

Bordács Bálint¹

Kritikus infrastruktúrák kiberbiztonsági célú információmegosztása az Egyesült Államokban

Cybersecurity Information Exchange of Critical Infrastructures in the United States

Absztrakt

A kritikus infrastruktúrák kiberbiztonsági információmegosztása napjaink egyik meghatározó kihívása. A kibertámadásokkal kapcsolatos naprakész információk segíthetik a vállalatokat védelmi képességeik fejlesztésében, sérülékenységeik és a potenciális fenyegetések azonosításában, valamint a támadások pénzügyi következményeinek mérséklésében. A tanulmány az Egyesült Államok jelenlegi információmegosztási rendszerét vizsgálja, és javaslatokat fogalmaz meg a vállalati részvétel, valamint a megosztott adatok minőségének és mennyiségének javítására. Ennek keretében bemutatja az ISAC-rendszer reformjának lehetőségét a Nemzeti Kiberbiztonsági Stratégiával összhangban, egy kötelező kritikusinfrastruktúra-információmegosztási modell kialakításán keresztül. A kutatás arra keresi a választ, hogy milyen strukturális és szabályozási tényezők akadályozzák az amerikai kiberbiztonsági információmegosztási rendszer hatékony működését, és milyen reformok javíthatják annak eredményességét. A vizsgálat dokumentum- és szakirodalom-elemzésre épül, különös tekintettel az ISAC-rendszerre és az amerikai kiberbiztonsági szabályozásra. A tanulmány megállapítása szerint az információmegosztás hatékonyságát elsősorban az alacsony részvételi hajlandóság, a bizalom hiánya, az interoperabilitási problémák és a finanszírozási korlátok csökkentik, amelyek kezelése nélkül a kritikus infrastruktúrák kibervédelmi ellenálló képessége sem erősíthető megfelelően.

Kulcsszavak: kiberbiztonság, kritikus infrastruktúrák, információmegosztás, Nemzeti Kiberbiztonsági Stratégia, ISAC

¹ Doktori hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: bord.balint@gmail.com

Abstract

Cybersecurity information sharing for critical infrastructures has become a key challenge in modern cybersecurity governance. Timely information on cyber threats can help organisations strengthen their defences, identify vulnerabilities and emerging threats, and mitigate the financial impact of cyber incidents. This study examines the current U.S. information-sharing framework and proposes measures to improve corporate participation as well as the quality and quantity of shared information. In this context, the paper outlines the potential reform of the ISAC system in line with the National Cybersecurity Strategy through the establishment of a mandatory critical infrastructure information-sharing model. The study seeks to identify the structural and regulatory factors that hinder the effective operation of the U.S. cybersecurity information-sharing system and to assess which reforms could improve its effectiveness. The research is based on document and literature analysis, with particular focus on the ISAC system and U.S. cybersecurity regulation. The findings suggest that the effectiveness of information sharing is primarily limited by low participation rates, lack of trust, interoperability challenges, and funding constraints, all of which undermine the cyber resilience of critical infrastructures if left unresolved.

Keywords: cybersecurity, critical infrastructure, information exchange, National Cybersecurity Strategy, ISAC

Bevezetés

Egy egyesült államokbeli kutatóintézet, a Center for Strategic and International Studies (CSIS) folyamatosan frissített adatbázisa szerint 2025-ben több tucat jelentős kibertámadás történt a világban, amelyek több millió dolláros veszteséggel jártak. A támadásoknak számos kritikus infrastruktúrának minősülő célpontja volt, így például a francia postavállalat, a venezuelai nemzeti olajvállalat, illetve az Egyesült Államok kormányzati ügynökségei.² A Department of Homeland Security (DHS) szerint a kritikus infrastruktúrát célzó kiberbiztonsági fenyegetések az egyik legjelentősebb stratégiai kockázatot jelentik az Egyesült Államok számára, mert veszélyeztetik az ország nemzetbiztonságát, gazdasági jólétét, valamint a közegészségügyet és a közbiztonságot. A kérdés aktualitását az is alátámasztja, hogy a jogalkotók és a szabályozó hatóságok is kiemelt figyelmet fordítanak a területre. Az Egyesült Államok³ közelmúltban elfogadott kiberbiztonsági stratégiája a kritikus infrastruktúrák védelmének a kiberbiztonsági keretrendszerben betöltött szerepére összpontosít, a kritikus infrastruktúrák fontossága a második Trump-adminisztráció kiberbiztonsági stratégiájában is teret kap,⁴ és számos *soft law* dokumentum és tanulmány is megjelent ezen a területen. Az információmegosztás a hatékony kiberbiztonság egyik központi eleme. A kibertámadásokkal kapcsolatos naprakész ismeretek segíthetnek a vállalatoknak abban,

² Center for Strategic and International Studies [é. n.].

³ Statement on the National Cybersecurity Strategy 2023.

⁴ President Trump's Cyber Strategy for America 2026.

hogy megerősítsék védelmi vonalaikat, megismerjék sebezhető pontjaikat, valamint az ezeket kihasználni igyekvő potenciális fenyegetéseket. A fenyegetésekkel kapcsolatos információk és jó gyakorlatok megosztásával az érdekelt felek sikeresen csökkenthetik az incidensek kockázatát.

A tanulmány célja annak vizsgálata, hogy az Egyesült Államok kritikus infrastruktúráinak kiberbiztonsági információmegosztási rendszere milyen strukturális és szabályozási kihívásokkal szembesül, különös tekintettel az ISAC-rendszer működésére, az interoperabilitásra, a részvételi hajlandóságra és az információmegosztás hatékonyságára. A kutatás központi kérdése, hogy a jelenlegi információmegosztási modell milyen tényezők miatt nem képes minden esetben biztosítani az időszerű, operatív módon felhasználható fenyegetési információk hatékony áramlását a kritikus infrastruktúrák szereplői között, illetve milyen szabályozási és szervezeti megoldások javíthatják a rendszer működését.

A tanulmány módszertanát elsősorban kvalitatív jogi és szakpolitikai elemzés képezi, amely az Egyesült Államok kiberbiztonsági stratégiájának, a CIRCIA szabályozási folyamatának, az ISAC-rendszer működésével kapcsolatos szakirodalomnak, valamint kormányzati és iparági jelentéseknek az elemzésére épül. A vizsgálat korlátját jelenti, hogy az információmegosztási rendszerek működésével kapcsolatos empirikus adatok nagy része nem nyilvános, továbbá az ISAC-ek működése ágazatonként jelentősen eltérhet.

A tanulmány elsőként bemutatja a kiberbiztonsági információmegosztás amerikai szabályozási és intézményi kereteit, ezt követően elemzi az alkalmazott hálózati modelleket és az ISAC-rendszer működését, majd áttekinti a részvétellel, adatminőséggel, interoperabilitással és finanszírozással kapcsolatos főbb kihívásokat. Végül a tanulmány a rendszer továbbfejlesztésének lehetséges irányait és szabályozási tanulságait foglalja össze.

Kritikus infrastruktúrák az Egyesült Államokban

Ahhoz, hogy megértsük az Egyesült Államok kiberbiztonságának keretrendszerét és az információmegosztás nehézségeit a kritikus infrastruktúrák esetében, szükséges bemutatni az Egyesült Államok kritikus infrastruktúrájához tartozó ágazatok felépítését. Az Egyesült Államok katonai és polgári infrastruktúrájának több mint 80%-a a magánszektor tulajdonában és üzemeltetésében van. Az elmúlt években ezen vállalkozások, különös tekintettel az infokommunikációs szektor szereplőire, valamint a kormányzati szervek egyre inkább az internetes hálózatok sebezhetőségeit kihasználó kibertámadások célpontjává váltak.⁵

Az elmúlt évtizedben az Egyesült Államok kritikus infrastruktúrájának kiberbiztonsági keretrendszerét két fő dokumentum határozta meg.

2024-et megelőzően az Egyesült Államok kritikus infrastruktúrájához tartozó ágazatokat egy *Presidential Policy Directive* (PPD)⁶ sorolta fel. A 21. számú PPD 16 ága-

⁵ GRIEGER 2023.

