GAZDASÁG ÉS PÉNZÜGY • 12. ÉVF. 3. SZ. • 2025. SZEPT. • DOI: 10.33926/GP.2025.3.1

KIBERBIZTONSÁG ÉS PÉNZÜGYI STABILITÁS: ÖSSZEFÜGGÉSEK, KOCKÁZATOK ÉS SZABÁLYOZÁSI MEGKÖZELÍTÉSEK

Biró Gabriella[1]

ABSZTRAKT

A digitális technológiák előretörésével a pénzügyi szektor működése is egyre inkább információs rendszerekre és hálózatokra támaszkodik, így a kiberbiztonsági kockázatok kezelése kulcsfontosságúvá vált nem csak egyedi intézményi, hanem rendszerszinten, azaz a pénzügyi stabilitás megőrzése szempontjából is. A tanulmány célja, hogy feltárja a kiberbiztonság és a pénzügyi stabilitás közötti összefüggéseket, meghatározza a releváns fogalmakat, bemutassa a rendszerszintű kiberkockázatok eszkalálódásának folyamatait, valamint értékelje a kockázatcsökkentésre alkalmazott nemzetközi és hazai szabályozási és intézményi megközelítéseket. A cikk első részében a kiberbiztonság, a kiberreziliencia és a kiberkockázat fogalmát tisztázzuk, különös tekintettel a pénzügyi szektorban használt meghatározásokra. A középpontban három modell (az IMF, az ESRB és az MNB által kidolgozott keretrendszerek) elemzése áll, amelyek a kiberbiztonsági események pénzügyi rendszert érintő hatásainak eszkalációját, illetve az átviteli csatornák természetét vizsgálják. A szerző összeveti a modellek logikai struktúráját, különbségeit és alkalmazhatóságát, valamint értékeli, hogy ezek milyen mértékben segítik elő a rendszerszintű kockázatok azonosítását és csökkentését. A pénzügyi stabilitás magyar vonatkozásait és kritikus infrastruktúra védelemmel való kapcsolatát is bemutatjuk. A tanulmány utolsó szakasza áttekinti rendszerszintű kiberkockázatok kezelése során alkalmazható kockázatcsökkentő intézkedéseket. A preventív, detektív és korrektív kontrollintézkedések háromszintű megközelítését alkalmazva megvizsgálja a szabályozás, az információmegosztás és a tesztelés adta kockázatkezelési lehetőségeket. Összegzésként hangsúlyozzuk, hogy a pénzügyi rendszer kiberrezilienciájának erősítése csak multidiszciplináris megközelítés révén, a kiberbiztonsági és pénzügyi stabilitási szakértők összehangolt munkájával lehetséges.

JEL-kódok: G18, G28, O33

Kulcsszavak: pénzügyi stabilitás, kiberbiztonság, kiberreziliencia, rendszerszintű kockázat, kockázatkezelés

1 *Biró Gabriella* kiberbiztonsági szakértő, PhD hallgató, Nemzeti Közszolgálati Egyetem. E-mail: biro.gabriella@uni-nke.hu.

1. BEVEZETÉS

A pénzügyi stabilitást fenyegető kiberbiztonsági incidensekkel kapcsolatban a szakértők gyakran úgy fogalmaznak: nem az a kérdés, hogy megtörténnek-e, hanem hogy mikor. Ahogy mindennapi életünk – és pénzügyeink, gazdasági tevékenységünk – egyre nagyobb része a kibertérben, digitális platformokon zajlik, mind fontosabbá válik, hogy megértsük és megfelelően kezeljük a pénzügyi stabilitást potenciálisan fenyegető kiberkockázatokat. Ezt a növekvő kockázati tendenciát a pénzügyi világ meghatározó szereplői is felismerték. Christine Lagarde, az Európai Központi Bank (EKB) elnöke 2020-ban azt nyilatkozta, hogy a következő pénzügyi válságot egy kibertámadás indíthatja el, ezért szükséges felkészülni az ilyen kockázatok kezelésére (Thornton, 2020). A Világgazdasági Fórum (World Economic Forum, WEF) éves globális kockázati jelentéseiben is régóta visszatérő elem a kiberbiztonság, a „kiberkémkedés és kiberhadviselés"[2] kockázatát pedig a legfrissebb értékelésben a megkérdezettek rövid távon (2 év) az öt legsúlyosabb kockázat közé sorolták és középtávon (10 év) is bekerült az első tízbe (WEF 2025). A Nemzetközi Valutaalap (International Monetary Fund, IMF) is kiemelt figyelmet szentel a kiberbiztonsági kockázatoknak; 2024-es globális pénzügyi stabilitási jelentésében külön fejezet foglalkozik annak alátámasztásával, hogy a kiberkockázatok növekvő aggodalomra adnak okot a makropénzügyi stabilitás szempontjából (IMF, 2024).

Jelentős kiberbiztonsági incidensek eddig is történtek a pénzügyi szektorban. Az ENISA, az Európai Unió kiberbiztonsági ügynöksége évről évre közzéteszi az EU kiberfenyegetettségi térképét, 2025-ben pedig külön a pénzügyi szektort érintő elemzést is közzétett, melyből látható, hogy az incidensek száma évről évre növekszik (ENISA, 2024b). Az ENISA jelentése szerint a pénzügy szektor a harmadik helyen áll legtámadottabb szektorok közt a közszféra és a közlekedés után. A kibertámadások mintegy 9%-a pénzügyi szervezetek ellen irányul (ENISA, 2024a). Az egyik legnevezetesebb bankot érintő incidens a bangladesi nemzeti bank (Bangladesh Bank) elleni támadás volt, melynek során 2016 februárjában hackerek kompromittálták a bank hálózatát és a bank SWIFT rendszer kapcsolatán keresztül próbáltak meg közel 1 milliárd dollárt ellopni. Végül a tényleges anyagi kár 81 millió dollár lett, de az eset arra késztette a SWIFT rendszer tulajdonosait, hogy újra gondolják a rendszer biztonsági követelményeit és kialakítsák a SWIFT ügyfelek számára kötelező biztonsági programot (Customer Security Programme. Bangladesh Bank robbery 2025). 2022-ben az orosz tulajdonú, amszterdami székhelyű Amsterdam Trade Bank bezárásához jelentősen hozzájárult,

2 A 2025-ös jelentésben módszertani változás, hogy a kiberbűnözést és a kiberbiztonsági gyengeségeket is a „cyber espionage and warfare" kategóriába sorolták.

hogy bár a bank pénzügyi értelemben még fizetőképes volt, a Microsoft érvényesítette ellene a szankciókat és megvonta a bank hozzáférését a felhő szolgáltatásban tárolt banki adatokhoz (Chamber International, 2022). Így tehát precedens született arra, hogyan teheti lehetetlenné egy bank működését a technológiai szolgáltató egyik napról a másikra.

A jelen cikkben arra a kérdésre keressük a választ, hogyan tudjuk értelmezni a kiberbiztonsági kockázatokat a pénzügyi stabilitásra vonatkozóan. Tehát, mi a kiberkockázat, valamint mikor és hogyan érheti el azt a szintet, amikor már veszélyeztetheti a pénzügyi stabilitást és milyen lehetséges eszközök állnak rendelkezésünkre a kockázatok kezelése érdekében. A kérdés azért is összetett, mert a kiberbiztonság és a pénzügyi stabilitás két egymástól elég távol álló szakterület, amelyek közt mindezidáig viszonylag kevés átjárás és kapcsolódási pont adódott. Általában a kiberbiztonság szakértői, kutatói kevésbé mozognak otthonosan a makroprudenciális politika[3] világában, míg a pénzügyi stabilitással foglalkozó szakemberek számára a kiber- és információbiztonság csúcstechnológiás világa idegen. Ugyanakkor mostanra mindkét oldalon és a határterületeken is megszülettek azok az általános definíciók és modellek, amelyek lehetővé teszik a kiberkockázat pénzügyi stabilitásra gyakorolt hatásának érdemi vizsgálatát.

