5298$	0,4659	0,64212
19 százalékos csökkenés a bevételkieséseket leíró piaci jelentés alapján (2018. július 26.)	AR (-1)	0,16%	$\alpha = -0{,}00067$	0,1105	0,91219
	AR (0)	-20,55%	$\beta = 1{,}33758$	-13,7854	**2,41E-26***
	AR (1)	0,17%	$p_{BP} = 0{,}04550$	0,1122	0,91083
	AR (2)	-1,38%	$p_{P_S} = 0{,}5263$	-0,9226	0,35808
	AR (3)	0,30%	$p_{P_M} = 0{,}5262$ $p_{Corr} = 0{,}5263$	0,2011	0,84095
A Techcrunch 419 millió rekordot érintő adatszivárgásról számol be (2018. szeptember 4.)	AR (-1)	-0,97%	$\alpha = -0{,}00135$	-0,4274	0,66985
	AR (0)	-2,26%	$\beta = 1{,}45744$	-0,9999	0,31943
	AR (1)	-1,81%	$p_{BP} = 0{,}43168$	-0,8006	0,42495
	AR (2)	-2,15%	$p_{P_S} = 0{,}6415$	-0,9529	0,34260
	AR (3)	0,77%	$p_{P_M} = 0{,}5103$ $p_{Corr} = 0{,}6415$	0,3415	0,73335
	AR (-1)	0,80%	$\alpha = -0{,}00074$	0,3765	0,70723
	AR (0)	-2,55%	$\beta = 1{,}45349$	-1,2042	0,23091

50 millió felhasználót érintő adatlopás (2018. szeptember 28.)	AR (1)	-1,69%	$p_{BP} = 0{,}36474$	-0,7971	0,42697
	AR (2)	-1,80%	$p_{P_S} = 0{,}8530$	-0,8496	0,39725
	AR (3)	1,90%	$p_{P_M} = 0{,}1260$	0,8947	0,37276
			$p_{Corr} = 0{,}8530$		
Az ICO 643 000 dollár büntetést szab ki a Cambridge Analytica adatszivárgása miatt (2018. október 24.)	AR (-1)	0,65%	$\alpha = -0{,}00177$	0,3060	0,76013
	AR (0)	-1,28%	$\beta = 1{,}30940$	-0,6037	0,54723
	AR (1)	1,07%	$p_{BP} = 0{,}55097$	0,5039	0,61527
	AR (2)	-1,30%	$p_{P_S} = 0{,}6894$	-0,6145	0,54010
	AR (3)	-1,24%	$p_{P_M} = 0{,}1823$	-0,5873	0,55813
			$p_{Corr} = 0{,}6894$		
A realizált negyedéves bevétel nem éri el a becsült negyedéves bevételt (2018. október 30.)	AR (-1)**	-1,32%	$\alpha = -0{,}00161$	-0,6275	0,53155
	AR (0)	1,14%	$\beta = 1{,}21653$	0,5397	0,59044
	AR (1)	2,59%	$p_{BP} = 0{,}27570$	1,2296	0,22129
	AR (2)	-1,14%	$p_{P_S} = 0{,}3866$	-0,5431	0,58808
	AR (3)	0,01%	$p_{P_M} = 0{,}0928$	0,0026	0,99796
			$p_{Corr} = 0{,}3866$		
A Facebook fellebbezett az Elsőfokú Bírósághoz (2018. november 21.)	AR (-1)	3,18%	$\alpha = -0{,}00147$	1,5031	0,13549
	AR (0)	1,54%	$\beta = 1{,}28986$	0,7304	0,46657
	AR (1)	-1,32%	$p_{BP} = 0{,}16738$	-0,6263	0,53234
	AR (2)	1,63%	$p_{P_S} = 0{,}9529$	0,7703	0,44264
	AR (3)	-1,29%	$p_{P_M} = 0{,}7591$	-0,6105	0,54269
			$p_{Corr} = 0{,}9529$		
Minden szolgáltatást érintő leállás (2019. március 14.)	AR (-1)	-0,09%	$\alpha = 0{,}00074$	-0,0510	0,95939
	AR (0)	-1,83%	$\beta = 1{,}23484$	-1,0467	0,29736
	AR (1)	-3,18%	$p_{BP} = 0{,}45731$	-1,8198	0,07132
	AR (2)	-3,91%	$p_{P_S} = 0{,}7333$	-2,2350	**0,02730***
	AR (3)	0,63%	$p_{P_M} = 0{,}9638$	0,3578	0,72114
			$p_{Corr} = 0{,}7333$		
Instagram adatvédelmi incidens (2019. március 25.)	AR (-1)	1,20%	$\alpha = 0{,}00103$	0,6534	0,51478
	AR (0)	1,18%	$\beta = 1{,}22883$	0,6435	0,52114
	AR (1)	-0,15%	$p_{BP} = 0{,}61060$	-0,0821	0,93472
	AR (2)	-0,62%	$p_{P_S} = 0{,}8935$	-0,3365	0,73713
	AR (3)	-0,74%	$p_{P_M} = 0{,}9154$	-0,4020	0,68841
			$p_{Corr} = 0{,}8935$		
A vállalat további információkat közöl. amelyek súlyosbítják az incidenst (2019. április 18.)	AR (-1)	0,13%	$\alpha = 0{,}00110$	0,0715	0,94315
	AR (0)	-0,59%	$\beta = 1{,}26832$	-0,3278	0,74362
	AR (1)	1,52%	$p_{BP} = 0{,}51517$	0,8440	0,40038
	AR (2)	0,06%	$p_{P_S} = 0{,}7263$	0,0307	0,97557
	AR (3)	-0,49%	$p_{P_M} = 0{,}9632$	-0,2704	0,78734
			$p_{Corr} = 0{,}7263$		
Mark Zuckerberg vezérigazgató levele a „potenciálisan problémás adatvédelmi gyakorlatokkal" kapcsolatos aggályokról (2019. június 12.)	AR (-1)	1,80%	$\alpha = 0{,}00107$	0,9541	0,34200
	AR (0)	-1,57%	$\beta = 1{,}32723$	-0,8325	0,40679
	AR (1)	0,73%	$p_{BP} = 0{,}50482$	0,3868	0,69960
	AR (2)**	2,26%	$p_{P_S} = 0{,}9525$	1,1984	0,23317
	AR (3)**	3,92%	$p_{P_M} = 0{,}8798$	2,0784	**0,03984***
			$p_{Corr} = 0{,}9525$		
A Törvényszék közbenső ítéletében kötelezte az ICO-t. hogy hozza nyilvánosságra	AR (-1)**	0,73%	$\alpha = 0{,}00096$	0,3854	0,70067
	AR (0)	2,27%	$\beta = 1{,}35376$	1,2013	0,23202
	AR (1)	3,93%	$p_{BP} = 0{,}47877$	2,0739	**0,04026***