⁶ *Presidential Policy Directive* 21 2013.

zatot nevez meg, amelyekből az USA létfontosságú infrastruktúráinak keretrendszere felépül. Ezek közé tartozik a vegyipar, a kereskedelmi létesítmények, a kommunikáció, a kritikus gyártás, a gátak, a védelmi ipari bázis, a sürgősségi szolgáltatások, az energiaágazat, a pénzügyi szolgáltatások, az élelmiszer- és mezőgazdasági szektor, a kormányzati létesítmények, az egészségügy és a közegészségügy, az informatikai szektor, a nukleáris reaktorok és a hulladékkezelés, a közlekedési rendszerek, valamint a víz- és szennyvízrendszerek. E szektorok kijelölésének célja azon rendszerek és szolgáltatások azonosítása, amelyek működésképtelenné válása vagy megsemmisülése súlyos következményekkel járna a nemzetbiztonságra, a gazdaságra, a közegészségügyre vagy a közbiztonságra nézve.

A szektorok olyan infrastruktúrákat foglalnak magukban, amelyek társadalmi és gazdasági szempontból nélkülözhetetlenek, és kölcsönösen függenek egymástól. Az energia-, kommunikációs és informatikai rendszerek például más kritikus ágazatok működésének előfeltételei, míg a pénzügyi, közlekedési vagy egészségügyi infrastruktúrák kiesése láncreakciószerű társadalmi és gazdasági zavarokat idézhet elő. A szabályozási keret ezért nem csupán az egyes ágazatok önálló védelmét célozza, hanem az infrastruktúrák közötti rendszerszintű kapcsolatok és függőségek kezelését is, különös tekintettel a kibertámadásokból eredő, ágazatokon átívelő kockázatokra.

A 21. számú PPD azt is meghatározza, hogy mely szövetségi ügynökségek tartoznak egy adott kritikusinfrastruktúra-ágazathoz. Ezek az ágazatspecifikus ügynökségek felelősek a kibervédelemhez szükséges intézményi tudás és a speciális szakértelem biztosításáért, valamint az adott ágazat biztonsági és ellenálló képességét fejlesztő és fenntartó programok irányításáért, illetve a szakmai támogatásért a jelenlegi, szerteágazó veszélyekkel fenyegető környezetben.

A 21. számú PPD-t az Egyesült Államok 2024-ben kiadott NSM-22 (*The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience*) szabályozása váltotta fel, amely a kritikus infrastruktúrák védelmének és rezilienciájának korszerűsített stratégiai keretrendszerét határozza meg. Az NSM-22 továbbra is fenntartja az ágazatspecifikus szövetségi ügynökségek központi szerepét, és a kijelölt szektorokon sem változtat. A korábbi szabályozáshoz képest nagyobb hangsúlyt helyez az összkormányzati koordinációra, a kockázatalapú megközelítésre. A szabályozás reflektál a 21. számú PPD megjelenése után felmerült új kihívásokra is, így az ellátási láncok sérülékenységre, a klímaváltozásra és egyéb hibrid fenyegetésekkel szembeni reziliencia erősítésére. A memorandum előírja a nemzeti szintű kockázatkezelési tervek rendszeres felülvizsgálatát, továbbá ösztönzi, hogy a kritikus infrastruktúrák üzemeltetői egységesebb biztonsági és ellenálló képességi követelményeknek feleljenek meg.⁷

⁷ HUMPHREYS 2024.

A kiberbiztonsággal kapcsolatos információmegosztás jelenlegi szabályozása az Egyesült Államokban

A kiberbiztonsággal kapcsolatos információmegosztás rendszerének megértéséhez szükséges a teljes keretrendszer ismerete a stratégiaalkotástól az intézményeken keresztül tényleges megvalósulásig, jelen fejezetben így ezek bemutatására kerül sor.

A Nemzeti Kiberbiztonsági Stratégia

A 2023-ban elfogadott Nemzeti Kiberbiztonsági Stratégia⁸ (NKS) kimondja, hogy a kiberbiztonság alapvető fontosságú az amerikai gazdaság megfelelő működéséhez és az amerikai kritikus infrastruktúrák feladatainak ellátásához. A kiemelt figyelem oka, hogy azok a szereplők, amelyek korábban nem voltak képesek hatékony támadást intézni ezen rendszerek ellen a kibertérben, és ezáltal az USA érdekeit sérteni, a technológiai eszközök széles körű hozzáférhetősége miatt napjainkra megszerezték az ehhez szükséges képességeket.

Az Egyesült Államok kormányának korábbi kiberbiztonsági stratégiája kiemelte, hogy a kibertér védelmének elsődleges eszköze nem a szövetségi szabályozás lesz. Az új kiberbiztonsági stratégia arra a felismerésre reagál, hogy a korábbi, kizárólag a piaci szereplőkre hagyatkozó stratégia hatástalan volt, mivel nem tudta megfelelően kezelni a kritikus rendszerek sebezhetőségét, és nem tudta megakadályozni a kritikus infrastruktúrát érintő támadásokat. Ennek okán a dokumentum sürgeti az áttérést a kizárólag az iparági önszabályozás rendszeréből a köz- és magánszféra közötti együttműködésre. A stratégia olyan új szabályozási keretrendszer bevezetését javasolja, amely kötelező minimális kiberbiztonsági előírásokat állapítana meg. Ez a változás kiegyenlítettebb feltételeket teremtené a szabályozási környezetben azáltal, hogy a biztonsági hibákért viselt felelősség egy részét a végfelhasználókról és a kis- és középvállalkozásokról a jelentős anyagi és technológiai háttérrel rendelkező infokommunikációs vállalatokra, valamint a kritikus infrastruktúrához tartozó vállalkozások tulajdonosaira és üzemeltetőire hárítaná.

Az új NKS első pillére a kritikus infrastruktúrák védelme. A kormányzat ezen a területen keresztül törekszik az Egyesült Államok digitális ökoszisztémájának szereplői közötti együttműködés kiépítésére és magasabb szintre emelésére. Ez a pillér segít megvalósítani azt a két alapvető változást is, hogy az Egyesült Államok hogyan osztja el a szerepeket, felelőségeket és erőforrásokat a kibertérben azáltal, hogy bevonja a hatékony kibervédelem kialakításában érdekelt összes szereplőt (magánszemélyeket, kisvállalkozásokat, állami és helyi önkormányzatokat és az infrastruktúra-üzemeltetőket), valamint előnyben részesíti a hosszú távú megoldásokat a kibervédelem területén.

A stratégia célja egy olyan, a szereplők közötti bizalmon alapuló „hálózatok hálózatainak” létrehozása, amely a kritikus infrastruktúrák védelme során magas szintű kiberbiztonsági ismeretek alkalmazására összpontosít, valamint kollektív és összehangolt fellépésre ösztönzi a szereplőket. Ebben a hálózatban mind a magán-, mind pedig

⁸ Statement on the National Cybersecurity Strategy 2023, 1.2. fejezet.

az állami szervek az információmegosztó és elemző szervezetek (*Information Sharing and Analysis Organizations*, ISAO-k), az ágazati információmegosztó és (*Information Sharing and Analysis Centers*, ISAC-ek) és más szervezetek információmegosztási eszközeit használnák a kibervédelmi műveletek megkönnyítése érdekében. A rendszert a *Cybersecurity and Infrastructure Security Agency* (CISA) koordinálná.⁹ A valós idejű, azonnal felhasználható információk többirányú megosztásának elérése érdekében a stratégia célja, hogy mind a személyek, mind pedig a gépek közötti együttműködést és adatmegosztást felhasználja.¹⁰

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

A kormányzati szervek szerepét illetően egy új jogszabály, a 2022-ben elfogadott *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (CIRCIA)¹¹ fontos mérföldkő az amerikai kritikus infrastruktúrák kiberbiztonságának előmozdításában. A CIRCIA eredményeként a CISA-nak olyan szabályozást kell kidolgoznia és végrehajtania, amely átalakítja a kritikus infrastruktúrák üzemeltetőire vonatkozó bejelentési kötelezettségeket. Az érintett vállalkozásoknak a végleges szabály hatálybalépése után jelenteniük kell a CISA felé a törvényben meghatározott incidenseket és zsarolóvírus-támadásokat. A CIRCIA alapján a kritikus infrastruktúrához tartozó szervezetek kötelesek a jelentős kibertámadásokat legkésőbb 72 órán belül jelenteni a CISA számára attól az időponttól számítva, hogy észszerűen megállapították az incidens bekövetkezését. Emellett minden szövetségi ügynökségnek a hozzá beérkező kibertámadási jelentéseket 24 órán belül továbbítania kell a CISA részére. A szabályozás célja egy gyors és központosított incidensinformációs rendszer kialakítása a kritikus infrastruktúrák védelmének erősítése érdekében. Ezek a bejelentések lehetővé teszik majd a CISA számára, hogy a támadások áldozatainak gyors és hatékony segítséget nyújtson, a különböző ágazatokból beérkező jelentéseket elemezze a minták azonosítása érdekében, és ezeket az adatokat azonnal megossza a védelemért felelős többi szervvel, valamint hogy figyelmeztesse a potenciális további áldozatokat.