2. A KIBERBIZTONSÁG ALAPFOGALMAI

A kiberkockázatok értelmezéséhez és kezeléséhez először meg kell határoznunk azt az alapállapotot, amelyet szeretnénk elérni, és amelyet a kockázat fenyeget. A pénzügyi szektorban és azon kívül is több, széles körben elfogadott definíció létezik a kiberbiztonságra, illetve a kiberbiztonsági ellenállóképességre (kiberrezilienciára) vonatkozóan. Ezek közös eleme, hogy mindegyik elvárja a *bizalmasság*, a *sértetlenség* és a *rendelkezésre állás* hármas feltételrendszerének fennállását. A Pénzügyi Stabilitási Tanács (Financial Stability Board, FSB) 2017-ban létrehozta, majd 2023-ban frissítette a Kiberlexikont, amely a pénzügyi szektorban használt definíciókat hivatott egységesíteni (FSB 2023). Az FSB Kiberlexikon a következő, cikkünk szempontjából fontos meghatározásokat tartalmazza (a szerző fordítása):

„***Kiberbiztonság:*** *Az információk és/vagy információs rendszerek bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése a kibertérben. Ezen*

3 A makroprudenciális politika a teljes pénzügyi rendszer vagy annak jelentős részeire irányuló szabályozást és felügyeletet jelenti, célja a rendszerszintű kockázatok felismerése és kezelése. Ezzel szemben a mikroprudenciális felügyelet az egyedi pénzügyi intézmények biztonságos működésére fókuszál.

túlmenően más tulajdonságok, például a hitelesség, az elszámoltathatóság, a letagadhatatlanság és a megbízhatóság is szerepet játszhatnak."[4]

„***Kiberreziliencia:*** *Egy szervezet azon képessége, hogy folyamatosan képes ellátni a feladatát azáltal, hogy felkészül és alkalmazkodik a kiberfenyegetésekhez és más releváns környezeti változásokhoz, valamint ellenáll a kiberincidenseknek, megfékezi azokat és gyorsan helyreáll."*[5]

„***Kiberkockázat:*** *A kiberbiztonsági incidensek bekövetkezési valószínűségének és azok hatásának kombinációja."*[6]

Az Európai Unióban a pénzügyi ágazat legfőbb kiberbiztonsági szabályozása a DORA (Digital Operational Resilience Act /DORA, 2022/), amely címében ugyan a digitális működési rezilienciáról szól, azonban tartalmát tekintve a kiberbiztonsági kockázatok kezelése az egyik megfogalmazott fő célja. A rendelet nem határozza meg a kiberbiztonság vagy a kiberkockázat fogalmát, azonban a *digitális működési reziliencia* definíciója eléggé hasonlít az FSB fenti, pragmatikusabb *kiberreziliencia* definíciójára:

„***Digitális működési reziliencia:*** *a pénzügyi szervezet képessége arra, hogy kiépítse, biztosítsa és felülvizsgálja működési integritását és megbízhatóságát azáltal, hogy harmadik fél IKT-szolgáltatók által nyújtott szolgáltatások igénybevételével közvetlenül vagy közvetetten biztosítja azon hálózati és információs rendszerek biztonságának kezeléséhez szükséges IKT-vonatkozású képességek teljes körét, amelyeket a pénzügyi szervezet használ, és amelyek a pénzügyi szolgáltatások folyamatos nyújtását és minőségét támogatják, többek között zavarok fennállásakor is."* (DORA, 2022).

A DORA fogalomrendszere egy általánosabb EU irányelvhez, a NIS2 direktívához (NIS2 2022) igazodik, mivel a NIS2 határozza meg az egységes magas szintű kiberbiztonsági követelményeket a hatálya alá tartozó ágazatok – egyebek közt a NIS2 terminológia szerinti „banki szolgáltatások" és „pénzügyi piaci infrastruktúrák" – részére. Maga a NIS2 viszont – a DORA-hoz hasonlóan – szintén nem határozza meg a kiberbiztonság fogalmát, hanem visszautal az EU Kiberbiztonsági rendeletére (Kiberbiztonsági rendelet, 2019), ami egy általánosabb *kiberbiztonság* definíciót tartalmaz:

4 Cyber Security: Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. (FSB 2023)

5 Cyber Resilience: The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents. (FSB 2023)

6 Cyber Risk: The combination of the probability of cyber incidents occurring and their impact. (FSB 2023)

***„Kiberbiztonság**: azok a tevékenységek, amelyek a kiberfenyegetésekkel érintett hálózati és információs rendszereknek, az ilyen rendszerek felhasználóinak és más személyeknek a védelméhez szükségesek."* (Kiberbiztonsági rendelet, 2019)

A fentiek rávilágítanak arra, miért érezhette szükségét a Pénzügyi Stabilitási Tanács, hogy tisztázza, milyen definíciókat alkalmaz és javasol a többi pénzügyi szabályozó számára is, mikor a kiberbiztonság pénzügyi stabilitási aspektusaival foglalkozik.

A kockázat fogalmának meghatározása ehhez képest sokkal egységesebb, részben mert a szabályozók sokszor nem érzik szükségét, hogy újraértelmezzék, részben pedig azért, mert az összes (kiber és nem kiber) definíció valamilyen formában a kockázat bekövetkezési valószínűségének és lehetséges hatásának függvényeként írja le a kockázat nagyságát. Abban is egyetértenek a különböző módszertanok, hogy a kockázat kezelése a kockázat megszüntetése, áthárítása, csökkentése vagy elfogadása révén történhet. Ha a kiberbiztonsági kockázat olyan mértékű, hogy a pénzügyi stabilitást veszélyezteti, akkor ezek közül csak a kockázat csökkentése jöhet szóba. Ha a pénzügyi rendszer reziliens, akkor folyamatosan képes ellátni a feladatát, mivel rendelkezik az FSB meghatározásában szereplő a képességekkel, azaz a kiberkockázatok kezelése szempontjából felkészül, alkalmazkodik, ellenáll, megfékez és adott esetben helyreáll.

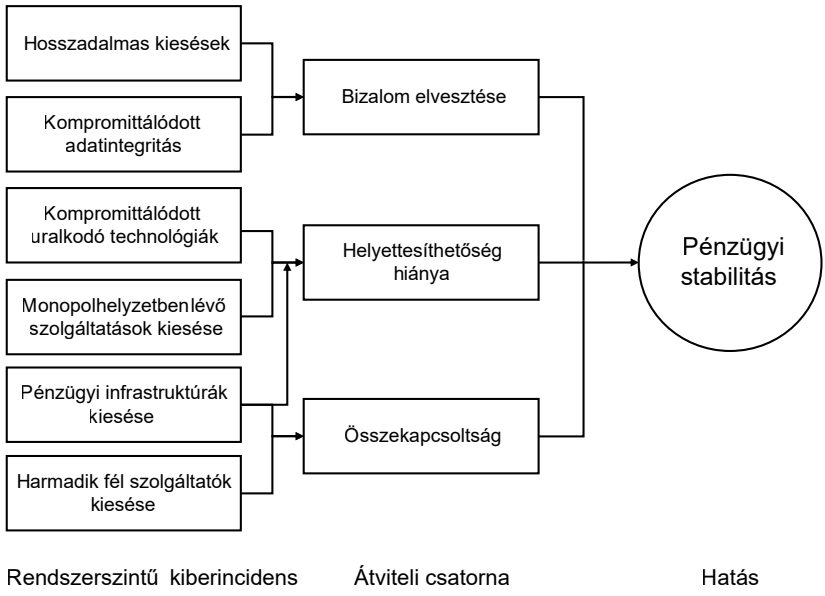
3. A KIBERBIZTONSÁG HATÁSA A PÉNZÜGYI STABILITÁSRA

A kiberbiztonsági kockázatok spektruma nagyon széles; az informatikai rendszereket érintő működési kockázati eseményektől (például egy viharban kidőlt nagyfeszültségű villanyoszlop okozta áramszünet) a szándékos hackertámadásokon át az ügyfeleket célzó kiberbűncselekményekig, mindent ide sorolhatunk. Mivel számtalan elképzelhető forgatókönyv létezik, az egyes fenyegetések elemzése helyett szükségünk van egy olyan általános módszertanra, amelyen keresztül megvizsgálhatjuk, hogyan fenyegetheti egy kiberbiztonsági incidens a pénzügyi stabilitást. Ennek elméleti alapjait többen próbálták leírni az elmúlt években, a szakértői munkacsoportok tevékenységének köszönhetően pedig két jelentős nemzetközi modell született.