döntéshozatali anyagát. (2019. június 14.)	AR (2)	-1,69%	$p_{P_S} = 0{,}9856$	-0,8931	0,37363
	AR (3)	-1,03%	$p_{P_M} = 0{,}8778$ $p_{Corr} = 0{,}9856$	-0,5418	0,58898
Az FTC 5 milliárd dolláros büntetést szab ki a Cambridge Analytica adatszivárgása miatt (2019. június 25.)	AR (-1)	0,87%	$\alpha = 0{,}00100$	0,4581	0,64769
	AR (0)	-0,90%	$\beta = 1{,}23191$	-0,4692	0,63977
	AR (1)	-0,57%	$p = 0{,}37060$	-0,3009	0,76401
	AR (2)	0,41%	$p_{P_S} = 0{,}9903$	0,2126	0,83203
	AR (3)	1,02%	$p_{P_M} = 0{,}9855$ $p_{Corr} = 0{,}9903$	0,5359	0,59305
Az ICO fellebbezett az ideiglenes határozat ellen (2019. szeptember 3.)	AR (-1)	-0,01%	$\alpha = -0{,}00010$	-0,0074	0,99413
	AR (0)	-0,95%	$\beta = 1{,}18391$	-0,5810	0,56238
	AR (1)	1,30%	$p_{BP} = 0{,}12823$	0,7955	0,42793
	AR (2)	0,47%	$p_{P_S} = 0{,}4019$	0,2861	0,77533
	AR (3)	-1,90%	$p_{P_M} = 0{,}4050$ $p_{Corr} = 0{,}4019$	-1,1588	0,24890
A Facebook kifizeti a büntetést (2019. október 30.)	AR (-1)	0,10%	$\alpha = -0{,}00038$	0,0760	0,93957
	AR (0)	-0,95%	$\beta = 1{,}32352$	-0,7159	0,47549
	AR (1)	2,23%	$p_{BP} = 0{,}23034$	1,6745	0,09667
	AR (2)	-0,21%	$p_{P_S} = 0{,}2907$	-0,1589	0,87399
	AR (3)	0,12%	$p_{P_M} = 0{,}4911$ $p_{Corr} = 0{,}2907$	0,0869	0,93093
A Kanadai Versenyhivatal 9 millió kanadai dollár bírságot szabott ki helytelen adatvédelmi gyakorlatok miatt (2020. május 19.)	AR (-1)	-1,90%	$\alpha = 0{,}00124$	-1,1833	0,23908
	AR (0)	2,57%	$\beta = 0{,}92412$	1,5982	0,11268
	AR (1)	4,21%	$p_{BP} = 0{,}81414$	2,6221	**0,00989***
	AR (2)	1,21%	$\boldsymbol{p_{P_S} = 0{,}0001}$****	0,7555	0,45147
	AR (3)	1,17%	$\boldsymbol{p_{P_M} = 0{,}0000}$**** $\boldsymbol{p_{Corr} = 0{,}0001}$****	0,7279	0,46809