A jogszabályt 2022-ben fogadták el, azonban a végrehajtási szabályok kialakítása jelen kézirat elkészültekor még nem zárult le. A CISA hivatalos tájékoztatása szerint a végrehajtási folyamat még tart, és a szabályok nem alkalmazandók addig, amíg a végleges rendelet hatályba nem lép. A hatóság jelen kézirat lezárásakor, 2026 júniusában az iparági szereplők, vállalatok és szakmai szervezetek visszajelzéseit dolgozza fel annak érdekében, hogy a szabályozás egyszerre legyen végrehajtható és hatékony. Ennek részeként 2026-ban további konzultációkat és *town hall* egyeztetéseket is szerveztek, különösen a *compliance* terhek, az incidensdefiníciók és az adatmegosztási kötelezettségek pontosítása érdekében.

A következő lépések közé tartozik a végleges végrehajtási rendelet elfogadása, amely várhatóan pontosítani fogja a *covered cyber incident* fogalmát, az érintett

⁹ *Statement on the National Cybersecurity Strategy 2023*, 1.2. fejezet.

¹⁰ *Cyber Incident Reporting for Critical Infrastructure Act of 2022*.

¹¹ BLAIR-FRASIER 2023.

szervezetek körét, a jelentések tartalmi követelményeit, valamint a végrehajtási és szankcionálási mechanizmusokat.

A CISA tájékoztatása alapján a végleges szabályozás elfogadását követően egy további átmeneti időszak következik majd, amely alatt az érintett szervezetek felkészülhetnek az új kötelezettségek teljesítésére. A CIRCIA ezért jelenleg még nem tekinthető teljesen implementált rendszernek, mindazonáltal már most jól látható, hogy az amerikai kibervédelmi szabályozás egyik központi elemévé válik, különösen az incidensinformációk gyorsabb megosztása és a kritikus infrastruktúrák rezilienciájának erősítése terén.¹²

A CIRCIA elfogadása jelentős lépés a kritikus infrastruktúrák biztonságának megerősítése szempontjából, és mind az állami szervek, mind pedig a magánszektor szereplőinek támogatását élvezi. Az érintettek nyilatkozatai szerint az új szabályozás elkerülhetetlen volt, mivel a korábbi, önszabályozáson alapuló rendszer nem volt alkalmas arra, hogy megvédje az Egyesült Államok érdekeit. A kiberbiztonsági incidensekre vonatkozó információk megosztása, még ha átszűrte, feldolgozott formában is, de lehetővé teszi a támadások elemzését és a védekezés hatékonyságának javítását.¹³

A kiberbiztonsági célú információmegosztás fő szervei

CISA

A DHS CISA az elsődleges szövetségi minisztérium, amely a kritikus infrastruktúrák védelmével és a kiberbiztonság előmozdításával foglalkozik. A CISA működteti és felügyeli a magánszektor és a közsféra szervezetei közötti információmegosztási programokat.¹⁴

A CISA emellett aktívan részt vesz a nemzetközi együttműködésekben. Ennek célja, hogy növelje a kiberbiztonság ellenálló képességének szintjét, és az NKS-sel összhangban a kiberbiztonsági intézkedéseket terhelte a fogyasztókról a széles körű eszközökkel rendelkező szervezetekre, a magán- és a közsféra intézményeire hárítsa.¹⁵

Information Sharing and Analysis Centers

Az ISAC-ek az Egyesült Államok kritikus infrastruktúráinak kibervédelmében meghatározó szerepet betöltő, jellemzően nonprofit alapon működő, ágazatspecifikus szervezetek, amelyeket a kritikus infrastruktúrák tulajdonosai és üzemeltetői hoztak létre és irányítanak. Feladatuk a kiber- és fizikai fenyegetésekkel kapcsolatos információk gyűjtése, elemzése és megosztása a tagok, más ágazatok és kormányzati szervek között. Emellett olyan eszközök és ajánlások biztosítása, amelyek támogatják a kockázatok mérséklését és a reziliencia növelését. Az információmegosztás mellett koordinálják

¹² *Cyber Incident Reporting for Critical Infrastructure Act of 2022* 2022.

¹³ Cybersecurity and Infrastructure Security Agency [é. n.].

¹⁴ SEFFERS 2023.

¹⁵ *Presidential Decision Directive 63* 1998.

az incidensekre adott válaszlépéseket, valamint hozzájárulnak az egységes operatív helyzetkép kialakításához.¹⁶

Az ISAC-ek az állami kritikusinfrastruktúra-védelem fontos kiegészítői, mivel számos szervezet folyamatos fenyegetésfigyelő és incidensjelentő képességgel rendelkezik, továbbá ágazatspecifikus szakértelmet biztosít. Működésük hatékonysága nagymértékben függ a tagok közötti önkéntes információmegosztástól, az együttműködési hajlandóságtól és az eltérő technikai felkészültségtől.¹⁷ Emellett az információáramlás sok esetben informális vagy decentralizált kommunikációs csatornákon – például e-hírleveleken és riasztási e-maileken – keresztül történik, ami korlátozhatja az egységes és gyors reagálást.¹⁸

A kritikus infrastruktúrák információmegosztási rendszerének kihívásai

A kiberbiztonsági célú információmegosztás különböző hálózati modellek szerint valósulhat meg. A szakirodalom alapvetően központosított (*centralized*), decentralizált vagy közvetlen résztvevők közötti (*peer-to-peer*), valamint elosztott (*distributed*) architektúrákat különböztet meg, amelyek az információáramlás módjában és a koordináció szintjében térnek el egymástól. A gyakorlatban a modellek nem feltétlenül különülnek el élesen a bemutatott kategóriák szerint, és több modell tulajdonságait ötvöző hibrid megoldások is kialakulhatnak.

A központosított modell tipikus formája a központi elosztó jellegű (*hub-and-spoke*) architektúra, amelyben egy központi szereplő fogadja és továbbítja a résztvevőktől érkező információkat. Előnye az egységes koordináció és a standardizált adatkezelés, ugyanakkor a központi csomópont egyetlen hibapontot (*single point of failure*) jelenthet, és vonzó célpont lehet a támadók számára.

A decentralizált vagy *peer-to-peer* modellben nincs központi koordináló szereplő, a résztvevők közvetlenül osztják meg egymással az információkat. Ez gyorsabb és rugalmasabb működést tesz lehetővé, valamint csökkenti a centralizációból eredő kockázatokat. Hátránya ugyanakkor, hogy nehezebb biztosítani az egységes szabványokat és az interoperabilitást.

A *distributed* architektúrában szintén nincs központi csomópont, azonban minden résztvevő azonos hozzáférési és megosztási jogosultságokkal rendelkezik.¹⁹ Az erőforrások és az adatkezelés elosztott módon működnek, ami javíthatja a skálázhatóságot és a rendelkezésre állást. Ugyanakkor ezek a rendszerek technikailag összetettebbek és nehezebben fenntarthatók.²⁰

Megfelelő működés esetén egy központi szerv nyílt, standardizált adatformátumok és információmegosztási protokollok használatával biztosíthatja a szervezetek közötti interoperabilitást annak érdekében, hogy a kiberfenyegetésekkel kapcsolatos

¹⁶ National Council of ISACs 2016.