Az Európai Unió pénzügyi rendszereinek makroprudenciális felvigyázásáért felelős Európai Rendszerkockázati Testület (European Systemic Risk Board, ESRB) 2017-ben állította fel azt a munkacsoportot (Európai Rendszerszintű Kiberkockázatok Csoportja – European Systemic Cyber Group, ESCG), amely 2020-ra kidolgozott és közzétett egy modellt, leírva a kiberbiztonsági incidensek rendszerszintű pénzügyi stabilitási eseménnyé eszkalálódásának általános folyamatát (ESRB 2020; Ros 2020). Röviddel ezután, szintén 2020-ban az IMF is köz-

zétette saját modelljét (Adelmann et al., 2020). Mindkét modell kiindulópontja egy-egy incidens, mely bizonyos feltételek teljesülése esetén a pénzügyi stabilitást érintő rendszerszintű problémává eszkalálódhat. Az IMF modellje kevésbé összetett, ezért először ezt tekintjük át.

1. ábra
A kiberbiztonság és a pénzügyi stabilitás kapcsolata az IMF modellje szerint



Forrás: saját szerkesztés (Adelmann et al., 2020 alapján)

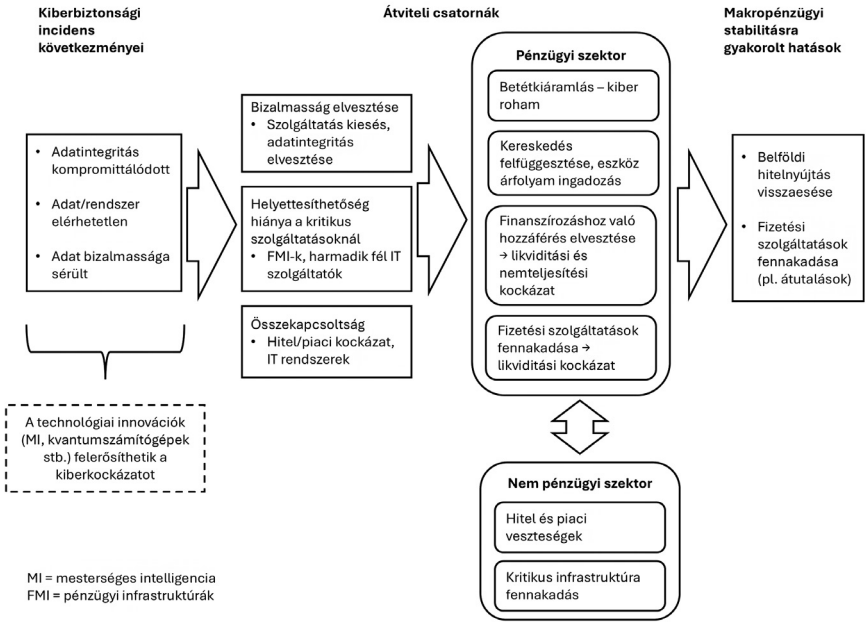
Az IMF eredeti modelljében (*1. ábra*) a kiberbiztonsági incidens eleve rendszerszintű esemény, ami attól éri el ezt a szintet, hogy olyan intézményt (pénzügyi infrastruktúrát[7], rendszerszinten jelentős bankot) érint, amelynek hatása van a pénzügyi stabilitásra[8]. Az IMF értékelése szerint ennek a hatásnak az átviteli csatornái három kategóriába eshetnek: bizalomvesztés, helyettesíthetetlenség

7 Például központi értéktárat, központi szerződő felet vagy fizetési rendszert működtető intézményt.

8 A rendszerszinten jelentős intézmények és szolgáltatások azonosításának módszertanát már korábban kidolgozták (FSB 2013).

vagy összekapcsoltság. A bizalomvesztés a pénzügyi stabilitás szempontjából ismerős tényező, kiváltó oka nemcsak kiberbiztonsági incidens lehet, hanem hagyományos, a pénzügyi stabilitással foglalkozó elemzők számára jól ismert forgatókönyvek is szóba jöhetnek, mint például a tőzsdepánik vagy a bankroham. Ugyanakkor a modell nem számol olyan lehetséges bemeneti eseményekkel, mint például az ügyfeleket érintő kiberbűncselekmények számának túlzott mértékű megugrása, vagy a közösségi médiában terjedő álhírek, melyek jelentős ügyfél-bizalomvesztéshez vezethetnek. Kérdés persze, hogy az ilyen bizalomvesztés milyen sebességgel következik be, azaz van-e idő és lehetőség beavatkozni és csökkenteni a kockázatot. A második csatorna a működést befolyásolja, tehát egy mással nem helyettesíthető technikai komponens vagy monopol helyzetben lévő szolgáltató (akár pénzügyi infrastruktúra) kiesésére épül. Ehhez hasonló a harmadik csatorna, amely a rendszerek összekapcsoltsága révén okozhat rendszerszintű kockázatot, ha egy pénzügyi infrastruktúrát vagy a beszállítói lánc egy elemét érinti a probléma. Az IMF modelljében a kiváltó kiberbiztonsági esemény az informatikai rendszer vagy az adatok bizalmasságára, sértetlenségére vagy rendelkezésre állására van hatással, tehát a kiberbiztonság hagyományos, az FSB Kiberlexikon által javasolt definíciójából indul ki. A modell előnye, hogy áttekinthető és szemléletes, a kiindulási események könnyen értelmezhetőek. Az eredeti modellt az IMF később továbbfejlesztette (*2. ábra*) a 2024-es Globális pénzügyi stabilitási jelentésében (IMF 2024). Ugyanakkor még a kibővített modellbe sem illeszthető bele minden lehetséges forgatókönyv, amiket a magasabb absztrakciós szinten megalkotott ESRB modell képes kezelni.

2. ábra
A kiberbiztonság és a makropénzügyi stabilitás kapcsolata az IMF részletesebb modellje szerint