Forrás: Saját szerkesztés

Magyarázat:

* Az adott abnormális hozam szignifikáns

** A megadott számítás az ablakok átfedése miatt egy másik eseményhez tartozik

**** α, β, Breusch-Pagan p érték (p_{BP}), Pearson féle korrelációalapuló p érték a részvényárfolyamra vonatkozó autokorreláció (p_{P_S}), a piaci indexre vonatkozó autokorreláció (p_{P_M}), valamint a részvényárfolyam és az index közötti keresztkorreláció (p_{Corr}) esetén

**** A korreláció fennállása miatt az abnormális hozam nem vehető figyelembe

KÖSZÖNETNYILVÁNÍTÁS

Ezúton köszönöm a témavezetőmnek, Prof. Dr. Rajnai Zoltánnak a doktori tanulmányaim során tanúsított szakmai és emberi támogatást, amivel segített eredményeim elérésében, és az értekezésem elkészítésében.

Köszönöm a Biztonságtudományi Doktori Iskola tagjainak és tanáraimnak a szakmai útmutatást és a publikálási lehetőségek biztosítását. Köszönöm Lévay Katalin, Farkasné Hronyecz Erika segítőkészségét a naprakész információk biztosításában, a tanulmányi és adminisztratív ügyek intézésében. Köszönöm Dr. Szádeczky Tamás és Dr. Jobbágy Szabolcs számára az előopponencia során megfogalmazott, a tervezet fejlesztését és véglegesítését elősegítő kritikát és javaslatokat.

Külön hálás vagyok Dr. Szádeczky Tamásnak szakmai és emberi hozzáállásáért, amivel elősegítette folyamatos fejlődésemet. Kiemelt köszönet illeti Dr. Berzsenyi Dánielt és Dr. Váczi Dánielt.

Köszönöm feleségemnek, dr. Boros Anikó Emesének a támogató közeget és lányomnak, Viviennek a türelmet és annak megértését, hogy miért mással és nem vele töltöttem el a rendelkezésre álló időt. Azon leszek a megszerzett tudással, hogy egy jobb világot teremtsek számára. Köszönöm szüleimnek, a feleségem szüleinek és a bátyámnak az évek során nyújtott támogatást.

NYILATKOZAT A MUNKA ÖNÁLLÓSÁGÁRÓL,

IRODALMI FORRÁSOK MEGFELELŐ MÓDON TÖRTÉNT IDÉZÉSÉRŐL

Alulírott **Bederna Zsolt** kijelentem, hogy „**A kiberbiztonság az Európai Unió szabályrendszerében. A kockázatok és incidensek kezelésére vonatkozó elvárások és lehetőségek, az incidensek potenciális hatásainak elemzése**” című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, a forrás megadásával egyértelműen megjelöltem.

Budapest, 2024. 03. 18.

……..

Bederna Zsolt