¹⁷ Cybersecurity and Infrastructure Security Agency 2016.

¹⁸ National Council of ISACs 2021b.

¹⁹ ALAEIFAR et al. 2024.

²⁰ BAKIS–WANG 2017.

információk gyorsan és hatékonyan áramolhassanak. A központosított rendszer tipikus példái az ISAC-ek. Az ISAC-ek ágazati központi platformot biztosítanak a kiberfenyegetésekkel (és sok esetben kritikus infrastruktúrával) kapcsolatos információk összegyűjtéséhez, és elősegítik az információk aktív áramlását a magán- és a közszféra között. Habár az ISAC-ek értékes szereplői az Egyesült Államok kibervédelmének, számos kihívással is szembesülnek.

Egy információmegosztási rendszer akkor működik megfelelő részvétel mellett, ha az adott kritikusinfrastruktúra-szektor szereplőinek nem csak korlátozott része vesz részt aktívan az információcserében, az incidensjelentések száma és gyakorisága elegendő a releváns fenyegetési mintázatok azonosításához, illetve a megosztott információk kellően időszerűek és konkrétak ahhoz, hogy operatív védekezési intézkedések alapjául szolgáljanak. A rendszerek hatékonysága különösen akkor csökken, ha a résztvevők jelentős része passzívan, információfogyasztóként van jelen, miközben csak kevés szervezet járul hozzá ténylegesen új fenyegetési adatokkal. Az ISAC-ek esetében azonban ezek az elvárások nem teljesülnek teljes egészében.

A részvételi hajlandóság növelésének szükségességét több ISAC és az ISAC-ek ernyőszervezete, a National Council of ISACs is hangsúlyozta. Jelenleg az információmegosztás gyakorisága és a részvétel elterjedtsége egyaránt a kívánatos szint alatt van. A National Council of ISACs által kiadott fehér könyv kötelező jelentési rendszer bevezetésére tett javaslatot.²¹ A CIRCIA által elindított szabályozási folyamat és a CISA szabályozási kötelezettségei alapján úgy tűnik, ezen a területen jelentős előrelépések történhetnek, de a kritikusinfrastruktúra-ágazatok számos szereplőjének részvétele még mindig nem biztosított.

Az ISAC-ek számára továbbra is kihívást jelent a szervezetek szélesebb körének bevonása, ami káros hatással van a megosztott információk mennyiségére és minőségére. Rob Labbé, a bányászati és fémipari ISAC vezérigazgatója és információbiztonsági vezetője (*chief information security officer, CISO*) kijelentette, hogy az információmegosztás működése a jelenlegi formájában többnyire a nagyobb, jelentős erőforrásokkal és képességekkel rendelkező szervezeteknek kedvez. A kisebb vállalatok azonban, amelyeknek nincsenek megfelelő informatikai képességeik, nem tudnak részt venni az információmegosztásban.²² Egyes ISAC-ek nehezen tudják bevonni a szektor szereplőinek széles körét, mivel a tagság önkéntes, ami tovább korlátozhatja az információmegosztás hatékonyságát.²³

A megosztott információk minősége szintén a kritikus infrastruktúrák szektoraiban működő ISAC-rendszer egyik gyenge pontja. A tagok által megosztott, támadásokkal és sebezhetőséggel kapcsolatos információk általában nem alkalmasak a hatékony védekezés elősegítésére, mivel az információmegosztásra csak azután kerül sor, hogy a támadások közvetlen veszélye fennáll. A legtöbb esetben a késedelem miatt a támadásokat nem lehet elhárítani anélkül, hogy komoly károk keletkeznének. A késedelem oka részben az ISAC-ek *hub-and-spoke* jellege, részben az érzékeny információk más piaci szereplőkkel és a kormányzattal való megosztásától való általános vonakodás. Ennek a tartózkodó magatartásnak számos oka van. Ezek lehetnek jogi akadályok,

²¹ LABBÉ 2017.

²² TURETSKY–NUSSBAUM–TATAR 2020.

²³ FLEMING–GOLDSTEIN 2012.

mint például a versenyjogi tilalmak, valamint a harmadik felekkel szembeni felelősségi kérdések, az információk üzleti titok jellege és a lehetséges hatósági eljárásoktól való félelem.²⁴

A vállalatok vagy visszatartják az információkat, vagy a *hubokat* (az ISAC-eket) használják közvetítőként, hogy az érzékeny adataik ne kerüljenek veszélybe. Mivel ezen folyamat, a feldolgozás, szűrés, elemzés és terjesztés időigényes, az információmegosztással járó előnyök lényegesen csökkennek. Továbbá a megosztott információk túl általánosak lehetnek ahhoz, hogy konkrét intézkedéseket lehessen fogantatni a felhasználásukkal.²⁵

A hatékony információmegosztási mechanizmus működtetése emellett pénzügyi terhet is ró a vállalatokra, különösen a kis- és középvállalkozásokra. A szövetségi kormány politikája régóta támogatja, hogy a kiberbiztonsági információmegosztás hangsúlya a magánszektorba kerüljön. Az új kiberbiztonsági stratégia szintén a magánszektorbeli információmegosztás híve. A kormányzati erőfeszítések azonban nem lépték túl a jogszabályi keretek megalkotását. Ezen rendelkezések egy része ráadásul számos potenciális felelősségi kérdést vetett fel a magánszektor azon szereplői számára, amelyek részt kívántak volna venni az információcserében, és így a jelentkezők számának csökkenéséhez vezetett.²⁶ A szövetségi kormány csak néhány ISAC számára biztosít szövetségi finanszírozást (például Multi-State ISAC, Electricity ISAC). Ezért sok ISAC rákényszerül a tagdíjak alapján való működésre, ami tovább növeli a vállalkozások kiberbiztonsággal kapcsolatos, már így is jelentős terheit.²⁷

Ahhoz, hogy a magánszektorban hatékony és általánosan elterjedt információmegosztási rendszer jöjjön létre, az információcserében való részvétel határhasznának meg kell haladnia a költségeket. A szervezetek számára a részvétel költségeit jelenthetik a tagsági díjak, a technikai integráció, a *compliance* terhek, valamint az érzékeny információk megosztásából eredő jogi és reputációs kockázatok. Ezzel szemben az információmegosztás előnyei közé tartozhat a korai fenyegetésészlelés, a gyorsabb incidenskezelés és a kibertámadásokból eredő károk mérséklése. Amennyiben azonban a megosztott információk nem kellően specifikusak, időszerűek vagy operatív módon felhasználhatók, a résztvevők számára a rendszerből származó előnyök nem feltétlenül haladják meg a részvétel költségeit.

Amint az a Government Accountability Office korábbi és a jelen kézirat lezárásakor hatályos jelentéseiből kiderül, a kritikus infrastruktúrákban érdekelt felek úgy érzik, hogy az információcserében való részvétel nem mindig előnyös számukra, mivel a specifikus, időszerű és hatékonyan felhasználható információk helyett korlátozott mennyiségű információt kapnak, és a részvételi költségek aránytalan pénzügyi terhet jelentenek számukra.²⁸ A jelentés szerint a kritikus infrastruktúrák tulajdonosai és üzemeltetői gyakran korlátozott finanszírozással és erőforrásokkal rendelkeznek; következésképpen nem mindig képesek hatékonyan megosztani a kiberfenyegetésekkel kapcsolatos információkat a szövetségi ügynökségekkel, vagy esetleg más kritikus

²⁴ The MITRE Corporation 2012.

²⁵ NOLAN 2015.

²⁶ Government Accountability Office 2023.

²⁷ Government Accountability Office 2004.