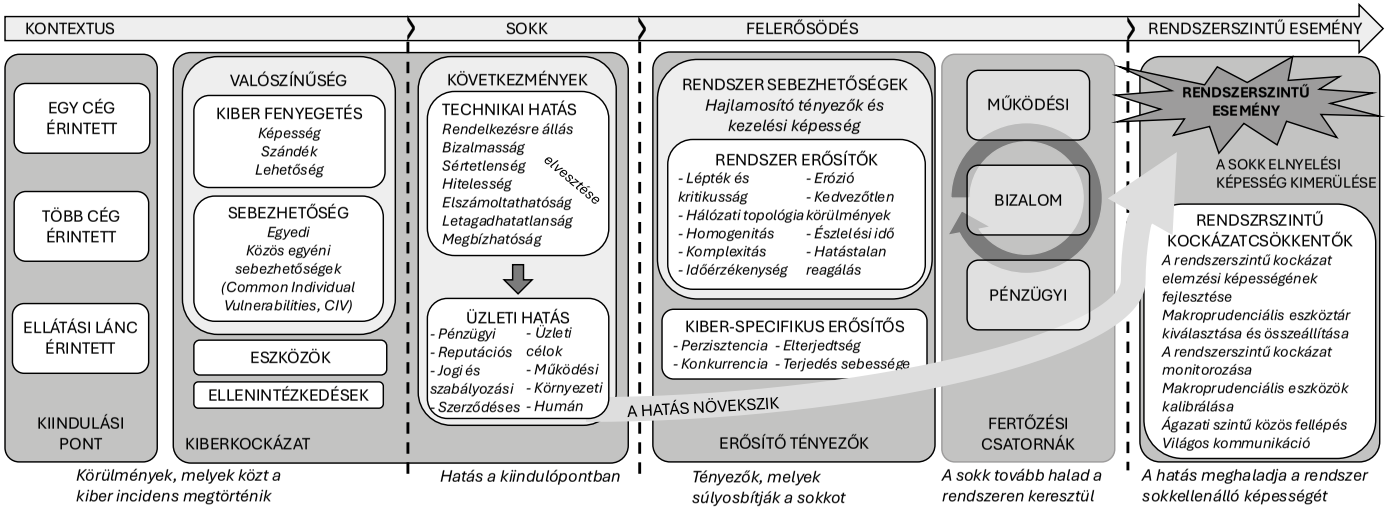


Forrás: saját szerkesztés (IMF 2024) alapján

Az ESRB megközelítése (*3. ábra*) valójában ott végződik, ahol az IMF elkezdődik, azaz a rendszerszintű kiberbiztonsági esemény bekövetkezésénél. Az ESRB modell kiindulási pontja egy kisebb (tehát még nem szükségszerűen rendszerszintű) kiberbiztonsági incidens, ami egy vagy több céget, vagy a beszállítói láncot érinti. Ez az eszkalációs folyamat első lépése, ahol a lehetséges kontextust vizsgálva a szakértők arra jutottak, hogy nemcsak egy rendszerszinten fontos intézményt érintő esemény vezethet a pénzügyi stabilitást veszélyeztető kockázathoz, hanem a több intézményt és/vagy beszállítói láncot egyidejűleg érintő események is elérhetik azt a kritikus szintet, ami kiválthatja azt a sokkot, ami végül felerősödve a rendszerszintű eseményhez vezet. A folyamat második lépése, az incidens tényleges bekövetkezése, azaz a sokk, amelynek technológiai hatása az informatikai rendszerek vagy adatok bizalmasságának, sértetlenségének vagy rendelkezésre állásának sérülése mellett más hatásokat, a hitelesség, az elszámoltathatóság, a letagadhatatlanság és a megbízhatóság elvesztését is magában foglalja. Ezek a tulajdonságok a FSB Kiberlexikonban található kiberbiztonsági definícióból követ-

keznek, ami nem meglepő, ha abból indulunk ki, hogy a modell elkészítése idején az FSB Kiberlexikon első kiadása már rendelkezésre állt (és az ESRB munkacsoport szakértőinek egy része dolgozott is rajta). Megjegyzendő, hogy a DORA a preambulumában hivatkozik az ESRB rendszerszintű kiberkockázatokkal kapcsolatos munkájára, azaz implicit módon elfogadja a felhasznált definíciókat (DORA, 2022).

3. ábra
A kiberbiztonsági esemény rendszerszintű pénzügyi stabilitást veszélyeztető eszkalálódása az ESRB modellje szerint



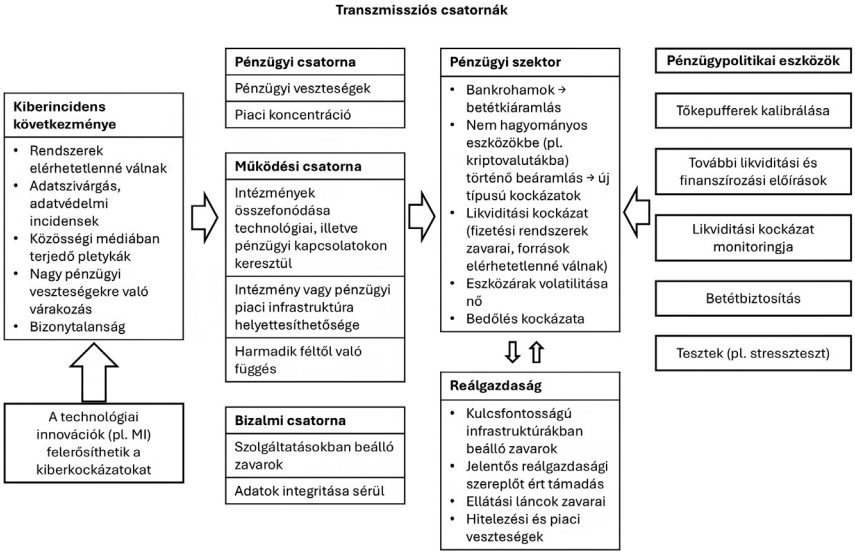
Forrás: saját szerkesztés (Ros 2020) alapján)

Az ESRB modell első és második fázisának határán a kockázat klasszikus definíciója tükröződik vissza, azaz a kockázati esemény bekövetkezési valószínűsége és lehetséges hatása határozza meg a kiberkockázat mértékét. A lehetséges hatás erősödik fel a harmadik fázisban, az amplifikáció során. Hasonlóan az IMF modellhez, az ESRB modell is három csatornát azonosít, melyek közül az egyik a bizalom (elvesztése), azonban az IMF által azonosított másik két csatorna (helyettesíthetőség, összekapcsoltság) az ESRB működésre vonatkozó csatornájába illeszthető és az ESRB szakértői arra a következtetésre jutottak, hogy harmadik csatornaként a pénzügyi hatás is közrejátszhat a sokk terjedésében, és a három terjedési csatorna kölcsönhatásba is léphet, tovább erősítheti egymást.

Az ESRB modell legvégső állomása az a pont, ahol a rendszerszintű esemény eszkalálódása eléri azt a szintet, amelyen a pénzügyi rendszer már nem képes elnyelni a sokkot. Ez a modell figyelembe veszi a rendszerszintű kockázatcsökkentési tényezőket is, amelyek lassíthatják vagy visszafoghatják a sokk terjedését. Összességében az ESRB modellje sokkal részletesebb és igyekszik minden lehetőséget számba venni, ugyanakkor kétségtelenül nehezebben átlátható, mint az IMF modellje.

A Magyar Nemzeti Bank (MNB) 2024-es Makroprudenciális jelentésében közzétette saját értelmezését a kiberkockázat és a pénzügyi stabilitás közötti transzmissziós csatornákról (*4. ábra*). Ez egy hibrid megközelítés, amely az IMF és az ESRB modelljéből is merít. A transzmissziós csatornákra koncentrál és konkrét lehetséges eseményekből indul ki, mint az IMF modellje, de az ESRB csatornái szerinti bontást követi. A kiberbiztonsági szakértő szemszögéből nézve azonban az MNB modelljéből hiányzik a bizalmasság, a sértetlenség és a rendelkezésre állás hármasára épülő elméleti megközelítés, amely mind az IMF, mind az ESRB modelljében tetten érhető. Szinte azt mondhatnánk, hogy az MNB értelmezésében a kiberkockázat elvesztette kiber-jellegét és betagozódott azon makroprudenciális feladatok közé, melyek kezelésében a technológiai szakértőknek nincs szerepe. Az MNB modell nagyon emlékeztet a monetáris politika transzmissziós mechanizmusánál alkalmazott modellekre is.

4. ábra
A kiberkockázat és a pénzügyi stabilitás közötti transzmissziós csatornák az MNB modellje szerint



Forrás: saját szerkesztés (MNB 2024) alapján)

Az MNB modellje abban is eltér az IMF és az ESRB modellektől, hogy az MNB nem beszélt rendszerszintű incidensről vagy rendszerszinten fontos intézményről. Ennek valószínűleg az az oka, hogy ha a modellek magyar vonatkozását nézzük, jelenleg nem találunk olyan intézményt, amely globális szinten jelentős hatást gyakorolhatna a pénzügyi stabilitásra, azaz G-SII lenne (Global Systemically Important Institution, G-SII). Az MNB modell és a másik két modell esetében is felmerülhet a kérdés, milyen intézményekre kell alkalmazni a leírt modellt, azaz mi számít rendszerszinten jelentős intézménynek. Az ESRB modell ezt a kérdést úgy válaszolja meg, hogy nem szükséges az incidensben érintett intézménynek vagy intézményeknek rendszerszinten jelentősnek vagy fontosnak lennie, hanem a körülmények megfelelően szerencsétlen együttállása során bármilyen intézményt érintő incidens rendszerszintűvé eszkalálódhat. Az IMF a modell leírásában a pénzügyi infrastruktúrákat (financial markets infrastructure, FMI), azok közül is első sorban a fizetési rendszereket tekinti rendszerszinten fontosnak, ami valószínűleg az IMF tevékenységének fókuszából adódik. Az MNB a kulcsfontosságú infrastruktúrákat érintő incidensekkel foglalkozik a saját modellje leírásában. Emellett a hazai pénzügyi szektor vonatkozásában az európai uniós szabályozási terminológia szerint több úgynevezett egyéb rendszerszinten jelentős

intézmény (Other Systemically Important Institution, O-SII) azonosítható. Ezek mind hitelintézetek, pontosabban nagybankok, és a cikk megjelenésének idején hét O-SII van Magyarországon.

Létezik egy másik megközelítés is annak eldöntésére, vajon Magyarország vonatkozásában melyek lehetnek azok az intézmények a pénzügyi szektorban, amelyek kiberbiztonsági incidensei bizonyos körülmények teljesülése esetén elérhetik a kritikus, pénzügyi stabilitás szempontjából jelentős szintet. A kritikus infrastruktúra-védelem hatókörébe tartozik a pénzügyi ágazati kritikus infrastruktúra-elemek azonosítása és kijelölése, ideértve a kritikus információs infrastruktúrákat is, melyek kiberbiztonsági szempontból relevánsak. Ez az azonosítás a pénzügyi ágazatban Magyarországon az MNB szakhatóságként történő közreműködésével már 2016 során megtörtént. A már említett DORA-rendelettel és a NIS2 irányelvvel egyidőben azonban megjelent az új, kritikus infrastruktúrák védelmére vonatkozó CER irányelv is (CER 2022), ezzel összefüggésben pedig a magyar jogszabályi környezet is megújult. A pénzügyi ágazatra vonatkozó azonosítási követelmények a korábbiakhoz képes keveset változtak, bár a kijelölt intézmények köre némileg szűkült. A kritikus pénzügyi infrastruktúraként azonosított intézmények listája nem nyilvános, azonban a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény a következő felsorolást tartalmazza:

1. Banki szolgáltatás: hitelintézeti pénzügyi szolgáltatás
2. Pénzügyi piaci infrastruktúra: kereskedési helyszínek üzemeltetése; fizetési- valamint klíring- és elszámolási rendszer üzemeltetése; központi szerződő fél tevékenysége; központi értéktár tevékenysége; készpénzellátás; a Magyar Nemzeti Bank alapvető feladatai, ide nem értve a monetáris politikát, a makroprudenciális politikát és a jegybanki információs rendszer működtetését.

A törvény és a hozzá kapcsolódó végrehajtási rendeletben szereplő pénzügyi ágazati követelmények alapján a magyar pénzügyi szektor ismeretében könnyen összse lehet állítani azon intézmények listáját, amelyekre gondolhatunk úgy, mint egy a pénzügyi stabilitást potenciálisan veszélyeztető kiberbiztonsági incidens lehetséges kiindulópontjára (*474/2024. (XII. 31.) Korm. rendelet*; *2024. évi LXXXIV. törvény*).

A kritikus infrastruktúra-védelem és a kiberbiztonság összefüggéseit az európai jogalkotó is felismerte, épp ezért hangolta össze a NIS2 irányelv, a CER irányelv és a DORA-rendelet tartalmát. Mindegyik európai jogalkotási aktusban előírta, hogy az érintett nemzeti hatóságok működjenek együtt a kockázatok minél hatékonyabb kezelése érdekében.

4. A RENDSZERSZINTŰ KIBERKOCKÁZATOK CSÖKKENTÉSE

A kiberbiztonsági incidensek pénzügyi stabilitást veszélyeztető eszkalációjának modellszintű leírása után az IMF, az ESRB és az MNB is megfogalmazott intézkedési javaslatokat a kockázatok csökkentése érdekében. Az ESRB ESCG munkacsoportja a modell kidolgozása és 2020-as közzététele után is folytatta munkáját és több irányból igyekezett megközelíteni a kérdéskört. Ezzel párhuzamosan már elkezdődött a DORA-rendelet szövegezése, amely szintén tartalmazott kifejezetten a rendszerszintű kiberkockázatok csökkentését célzó előírásokat. Mivel a különböző szakmai fórumok és hatóságok által meghatározott javasolt és kötelező intézkedéseket többféle szempont szerint lehet csoportosítani, a jelen cikkben az információbiztonsági szempontból hagyományosnak tekinthető hármas felosztást, a kontrollintézkedések preventív, detektív és korrektív felosztását alkalmazzuk. Ez a felsorolás nem teljes körű, de a főbb intézkedéscsoportokat tartalmazza és igyekszik rávilágítani a köztük fennálló összefüggésekre.

A megelőző (korrektív) intézkedések közé tartozik a jogszabályokban és felügyeleti szabályozó eszközökben (ajánlásokban, körlevelekben) előírt intézkedések sora, amelyeket a pénzügyi szervezeteknek meg kell hoznia ahhoz, hogy a kiberkockázatok bekövetkezési valószínűségét és/vagy lehetséges hatását csökkentsék. Az információbiztonság, a kiberbiztonság és a kiberreziliencia témakörében, vagy éppen a működési kockázatok csökkentésére vonatkozó felügyeleti elvárások részeként a különböző hatóságok és szervezetek már az 1990-es évek óta adnak ki ajánlásokat. Az informatikai felügyeleti tevékenységnek, azaz a pénzügyi felügyeleti hatóságok célzott, informatikai ellenőrzési szakértelemmel rendelkező felügyelők által végzett ellenőrzési, felügyeleti és felvigyázó tevékenységének világszerte a 2000-es év dátumváltási problémájára[9] való felkészülés adott nagyobb lendületet. Valószínűleg ezt volt az az informatikai kockázat, amelyet nem csak az IT rendszerek szakértői tárgyaltak meg egymás közt, hanem elérte a vállalkozások felsővezetőinek a szintjét is és téma lett a cégek igazgatósági ülésein. A magyar informatikai felügyelet kialakulásáról és a nemzetközi szabályozás fejlődéséről (Kandrács, 2023.07.1.) ad részletes áttekintést. A szabályozás tekintetében a 2016-os év volt a fordulópont: az EU ekkor tette közzé a NIS2 irányelv elődjét, a NIS-direktívát (NIS, 2016), a G7[10] együttműködés magas szintű kiberbiztonsági elvárásokat fogalmazott meg a pénzügyi szektor részére (G7, 2016), CPMI (Committee on Payments and Market Infrastructures) és az

9 A 2000-es év előtt sok informatikai rendszer csak 2 helyértéken tárolta az évszámot, így félő volt, hogy a nem megfelelően felkészített rendszerekben 2000. január 1-én 1900. január 1-ét mutathat a rendszerek órája, ami fennakadásokhoz vezethet.

10 Franciaország, Németország, Olaszország, Japán, Egyesült Királyság, Egyesült Államok, Kanada.

IOSCO (International Organization of Securities Commissions) pedig a mai napig használatban lévő közös iránymutatást adott ki a pénzügyi infrastruktúrák kiberbiztonsági ellenállóképességére vonatkozóan (CPMI–IOSCO, 2016). A következő években több elvárásrendszer, ajánlás és módszertan jelent meg, mivel minden szereplő fontosnak érezte, hogy maga is hozzájáruljon a kiberbiztonsági kockázatok csökkentéséhez. Ez a sokszínű szabályozási paletta vezetett végül ahhoz, hogy az európai szabályozó 2022-ben a DORA-rendelet révén egységesítette a töredezett elvárásrendszert.