²⁸ Government Accountability Office 2023.

kiberbiztonsági kérdések (elavult és sérülékeny berendezések cseréje) megoldását kell előnyben részesíteniük a információmegosztó rendszerek kiépítésével szemben.²⁹

A másik ok, amiért egyes szervezetek vonakodhatnak részt venni a magánszektor-beli kiberbiztonsági tárgyú információcserében, az úgynevezett potyautas-probléma. A vállalkozások attól tartanak, hogy az információmegosztás jelentős költségeit és kockázatait a megosztó szervezeten belüli társaik nem viszonozzák, és így az információmegosztás a jelentős költségek ellenére egyoldalúvá válik. Az információmegosztási rendszerekben való részvételt a vállalkozások elsődlegesen potyautas-probléma miatt kezelik fenntartásokkal.³⁰

A potyautas-probléma kapcsán szükséges megemlíteni, hogy a kiberbiztonsági információmegosztási rendszerek működésének egyik alapvető feltétele a résztvevők közötti bizalom megléte. A szervezetek attól tarthatnak, hogy az érzékeny incidensadatok megosztása reputációs, jogi vagy versenyjogi következményekkel járhat, ami visszatarthatja őket az aktív részvételtől. Ennek következtében a bizalom hiánya közvetlenül csökkentheti a megosztott információk mennyiségét, minőségét és időszerűségét.

Az interoperabilitás és az automatizálás szintén kulcsfontosságú kérdés, amely a hatékony kiberbiztonsági információmegosztási keretrendszer előfeltétele, és amelynek elérése napjaink egyik legjelentősebb kihívása.³¹ A *peer-to-peer* megosztási rendszereket használó szervezetek számára a különböző rendszerek közötti átjárhatóság megvalósítása nagyobb kihívás, mint a központosított rendszerek számára. Mindkét típusú megosztási rendszernek azonban kezelnie kell az automatizálással és a teljes interoperabilitás elérésével összefüggésben felmerülő technikai kihívásokat.

A bemutatott kihívások mellett azonban szükséges rögzíteni, hogy az ISAC-rendszereknek számos olyan előnyük van, amelyek miatt továbbra is a kritikus infrastruktúrák kibervédelmének meghatározó elemei. Az ágazatspecifikus működés lehetővé teszi a releváns fenyegetések gyorsabb azonosítását, elősegíti a bizalmi alapú együttműködést, valamint támogatja a korai figyelmeztetési és incidenskezelési mechanizmusok kialakítását. A központi koordináció emellett hozzájárulhat a standardizált adatkezeléshez és a különböző szervezetek közötti interoperabilitás biztosításához.

A bemutatott modellek és az ISAC-rendszerek tapasztalatai alapján a kiberbiztonsági információmegosztás hatékonyságát elsősorban a részvételi hajlandóság, a résztvevők közötti bizalom, a megosztott adatok minősége, az interoperabilitás, valamint a finanszírozási kérdések határozzák meg. Az ISAC-ek előnye, hogy ágazatspecifikus és koordinált keretet adnak a fenyegetési információk gyors megosztásának, ugyanakkor a rendszer hatékonyságát korlátozhatja az alacsony részvételi arány, a potyautas-probléma, valamint az érzékeny információk megosztásával kapcsolatos jogi és reputációs aggályokból eredő bizalomhiány. További problémát jelenthet, hogy a megosztott információk gyakran nem kellően konkrétak vagy időszerűek az operatív védekezés támogatásához, miközben az interoperabilitás és az automatizált adatmegosztás technikai megvalósítása továbbra is jelentős kihívás. Emellett a részvétel költségei – különösen a kisebb szervezetek számára – aránytalanul magasak lehetnek, ami hosszú távon a rendszer fenntarthatóságát és széles körű elterjedését is korlátozhatja.

²⁹ DYKSTRA et al. 2023.

³⁰ JOHNSON et al. 2016.

³¹ JOHNSON et al. 2016: 29.

Az információmegosztási rendszer lehetséges fejlesztési irányai

A fejlesztési irány alapjául szolgáló gyakorlatok

A vizsgált források alapján a kritikus infrastruktúrák megfelelő kiberbiztonságának eléréséhez a kulcs egy átfogó információmegosztó közösség megalapozása. Ez a közösség információkat szerezhetne be állami és magánszervezetektől, kormányzati forrásokból és nyílt forrásokból. A részvétel lehetővé tenné a vállalkozások számára, hogy kiegészítsék a meglévő fenyegetésekkel kapcsolatos információikat, és olyan hatékonyan felhasználható információkhoz jussanak hozzá, amelyek növelik a helyzetismeretüket (*situational awareness*), anélkül, hogy több információmegosztó szervezetben kellene részt venniük.³² A különböző ISAC-ek közötti kommunikáció már létező jelenség, és ígéretes eredményeket mutat,³³ de nem biztos, hogy a kritikus infrastruktúrák esetében az önkéntes alapú részvétel elegendő lesz egy olyan időszakban, amikor a potenciális támadók egyre kifinomultabb módszereket alkalmaznak.

A fent felsorolt problémák közül sok kapcsolódik az új szervezetek bevonásának nehézségeihez. Számos eszköz áll azonban rendelkezésre a magasabb részvétel elérésére.

A pénzügyi szervezeteket összefogó FS-ISAC jó példája, hogy nagyszámú és eltérő jellegű szervezetek között is lehetséges a hatékony információmegosztás. Önkéntes jellege és tagdíjakon alapuló finanszírozása ellenére tagsága 39 ország mintegy 7000 pénzügyi intézményéből áll. A pénzügyi szektor szereplőiből álló aktív felhasználóinak a száma folyamatosan növekszik, így a széles körű közösségi részvétel és az anonimizált platform hatékony felületet nyújt a cégek számára az információmegosztáshoz.³⁴ A kisebb és közepes méretű vállalkozásokat iparági szövetségeik képviselik.³⁵ Az FS-ISAC egy sikeres információmegosztó együttműködés példája, amely globális szintű szolgáltatásokat kínál tagjai számára.³⁶

Az ágazatközi információmegosztási és elemzőközpont koncepciója

A modell célja és alapelvei

A tanulmányban azonosított problémák alapján indokolt lehet egy közös, nem ágazatspecifikus kiberbiztonsági információmegosztó és elemzőközpont létrehozása a kritikus infrastruktúrák számára. A modell célja olyan központi platform kialakítása, amely képes biztosítani a kritikusinfrastruktúra-ágazatok közötti gyors, interoperábilis és biztonságos információáramlást, miközben csökkenti az információmegosztással kapcsolatos jogi, technikai és bizalmi akadályokat.

Egy, valamennyi kritikus infrastruktúrát átfogó, közös információmegosztási platform abból a szempontból is hasznos lenne, hogy kiküszöbölhetné az egyes

³² National Council of ISACs 2021a.

³³ FS-ISAC 2023.

³⁴ ATKINS–LAWSON 2021.

³⁵ CARLSON et al. 2017.

³⁶ Government Accountability Office 2023.

információk eltérő értékelésének hátrányait. Az információt fogadó szervezeteknek eltérő elképzeléseik lehetnek a kiberfenyegetésekről, ezért előfordulhat, hogy egyes információkat figyelmen kívül hagynak vagy alacsony fenyegetettségű szintűnek minősítenek. Ágazatközi együttműködésre van szükség ahhoz, hogy a kritikus infrastruktúrák kiberbiztonsági keretrendszere rugalmas legyen. A kritikus ágazatok ugyanis kölcsönösen függenek egymástól, számos szolgáltatáson osztoznak, és ugyanazon támadók célpontjai lehetnek. Egy jól működő ágazatközi partnerség megvalósításához elengedhetetlen a vállalatok közötti gördülékeny kommunikáció, azonban ennek eléréséhez kormányzati beavatkozásra is szükség van a bürokratikus problémák leküzdése és egy semleges szervezeti keret biztosítása érdekében.³⁷

A modell szereplői és az adatáramlás mechanizmusa

A rendszer szereplői közé tartoznának a kritikus infrastruktúrák üzemeltetői, az ágazati ISAC-ek, a szövetségi kormányzati szervek – különösen a CISA –, valamint adott esetben külső fenyegetésfelderítő és incidenskezelő szervezetek. A modell *hub-and-spoke* jelleggel működne, ahol a központi elemzőközpont fogadná, szűrné, anonimizálná és elemezné a beérkező adatokat, majd azokat standardizált formában osztaná vissza a résztvevők felé.

A közös elemzőközpont átfogó képpel rendelkezne a kiberbiztonsági helyzetről, és olyan tudást összpontosítana, amely lehetővé tenné a megfelelő információk megosztását a kiberfenyegetésekről a kritikus infrastruktúrák valamennyi szereplőjével.³⁸ A közös információmegosztási platform az adatok minőségének javulását is eredményezné. Az ISAC-ek között már most is létezik információmegosztás, mivel felismerték, hogy tagságuk átfedésben van, és a rendelkezésükre álló információk diverzitása megerősítheti ellenálló képességüket. Ezért ha egy ISAC értékes információkhoz jut, jelentős előnyökkel járhat, ha azokat a tagságán túli szervezetekkel is megosztja.³⁹ A közös megosztási folyamatban való kötelező részvétel egy lépéssel meghaladná a jelenlegi rendszert, és segítené elérni a megfelelő adatmennyiséghez és -minőséghez szükséges, kellő mértékű vállalati részvételt.

Egy ilyen közös platform vonzóbbá tenné az információcserében való részvételt a kis- és nagyvállalatok számára is. Olyan korai figyelmeztető rendszerként szolgálna, amelyből minden részt vevő szervezet profitálhatna. A szervezetek tapasztalataik bejelentésével hozzájárulnának a központ tudásbázisához, és ezáltal segítenék a központi szervet abban, hogy megértse a támadások jellegét és méretét. Cserébe a KKV-k naprakész, hatékonyan felhasználható információkat kapnának olyan fenyegetésekről, amelyeket egyedül csak korlátozottan tudnának észlelni. Az indikátorokat beküldő nagyobb szervezetek számára előnyt jelentene, hogy azonnali visszajelzést, megerősítést és közösségi tapasztalatomegosztást kapnának a hálózatukban észlelt fenyegetések jelentőségével kapcsolatban. Az ágazati különbségek, valamint az érintett vállalatok jelentős száma miatti bizalmatlanság kezelése érdekében lehetőséget kell biztosítani

³⁷ TOSH et al. 2015.

³⁸ TURETSKY–NUSSBAUM–TATAR 2020.

³⁹ ATKINS–LAWSON 2021.

a szervezeten belüli alcsoportok kialakítására. Mivel azonban az új rendszer fő célja, hogy átfogó legyen, biztosítani kell, hogy ne alakuljanak ki zárványok, és megfelelő intézkedések szavatolják, hogy a biztonsági fejlesztéseket a nagyvállalatokon túl az ágazat többi részére is kiterjesszék.⁴⁰ Így a vállalatok nemcsak a saját iparáguk „buborékából”, hanem a kapcsolódó szervezetektől is kapnának információkat, és ebből közös hasznuk származna.⁴¹

Interoperabilitás és automatizált információmegosztás

A rendszer egyik alapvető eleme az interoperabilitás biztosítása lenne. Az interoperabilitás eléréséhez az adatmegosztásban részt vevő szervezeteknek meg kell állapodniuk az alkalmazandó adatformátumban és a módszertanban. Ezen peremfeltételek lehetővé tennék az automatizált információmegosztást is.⁴² Egy közös, nem ágazatspecifikus információmegosztó és elemzőközpont azért lenne hasznos, mert így a szervezetek elkerülhetnék a közvetlen információmegosztásból eredő versenyjogi és üzleti titokkal kapcsolatos kockázatokat, és a lehető legtöbb résztvevőt lehetne elérni. A központosított információmegosztó rendszer másik előnye, hogy megkönnyíti az anonim információmegosztást. A tanulmányok szerint az anonim információmegosztás ösztönözné a részvételt és enyhítené a potyautas-problémát, amely a fent említettek szerint az információmegosztás egyik fő akadálya.

Az automatizált információmegosztás hozzáadása ehhez az átfogó információmegosztási rendszerhez meghaladná az ágazati szintű védekezést, és a teljes kritikus infrastruktúrát magában foglaló, rendszerszintű védelmet eredményezne. Az automatizálás a lassú információáramlás problémáját is megoldhatná, ami a jelenlegi rendszer egyik fő kritikája. Ez lehetővé tenné a magasan képzett, nemzetállami hátterű támadások kezelését, ami napjainkban még a több milliárd dolláros árbevételű vállalatok, például a nagyobb bankok számára is nehézséget okoz.⁴³

Bizalom, anonimizálás és hozzáférés-kezelés

A modell működésének előfeltétele a résztvevők közötti bizalom erősítése. Ennek érdekében a platformnak támogatnia kellene az anonim vagy részben anonimizált információmegosztást, valamint differenciált hozzáférési szinteket kellene létrehoznia. Ez csökkenthetné a reputációs, versenyjogi és felelősségi kockázatokkal kapcsolatos aggályokat, amelyek jelenleg sok szervezetet visszatartanak az aktív részvételtől. Sok vállalkozás ugyanis az információbiztonsági aggályai miatt nem vesz részt a kiberbiztonsági információmegosztás rendszerében. Attól tartanak, hogy érzékeny adataik rossz kezekbe kerülhetnek, ami a jogszabályi követelmények megsértése miatt hatósági vizsgálathoz vezethet, vagy egyéb felelősségvállalási kötelezettséggel járhat. Továbbá

⁴⁰ LABBÉ 2017.

⁴¹ ATKINS–LAWSON 2021.

⁴² ATKINS–LAWSON 2021.

⁴³ NWEKE–WOLTHUSEN 2020.

egyes érzékeny információk, üzleti titkok megosztása esetén a vezető beosztású munkavállalók polgári jogi felelőssége is felmerül. Ezen aggályok csökkentése érdekében az FS-ISAC jelzőlámpás protokolljának átemelése lenne indokolt az ágazatokon felüli információmegosztásba.

A *traffic light protocol* (TLP) a kibervédelmi információk megosztására szolgáló besorolási rendszer, amelynek célja annak meghatározása, hogy az adott információ milyen körben és milyen korlátozások mellett osztható tovább. A TLP öt kategóriát különböztet meg. A TLP:RED a legszigorúbb szint, amely esetében az információ kizárólag a közvetlen címzettek között osztható meg, további terjesztés nélkül. A TLP:AMBER+STRICT kategóriába tartozó információk csak az adott szervezeten belül oszthatók meg, kizárólag azokkal a személyekkel, akik számára az információ ismerete feltétlenül szükséges. Ezt a kategóriát jellemzően olyan esetekben alkalmazzák, amikor az információ szélesebb körű megosztása adatvédelmi, reputációs vagy működési kockázatot hordozna. A TLP:AMBER ennél szélesebb megosztást tesz lehetővé, mivel az információ a címzett szervezetén kívül is továbbítható olyan partnerek vagy ügyfelek részére, akiknek az információ a védekezéshez szükséges, azonban nyilvánosságra továbbra sem hozható. A TLP:GREEN kategóriába sorolt információk megoszthatók egy adott közösségen vagy szektoron belül, azonban nyilvános közzétételük nem megengedett. Ezzel szemben a TLP:CLEAR kategóriába tartozó információk szabadon terjeszthetők és nyilvánosan is hozzáférhetővé tehetők, mivel nem tartalmaznak érzékeny vagy korlátozott adatokat.⁴⁴

Ez a módszer eloszthatja az információval való visszaéléstől vagy a hatósági intézkedésektől való félelmet, és ezáltal előrelépést érhet el a kritikus infrastruktúrákban érdekelt felek között megosztott információk minősége és mennyisége vonatkozásában. További előny, hogy egy központi információmegosztó szervezet szűrni tudná a tagok által megosztott adatokat, hogy elkerülje az érzékeny vagy minősített információk nyilvánosságra kerülését.