A DORA-rendelet és a hozzá kapcsolódó felhatalmazáson alapuló rendeletek az általános infokommunikációs technológiákkal (IKT) kapcsolatos kockázatkezelési keretrendszer felállítása mellett több más, a kiberkockázatok megelőzésével kapcsolatos elvárást is megfogalmaznak. Ezek közt újdonság a harmadik fél IKT-szolgáltatóktól eredő kockázatok kezelésének hangsúlyossá tétele. Az elmúlt évek nagyobb incidensei ráirányították a figyelmet a beszállítói láncok jelentette informatikai kockázatokra, amik az IMF és az ESCG modelljeiben is megjelennek. A DORA újdonsága, hogy nem csak előírásokat tartalmaz a pénzügyi szervezetek számára, hanem felvigyázói[11] hatáskört is ad a pénzügyi felügyeleteknek bizonyos kiemelten fontos harmadik fél IKT-szolgáltatók – különösen a nagy felhőszolgáltatók – esetében.

A pénzügyi szektor az egyik legszabályozottabb szektor, mostanra pedig a kiberbiztonság szabályozottsága is elérte azt a szintet, hogy több és részletesebb szabályozással valószínűleg már nem lehet tovább javítani az intézmények kiberbiztonsági ellenállóképességét. A megvalósítás szempontjából ez azt is jelentheti, hogy a korlátozott erőforrásokkal rendelkező intézményeknek választani kell: a jogszabályi megfelelésre költ, vagy a kiberbiztonság gyakorlati aspektusaiba, technológiákba, folyamatokba és szakemberekbe fektet inkább. Ideális esetben persze a kiberbiztonság szabályozási és gyakorlati aspektusa találkozik; a jobb technológiai védelem egyben jogszabályi megfelelést is jelent, de ez a szerencsés együttállás viszonylag ritka a mindennapokban.

Olyan hangokat is lehet hallani, hogy a pénzügyi szektor kiberbiztonságának kérdésköre mára már túlszabályozottá vált és inkább egyszerűsíteni szükséges a meglévő, immár egységes európai szabályozást. Az Európai Bankföderáció (European Banking Federation, EBF) közzé is tett egy általánosabb (nem csak kiberbiztonsági szabályozásra fókuszáló) elemzést, melyben egyszerűsítéseket javasol a szabályozásban (EBF 2025). Ezzel párhuzamosan a pénzügyi szektoron kívül is megjelentek azok a vélemények, melyek szerint a kiberbiztonsági témák

11 A felügyelet és a felvigyázás eszköztára némiképp eltér egymástól, a felvigyázás általában finomabb, gyakran indirekt eszközökkel működik.

túlzott szabályozása versenyhátrányt okoz az EU-ban működő cégeknek. Egyelőre még nem indultak el a jogalkotók az egyszerűsítés irányába, de várhatóan a hangsúly át fog tevődni a létező szabályozás alkalmazására és érvényre juttatására. Ehhez még ki kell alakulnia az egységes, szervezeteken átívelő európai felügyeleti gyakorlatnak. A DORA felülvizsgálata várhatóan 2028 januárjában válik esedékessé a rendelet 58. cikk (1) bekezdése alapján.

Az IMF javaslatai közt az is szerepel, hogy fejleszteni kell a kiberbiztonsági kockázatelemzés módszertanát és hangsúlyosabban integrálni kell a pénzügyi stabilitással kapcsolatos elemzésekbe (Adelmann et al., 2020). Ez a megállapítás még most, 2025-ben is helytállónak tűnik, mert ugyan az információbiztonsági kockázatok elemzésére több, jól kimunkált módszertan áll rendelkezésre, a technológiai fejlődés miatt mindig vannak új kockázatok, amikkel korábban nem kellett számolni. Például ilyen új tényező a mesterséges intelligencia gyors térnyerése, vagy a kvantumszámítógépek jelentette, egyre valóságosabb fenyegetés a jelenleg használt kriptográfiai algoritmusokra. Emellett nyitott kérdés, hogyan tudnak hatékonyan együtt dolgozni a kiberbiztonsági és pénzügyi stabilitási szakemberek, hogy a két oldal elemzései homogén egésszé álljanak össze és pontos képet adjanak a tényleges, pénzügyi stabilitást veszélyeztető kiberkockázatokról. A kockázatok azonosítása és pontos felmérése elengedhetetlen a hatékony kockázatkezeléshez.

A kockázatkezelő intézkedések második nagyobb csoportja a detektív kontrollintézkedések, melyek hozzájárulnak a kockázatok időben történő észleléséhez. A DORA-rendeletben nagy hangsúlyt kap az információk megosztása: mind a bekövetkezett incidensek jelentése a felügyeleti hatóságoknak, mind az észlelt fenyegetések (tipikusan támadási minták, módszerek) önkéntes bejelentése. Ez a tudásmegosztás segíthet abban, hogy az intézmények könnyebben észleljék a már ismert támadási mintákat és hatékonyabban tudjanak védekezni ellenük, különösen akkor, ha arról is kapnak információt, milyen védekezési technikák működnek hatékonyan az adott támadás esetében. Az információmegosztás szerepét az IMF is hangsúlyozza, például az eurózóna pénzügyi stabilitási szempontú kiberkockázati értékelésében több konkrét javaslatot is megfogalmaz erre vonatkozóan (IMF, 2025). Már léteznek ugyan olyan európai platformok, amelyek a kiberbiztonsági incidensekkel kapcsolatos információk megosztására szolgálnak, azonban ezek nem terjednek ki a teljes pénzügyi szektorra. Például az Európai Központi Bank által 2018-ban létrehozott Euro Kiber Reziliencia Testület (Euro Cyber Resilience Board, ECRB) a határon átnyúló európai pénzügyi infrastruktúrák kiberrezilienciájával foglalkozik és saját információmegosztó platformot működtet (Cyber Information and Intelligence Sharing Initiative, CIISI-EU, IMF 2025).

A már említett ESRB ESCG munkacsoport is arra a következtetésre jutott az eszkalációs modell felvázolása után, hogy a kiberkockázatok nem állnak meg az országhatároknál, ahogy a nagy technológiai szolgáltatók és a rendszerszinten fontos pénzügyi cégcsoportok kiberkockázatai is össz-európai szintű kezelést igényelnek. A munkacsoport szerint a következő lépés egy pán-európai rendszerszintű kiberkockázati koordinációs keretrendszer felállítása lenne a kockázatok kezelése érdekében. 2021 végén és 2022 elején több formában közzé is tették javaslatukat az Európai Rendszerszintű Kiberincidens Koordinációs Keretrendszer (European Systemic Cyber Incident Coordination Framework, EU-SCICF) felállítására (ESRB 2021, 2022). Az EU–SCICF működésének részletes kidolgozása később betagozódott a DORA-rendelet által előírt feladatok végrehajtásába, mivel egyébként illeszkedik a DORA incidenskezelési és együttműködést támogató logikájába.

A kiberbiztonsági incidensek hatékony kezelésének elengedhetetlen kelléke a jól begyakorolt reagálási folyamat, melynek során a már bekövetkezett esemény következményeit hárítja el a szervezet. Ez a harmadik kontrollintézkedés csoport, a korrektív kockázatcsökkentő intézkedések, amelyek az incidens lehetséges hatását igyekeznek mérsékelni. A DORA-rendelet a nagyobb intézmények számára elő is írja, hogy rendszeresen végezzenek fenyegetésalapú behatolási tesztet (Threat-Led Penetration Test, TLPT). A pénzügyi szektorban már viszonylag régóta előírás, hogy a pénzügyi szervezetek végezzenek az informatikai rendszereiken (pl. az internetbanki alkalmazáson) behatolási teszteket, azaz kérjenek fel etikus hekkereket annak vizsgálatára, hogy egy támadó be tudna-e jutni a rendszerekbe. A TLPT ennél komplexebb forgatókönyvek alapján zajlik és valósághű támadásokra törekszik: első lépésként az aktuális fenyegetési információk (valós támadási mintázatok) alapján kidolgozott forgatókönyveket készítenek, a megbízott támadók pedig ezek alapján igyekeznek bejutni a célrendszerekbe. A sima behatolási tesztekhez képest az is fontos különbség, hogy a TLPT során a szervezet védekező csapata, a belső IT biztonsági és üzemeltetési csapat nem tudja, hogy teszt zajlik, azaz úgy kell reagálniuk, ahogy egy valós támadás esetén tennék. Ez nagyban fejleszti a csapat készségeit, mivel az éles gyakorlat lezárulta után a tanulságokat is feldolgozzák és részletes visszajelzést kapnak a támadó csapattól. A DORA-rendeletben megfogalmazott TLPT elvárásokhoz az EKB által kidolgozott TIBER–EU (Threat Intelligence-Based Ethical Red teaming, ECB, 2023) keretrendszer adta a mintát. Ahogy az EU–SCICF esetében, a TIBER–EU-nál is azt látjuk, hogy egy már korábban megkezdett munka betagozódott az egységes európai digitális működési reziliencia elvárásrendszer keretei közé.

A pénzügyi stabilitási szempontból releváns kiberbiztonsági teszteknek van egy másik formája, a kiber stressztesztek. A pénzügyi szektorban zajló többi stressztesthez hasonlóan ennek is az a célja, hogy „nyomáspróba" alá helyezze

a rendszert és meghatározza annak teherbíró képességét. A stressztesztek során bizonyos előre meghatározott paramétereket változtatunk és figyeljük, ez milyen hatással van a rendszer egészére és milyen stressz-szintnél fenyeget az összeomlás. A kiber stressztesztnél a kiinduló stresszforrás valamilyen kiberbiztonsági esemény, azonban a TLPT-vel ellentétben itt nem az incidensreagálási képességeket vizsgáljuk, hanem a kiberincidens hatását az adott intézmény vagy pénzügyi rendszer egészére. A tesztelés is másképp zajlik, a kiber stressztesztnél nem egy valós idejű szimuláció. Az egyik fő kihívás az ilyen teszteknél az, hogy a kiberbiztonsággal és digitális működési rezilienciával kapcsolatos paramétereket nehezebb számszerűsíteni, mérni vagy számítani, mint a hagyományos gazdasági és pénzügyi mutatókat. A jelenleg létező kiber stressztesztek módszertanok kétféle megközelítést (vagy ezek kombinációját) alkalmaznak: felülről lefelé, a gazdasági hatás irányából haladnak a technológiai szint felé, vagy lentről egy kiberincidens forgatókönyvéből haladnak felfelé, a lehetséges hatások irányába (Vermeulen et al. 2025, Khiaonarong–Korpinen–Islam 2025). Jelenleg a kiber stressztesztekkel kapcsolatban még viszonylag kevés tapasztalat áll rendelkezésre, de tanulságok már így is vannak (ECB 2024). A hatóságok érthető módon viszonylag szűkszavúak a feltárt hiányosságokkal kapcsolatban, hiszen nem akarnak ötleteket adni a potenciális támadóknak. Másrészt a kiber stressztesztekre fokozottan igaz, hogy olyan határterületet képviselnek, ahol érteni kell mind a kiberbiztonsági, mind a pénzügyi stabilitási komponenseket, és sok esetben a tesztelési módszertant is menet közben kell kidolgozniuk a szakértőknek, ezért nehéz konzisztens, évről évre összemérhető és publikálható eredményeket elérni.

Ha megvizsgáljuk a kiberbiztonsági kockázatcsökkentési logika szerint csoportosított preventív, detektív és korrektív védelmi intézkedéseket, azt láthatjuk, hogy összességében a kiberreziliencia definíciójában szereplő tevékenységeket alkalmazzuk, azaz *felkészülünk* az incidensekre, *alkalmazkodunk* a helyzethez és megpróbáljuk fenntartani a működést, *ellenállunk* a támadásoknak, a reagálással *megfékezzük* az incidens továbbterjedését és csökkentjük a következményeit, majd *helyreállítjuk* a megszokott működést. Tehát a kockázatcsökkentő intézkedéseket áttekintve visszajutottunk az FSB Kiberlexikon definíciójához (FSB 2023).

5. ÖSSZEGZÉS

A cikk elején láthattuk, hogy a pénzügyi szektor meghatározó szereplői valószínűnek tartják egy olyan rendszerszintű kiberbiztonsági esemény bekövetkezését, amely tényleges kockázatot jelenthet a pénzügyi stabilitásra. Eddig is voltak már súlyos kiberbiztonsági incidensek a pénzügyi szektorban, az esetek száma pedig évről évre növekszik, ami csak részben magyarázható a szigorodó

incidensbejelentési szabályokkal, amik miatt a hatóságok egyre több incidensről értesülnek. Előfordulhat persze az is, hogy a pénzügyi szervezetek egyre inkább képesek az incidenseket észlelni, csökken a látencia, emiatt nő a detektált és bejelentett események száma. Ugyanakkor az incidensek száma gyorsabban nő, mint ahogy a szabályozási környezet vagy az intézmények belső folyamatai és technikai eszközei fejlődnek, ezért valószínűleg abszolút értelemben is egyre több incidens történik. Így vélhetően tényleg csak idő kérdése, hogy valahol egy rendszerszinten jelentős kiberbiztonsági incidens is történjen a pénzügyi szektorban.

Ahhoz, hogy felismerjük és kezelni tudjuk a rendszerszinten jelentős, pénzügyi stabilitási szempontból is kockázatot jelentő kiberbiztonsági incidenst, meg kell határoznunk a jellemzőit. A cikkben arra kerestük a választ, hogyan tudjuk értelmezni a kiberbiztonsági kockázatokat a pénzügyi stabilitásra vonatkozóan. Ehhez megvizsgáltuk a kiberbiztonsággal és a kiberkockázattal kapcsolatos legfontosabb definíciókat: a bizalmasság, sértetlenség és rendelkezésre állás hármasát, valamint a kiberreziliencia és a digitális működési reziliencia fogalmi meghatározásait a különböző releváns keretrendszerekben (FSB, DORA). Láttuk, hogy a kiberkockázat képlete jól illeszkedik a működési kockázat, illetve más kockázattípusok meghatározására szolgáló módszertanokhoz, mivel a kockázatot a bekövetkezési valószínűség és a lehetséges hatás függvényének tekinti. Ebből a szempontból tehát nem okoz problémát a kiberbiztonsági kockázat beillesztése azon kockázatok sorába, amelyek veszélyeztethetik a pénzügyi stabilitást.

Több elméleti modell is igyekszik választ adni arra a kérdésre, hogyan érheti el a kiberkockázat azt a szintet, amikor már veszélyeztetheti a pénzügyi stabilitást. A cikkben megvizsgáltuk és összevetettük az ESCG, az IMF, és a két nagyobb modell által inspirált MNB modellt. A legösszetettebb és leguniverzálisabb az ESCG modellje, amely szinte minden forgatókönyvre alkalmazható. Az ESCG munkacsoport, amely a modellt működése első szakaszában, 2017–2020 között dolgozta ki, folytatta a munkát és több más értékes javaslattal állt elő, melyek közül a legjelentősebb az EU-SCICF pán-európai incidensreagálási keretrendszer. Ezzel párhuzamosan több más szakértői munkacsoport is dolgozott a rendszerszintű kiberkockázatok különböző eszközökkel történő kezelésén. A kiberbiztonsági szabályozás szempontjából a legjelentősebb, a kockázatok megelőzésére tett intézkedés a DORA-rendelet megalkotása volt. Maga a rendelet több olyan követelményt előír a pénzügyi szervezetek számára, amelyek végrehajtása csökkentheti a kiberbiztonsági kockázatokat. Ezek közül az IKT-kockázatkezelési keretrendszer felállítása mellett a kiberreziliencia fejlesztése szempontjából az információmegosztás és a valósághű kibertámadásokat imitáló TLPT tesztek a legfontosabbak. A kiber stressztesztek is hasonló célt szolgálnak, azonban fejlődésük a DORA-rendelettől független, végrehajtásuk pedig még korántsem olyan kiforrott módszertanokat követ, mint a TLPT-k. Várhatóan a következő néhány

év során a kiberkockázatok kezelésére rendelkezésre álló felügyeleti és szabályozói eszközök még jobban konvergálnak, ahogyan az EU–SCICF és a TLP bekerült a DORA égisze alá, úgy mind több felügyeleti kezdeményezést és módszertant integrálnak majd az egységes európai kiberkockázati felügyeleti keretrendszerbe. Ezt a hatást a pénzügyi szektoron kívülről jövő EU-s kezdeményezések, például a NIS2 és a CER irányelv végrehajtása is erősíthetik.