Egy központi információmegosztó szervben lévő tagság fent említett előnyeinek elegendőnek kellene lenniük ahhoz, hogy meggyőzzék a vállalatokat a csatlakozásról. Mivel azonban a hasonló szervezetek hagyományosan nehezen tudtak magas taglétszámot elérni, az eddigi tapasztalatok alapján a kritikusinfrastruktúra-ágazatok vállalatai számára indokolt a kötelező tagság, mivel sebezhetőségük jelentős nemzetbiztonsági fenyegetést is jelent. A kötelező részvétel nem tekinthető felesleges tehernek, mivel a résztvevők élveznék a magas színvonalú, naprakész információk előnyeit, és kevésbé lennének kiszolgáltatottak a támadásoknak.

Finanszírozás és intézményi felügyelet

Mindezen célok elérése érdekében a szervezeteknek további erőforrásokat kell befektetniük annak biztosítására, hogy a megosztott kiberfenyegetettségi információk megfeleljenek az automatizált információmegosztás és az interoperabilitás feltételeinek, és a többi

⁴⁴ Cybersecurity and Infrastructure Security Agency 2022.

részt vevő szervezet által könnyen újrafelhasználhatók legyenek.⁴⁵ Annak érdekében, hogy a vállalatok könnyebben viselhessék az új információmegosztási rendszerhez való csatlakozás költségeit, a szervezet részleges szövetségi finanszírozása lenne indokolt. Mivel mind a magánszereplők, mind a kormányzat haszonélvezői a rendszernek, a pénzügyi terhek megosztása is szükségszerű. A kormányzat így enyhítheti a kritikus infrastruktúrákat fenyegető nemzetbiztonsági veszélyeket, míg a magánszereplők magas színvonalú és hatékonyan felhasználható kiberbiztonsági információkhoz juthatnak hozzá.

A javasolt modell nem egy új, a CISA-tól független szövetségi hatóság létrehozására irányulna, hanem a CISA meglévő koordinációs és kibervédelmi feladataira épülne. A CISA felügyeleti és stratégiai koordinációs szerepet töltené be, biztosítaná az interoperabilitási és adatmegosztási szabványok kialakítását, valamint kapcsolatot teremtené a szövetségi szervek és a kritikus infrastruktúrák szereplői között. A platform operatív működtetését egy nonprofit szervezeti forma látná el a piaci szereplők és az ágazati ISAC-ek bevonásával, ami csökkenthetné a túlzott állami kontrollal kapcsolatos bizalmi aggályokat. Az adatkezelési felelősség megosztott módon érvényesülne: a részt vevő szervezetek felelnének az általuk megosztott adatok jogszerűségéért és pontosságáért, míg a központi platform feladata lenne az anonimizálás, a hozzáférési jogosultságok kezelése, valamint az érzékeny információk védelme. Ez a modell összhangban állna az NKS azon célkitűzésével, amely a kormányzati koordináció és a magánszektor aktív részvételének együttes erősítésére törekszik.

1. táblázat: Az ISAC és a javasolt elemzőplatform összehasonlítása

Azonosított probléma	Következmény	Javasolt megoldás
Alacsony részvételi hajlandóság	Korlátozott adatbázis és gyenge helyzetismeret	Kötelező részvétel a kritikus infrastruktúrák számára
Potyautas-probléma	Egyoldalú információmegosztás	Központi platform és közös előnyrendszer
Bizalomhiány	Információ-visszatartás	Anonimizálás és TLP-alapú hozzáférési rendszer
Eltérő adatminőség	Operatív szempontból nehezen használható információk	Központi elemzés és validáció
Lassú információáramlás	Késedelmes reagálás	Automatizált információmegosztás
Interoperabilitási problémák	Rendszerek közötti inkompatibilitás	Standardizált adatformátumok és protokollok
Kkv-k korlátozott részvétele	Információs aszimmetria	Részleges szövetségi finanszírozás
Ágazati elszigeteltség	Rendszerszintű fenyegetések felismerésének hiánya	Ágazatközi közös elemzőközpont
Jogi és reputációs kockázatok	Passzív tagság	Nonprofit működtetés és CISA-felügyelet
Széttagolt helyzetkép	Korlátozott stratégiai elemzés	Központi, aggregált fenyegetéselemzés

Forrás: a szerző szerkesztése

⁴⁵ NWEKE-WOLTHUSEN 2020.

A központi intézmény pontos szervezeti felépítése és jogi formája szétfeszítené ezen tanulmány kereteit. Általános megállapításként azonban a platformot a részt vevő vállalkozások és más érdekeltek egy nonprofit szervezeten keresztül működtetnék, a kormányzat felügyelete mellett. Ez összhangban lenne az NKS-sel is, amely a piaci szereplők aktívabb részvételét szeretné elérni.

Az ISAC-alapú rendszer és a tanulmányban javasolt ágazatközi közös elemző-platform közötti főbb különbségeket az 1. táblázat foglalja össze.

A koncepció korlátai

A bemutatott kutatásokból levonható következtetések alapján ez a rendszer csak a kritikus infrastruktúrákban lenne alkalmas ágazatközi információmegosztás megvalósítására. Egy ennél szélesebb körű rendszer olyan sok vállalatot vonna be, hogy az információ mennyisége és az érintettek száma kezelhetetlen lenne, és az egész projektet kudarcra ítélné.

Az iparági szereplők körében is megjelent egy kizárólag állami irányítású rendszer korlátait jelző álláspont, miszerint a túlzottan centralizált, kormányzatvezérelt információmegosztási modellek csökkenthetik a vállalkozások részvételi hajlandóságát és bizalmát.⁴⁶ Ezért a javasolt rendszer hatékony működésének előfeltétele lehet egy olyan hibrid irányítási modell kialakítása, amelyben a CISA koordinációs és felügyeleti szerepet lát el, míg az operatív működésben az ISAC-ek és a magánszektor szereplői is aktívan részt vesznek.

Konklúzió

A kritikus infrastruktúrák kibervédelme korunk egyik legfontosabb biztonságstudományi kérdése. A kiberfenyegetések változó dinamikája, valamint a probléma összetettsége miatt fennálló túlszabályozás veszélye csak súlyosbítja a problémát. Ez ugyanis arra kényszeríti a vállalkozásokat, hogy szűkös erőforrásaikat a kiberbiztonsági védelmük fokozása helyett a szabályozási követelményeknek való megfelelésre fordítsák. Ezen túlmenően a kiberbiztonsági szabványokról szóló közmegegyezés hiánya hozzájárul az e szabályozások hatálya alá tartozó szervezetekkel és rendszerekkel kapcsolatos zűrzavarhoz, például a kritikusinfrastruktúra-ágazatok eltérő kijelölése és a különböző szabályozási keretek eltérő alkalmazási köre miatt az Egyesült Államokban.⁴⁷

A tanulmány arra a kérdésre kereste a választ, hogy az Egyesült Államok kritikus infrastruktúráinak kiberbiztonsági információmegosztási rendszere milyen strukturális és szabályozási kihívások miatt nem képes minden esetben biztosítani a fenyegetési információk hatékony és időszerű áramlását. A vizsgálat alapján megállapítható, hogy az ISAC-rendszer továbbra is a kritikus infrastruktúrák kibervédelmének meghatározó eleme, azonban működését jelentősen korlátozzák a részvételi hajlandóság

⁴⁶ WEISS 2025.

⁴⁷ World Economic Forum 2023.

hiányosságai, a bizalommal kapcsolatos problémák, az információk változó minősége, az interoperabilitási nehézségek, valamint a finanszírozási és erőforrásbeli korlátok. A kutatás rámutatott arra is, hogy az információmegosztási rendszerek hatékonysága nem kizárólag technológiai kérdés, hanem nagymértékben függ a megfelelő intézményi ösztönzők, a bizalmi mechanizmusok és a szabályozási környezet kialakításától.