Összefoglalva kijelenthető tehát, hogy a pénzügyi rendszer kiberrezilienciájának erősítése csak multidiszciplináris megközelítés révén lehetséges. A kiberbiztonsági és pénzügyi stabilitási szakértők összehangolt munkájára van szükség a kockázatok azonosításához, felméréséhez és hatékony kezeléséhez. A szabályozási keretek, az információmegosztás és a rendszeres kiberbiztonsági és pénzügyi stabilitási szempontú tesztelés mind hozzájárulnak ahhoz, hogy a pénzügyi szektor felkészüljön, alkalmazkodjon, ellenálljon, megfékezze az eszkalálódó kiberbiztonsági eseményeket és helyreállítsa működését egy esetleges kiberincidens után, biztosítva ezzel a pénzügyi stabilitást a folyamatosan változó digitális környezetben. A jövő technológiai fejlődésben rejlő kihívásai, mint például a mesterséges intelligencia és a kvantumszámítógépek térnyerése, újabb kockázatokat vetnek fel, amelyek folyamatos szabályozói figyelmet és innovatív megoldásokat igényelnek a kiberreziliencia fenntartásához. A már említett kockázatok mellett ugyanakkor egyre nagyobb kihívás a megfelelően képzett szakemberek megtalálása és alkalmazása, mind a pénzügyi szervezetek, mind az őket felügyelő hatóságok vagy szabályozók részéről.

HIVATKOZÁSOK

474/2024. (XII. 31.) Korm. rendelet (2024). https://njt.hu/jogszabaly/2024-474-20-22

2024. évi LXXXIV. törvény (2025). https://njt.hu/jogszabaly/2024-84-00-00

Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) 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) (EGT-vonatkozású szöveg) (2019). https://eur-lex.europa.eu/eli/reg/2019/881/oj/hun

Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (EGT-vonatkozású szöveg). 333 OJ L (2022). http://data.europa.eu/eli/reg/2022/2554/oj/hun

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) 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 (NIS2 irányelv) (EGT-vonatkozású szöveg) (2022). https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (EGT-vonatkozású szöveg) (2022). https://eur-lex.europa.eu/eli/dir/2022/2557/oj/hun

Bangladesh Bank robbery (19.05.2025): in: *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Bangladesh_Bank_robbery&oldid=1291091781

Chamber International (06.07.2022): Solvent but bankrupt: how sanctions felled Amsterdam Trade Bank. *Chamber International*. https://www.chamber-international.com/news/latest-news/solvent-but-bankrupt-how-sanctions-felled-amsterdam-trade-bank/ (Letöltve: 2025.07.29).

CPMI – IOSCO (ed., 2016): Guidance on cyber resilience for financial market infrastructures. June 2016. Basel: *Bank for International Settlements*. https://www.bis.org/cpmi/publ/d146.pdf

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *OJ L* (2016). http://data.europa.eu/eli/dir/2016/1148/oj/eng

EBF (10.02.2025): Less Is More – Proposals To Simplify And Improve European Rule-Making In The Financial Services Sector. *EBF*. https://v3.globalcube.net/clients/eacb/content/medias/publications/eacb_studies/report_lessismore_fin.pdf

ECB (23.03.2023): What is TIBER-EU? https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html (Letöltve: 2025.07.29).

ECB (26.07.2024): ECB concludes cyber resilience stress test. https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240726~06d5776a02.en.html (Letöltve: 2025.07.29).

ENISA (2024a): ENISA threat landscape 2024. *LU: ENISA Publications Office*. https://data.europa.eu/doi/10.2824/0710888

ENISA (2024b): ENISA threat landscape: finance sector: January 2023 to June 2024. *LU: ENISA*. https://data.europa.eu/doi/10.2824/5410466

ESRB (2020): Systemic cyber risk. *European Systemic Risk Board*. https://data.europa.eu/doi/10.2849/566567

ESRB (25.03.2022): Recommendation of the European Systemic Risk Board of 2 December 2021 on a pan-European systemic cyber incident coordination framework for relevant authorities (ESRB/2021/17). *ESRB*. https://www.esrb.europa.eu/pub/pdf/recommendations/esrb.recommendation220127_on_cyber_incident_coordination~0ebcbf5f69.en.pdf?f2ec57c21993067e9ac1d73ce93a0772

ESRB (2022): Mitigating systemic cyber risk: January 2022. *LU: ESRB*. https://data.europa.eu/doi/10.2849/99500

Adelmann, F. – Elliott, J. – Ergen, I. –Gaidosch, T. – Jenkinson, N. – Khiaonarong, T. – Morozova, A. – Schwarz, N. – Wilson, C. (2020): Cyber Risk and Financial Stability: It's a Small World After All. In: *Staff Discussion Notes*. *International Monetary Fund*,7. https://doi.org/10.5089/9781513512297.006

FSB (16.07.2013): Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical Functions and Critical Shared Services. *Financial Stability Board*.: https://www.fsb.org/uploads/r_130716a.pdf

FSB (04.13.2023): Cyber Lexicon: Updated in 2023. *Financial Stability Board*. https://www.fsb.org/uploads/P130423-3.pdf

G7 (2016): G7 Fundamental Elements of Cybersecurity for the Financial Sector. *G7*. https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

IMF (2024): Global Financial Stability Report, April 2024: The Last Mile: Financial Vulnerabilities and Risks. Washington, D.C.: *International Monetary Fund*. https://doi.org/10.5089/9798400257704.082

IMF (2025): Euro Area: Publication of Financial Sector Assessment Program Documentation-Technical Note on Cyber Risk and Financial Stability-Selected Issues in Regulation and Supervision. *IMF Staff Country Reports* 2025(213): 1. https://doi.org/10.5089/9798229019873.002

Kandrács, C. (ed., 2023): Stabilitás és bizalom: A magyar pénzügyi felügyelés története. Budapest: *Magyar Nemzeti Bank. Stabilitás és Bizalom by MNB | Magyar Nemzeti Bank | The Central Bank of Hungary - Issuu*

Khiaonarong, T. – Korpinen, K. – Islam, E. (2025): Using Simulations for Cyber Stress Testing Exercises. *International Monetary Fund (IMF)*. https://doi.org/10.5089/9798229008952.001.a001

MNB (2024): Makroprudenciális jelentés 2024. *Magyar Nemzeti Bank*. https://www.mnb.hu/letoltes/mnb-makroprudencialis-jelentes-2024.pdf

Ros, G. (2020): The making of a cyber crash: a conceptual model for systemic risk in the financial sector. *LU: European Systemic Risk Board*. https://data.europa.eu/doi/10.2849/915512

Thornton, P. (02.06.2020): Cyber attacks could cause next financial crisis, says ECB boss. *The Independent*. https://www.independent.co.uk/news/business/news/cyber-attack-financial-crisis-christine-lagarde-ecb-a9322556.html (Letöltve: 2025.07.26.).

Vermeulen, R. – Sydow, M. – Brousse, C. – Cascão, F. – Fique, J. – Marques, C. – Nyholm, J. – Virel, F. (2025): Cyber resilience stress testing from a macroprudential perspective. *Macroprudential Bulletin* (27): https://www.ecb.europa.eu/press/financial-stability-publications/macroprudential-bulletin/html/ecb.mpbu202502_01~f4914a46c1.en.html (Letöltve: 2025.03.28.).

WEF (2025): The Global Risk Report 2025. Köt. 20. Cologny/Geneva, Switzerland: *World Economic Forum*.