A tanulmány alapján megállapítható, hogy ezen nehézségek egy hatékonyabb, interoperábilisabb és szélesebb részvételen alapuló kiberbiztonsági információmegosztási rendszerrel enyhíthetők lennének. Az NKS által biztosított szabályozási keret, valamint az ISAC-rendszerek működésével kapcsolatban felhalmozott több évtizedes tapasztalat megfelelő alapot teremthet egy fejlettebb információmegosztási modell kialakításához. A kutatás eredményei alapján az ISAC-rendszer jelenlegi hiányosságainak kezelése, az interoperabilitás és az automatizáció fejlesztése, valamint a kormányzati és magánszektorbeli szereplők közötti együttműködés erősítése hozzájárulhatna a kritikus infrastruktúrák kibertámadásokkal szembeni ellenálló képességének növeléséhez. Egy ilyen rendszer nemcsak az Egyesült Államok kritikus infrastruktúrák védelmével kapcsolatos stratégiai célkitűzéseinek megvalósítását támogathatná, hanem szabályozási és intézményi modellként is szolgálhatna más államok és jogalkotók számára.

A tanulmány megállapításai európai és magyar szempontból is relevánsak. Az Európai Unió az elmúlt években az Európai Parlament és a Tanács 2022/2555 sz. irányelve (NIS2 irányelv), az Európai Parlament és a Tanács 2022/2557 sz. irányelve (CER-irányelv), valamint az Európai Unió Kiberbiztonsági Ügynökség (ENISA) koordinációs tevékenysége révén egyre nagyobb hangsúlyt helyez a kritikus infrastruktúrák kibervédelmére, az interoperabilitás erősítésére és az ágazatok közötti együttműködés fejlesztésére. Az EU energiaszektorral kapcsolatos kibervédelmi politikái is arra épülnek, hogy a kritikus infrastruktúrák biztonsága nem kizárólag nemzeti, hanem uniós szintű rezilienciakérdés, különösen a határokon átnyúló digitális és energetikai rendszerek esetében.

Magyarország számára a kutatás azért lehet különösen jelentős, mert a NIS2 irányelv átültetése és a kritikus infrastruktúrák kibervédelmének megerősítése folyamatban van. A hazai szabályozási és intézményi környezet számára hasznos tanulságként szolgálhat az amerikai ISAC-rendszer működésének vizsgálata, különösen a részvételi hajlandóság, az interoperabilitás, az automatizált információmegosztás és az állami-magánszektorbeli együttműködés kérdéseiben. A tanulmányban javasolt közös, ágazatokon átívelő elemzőplatform koncepciója hosszabb távon az európai és magyar kibervédelmi együttműködések fejlesztéséhez is hozzájárulhatna, különösen az energia-, pénzügyi, közlekedési és egészségügyi szektorok közötti koordináció erősítésével.

Felhasznált irodalom

ALAEIFAR, Poopak et al. (2024): Current Approaches and Future Directions for Cyber Threat Intelligence Sharing: A Survey. *Journal of Information Security and Applications*, 83. Online: <https://doi.org/10.1016/j.jisa.2024.103786>

- ATKINS, Sean – LAWSON, Chapell (2021): Cooperation amidst Competition: Cybersecurity Partnership in the US Financial Services Sector. *Journal of Cybersecurity*, 7(1). Online: <https://doi.org/10.1093/cybsec/tyab024>
- BAKIS, Bruce J. – WANG, Edward D. (2017): *Building a National Cyber Information-Sharing Ecosystem*. [H. n.]: The MITRE Corporation. Online: www.mitre.org/sites/default/files/2021-09/building-national-cyber-information-sharing-ecosystem-pr-17-1125.pdf
- BLAIR-FRASIER, Rachele (2023): Experts Weigh in on CIRCIA One Year Later. *Security Magazine*, 2023. március 31. Online: www.securitymagazine.com/articles/99138-experts-weigh-in-on-circia-one-year-later
- CARLSON, John et al. (2017): *Cybersecurity in the Financial Services Sector*. Online: www.jstor.org/stable/resrep20737
- Center for Strategic and International Studies [é. n.]: *Significant Cyber Events List*. Online: www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (2022). Online: www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia
- Cybersecurity and Infrastructure Security Agency [é. n.]: *Information Sharing*. Online: www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing
- Cybersecurity and Infrastructure Security Agency (2016): *Critical Infrastructure Threat Information Sharing Framework. A Reference Guide for the Critical Infrastructure Community*. Online: www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf
- Cybersecurity and Infrastructure Security Agency (2022): *Traffic Light Protocol (TLP) Definitions and Usage*. Online: www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage
- DYKSTRA, Josiah et al. (2023): Maximizing the Benefits from Sharing Cyber Threat Intelligence by Government Agencies and Department. *Journal of Cybersecurity*, 9(1). Online: <https://doi.org/10.1093/cybsec/tyad003>
- FLEMING, Mathew – GOLDSTEIN, Eric (2012): *Metrics for Measuring the Efficacy of Critical-Infrastructure-Centric Cybersecurity Information Sharing Efforts*. Online: <http://dx.doi.org/10.2139/ssrn.2201033>
- FS-ISAC (2023): *2023 Year in Review*. Online: www.fsisac.com/hubfs/EOY/23_YearInReview.pdf
- Government Accountability Office (2004): *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*. Online: www.gao.gov/products/gao-04-780
- Government Accountability Office (2023): *National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods*. Online: www.gao.gov/assets/d23105468.pdf
- GRIEGER, Gisela (2023): *The US Cybersecurity Posture under Biden*. European Parliamentary Research Service. Online: [www.europarl.europa.eu/RegData/etudes/ATAG/2023/753929/EPRS_ATA\(2023\)753929_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/ATAG/2023/753929/EPRS_ATA(2023)753929_EN.pdf)

- HUMPHREYS, Brian E. (2024): *The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience*. 2024. július 25. Congression Research Service. Online: www.congress.gov/crs-product/IF12716
- JOHNSON, Chris et al. (2016): *Guide to Cyber Threat Information Sharing*. Gaithersburg: National Institute of Standards and Technology. Online: <http://dx.doi.org/10.6028/NIST.SP.800-150>
- LABBÉ, Rob (2017): Building a Successful ISAC/ISAO – Don't Forget the Community. *LinkedIn*, 2017. október 2. Online: www.linkedin.com/pulse/building-successful-isacisao-dont-forget-community-rob-labbé/
- National Council of ISACs (2016): *Information Sharing and Analysis Centers (ISACs) and Their Role in Critical Infrastructure Protection*. Online: https://1d74b95c-e5fa-4920-9b2e-254ec35a1c46.filesusr.com/ugd/416668_2e3fd9c55185490abcf2d7828abfc4ca.pdf
- National Council of ISACs (2021a): *National Council of ISACs Congressional Update. Critical Infrastructure Information Sharing Successes and Opportunities*. Online: www.nationalisacs.org/_files/ugd/b8fa6c_4add9893be20400a925ca4868ec1e975.pdf
- National Council of ISACs (2021b): *NCI Principles on Mandatory Reporting*. Online: www.nationalisacs.org/_files/ugd/b8fa6c_deb4d9982b3a42a4b0d77992d1e75b73.pdf
- National Cybersecurity Strategy*. 2023. március. Online: <https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>
- NOLAN, Andrew (2015): *Cybersecurity and Information Sharing: Legal Challenges and Solutions*. Congression Research Service. Online: <https://sgp.fas.org/crs/intel/R43941.pdf>
- NWEKE, Livinus O. – WOLTHUSEN, Stephen (2020): Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure. In *2020 12th International Conference on Cyber Conflict*. Tallinn: NATO CCDCOE Publications, 63–78. Online: <https://doi.org/10.23919/CyCon49761.2020.9131721>
- President Trump's Cyber Strategy for America*. 2026. március. Washington: The White House. Online: www.whitehouse.gov/wp-content/uploads/2026/03/President-Trump's-Cyber-Strategy-for-America.pdf
- Presidential Decision Directive 63*. 1998. május 22. Washington D.C.: The White House. Online: <https://irp.fas.org/offdocs/pdd/pdd-63.htm>
- Presidential Policy Directive 21*. 2013. február 12. Washington D.C.: The White House. Online: www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf
- SEFFERS, George I. (2023): CISA Views Critical Infrastructure and Cybersecurity Through Global Lens. *The CyberEdge by Signal*, 2023. október 1. Online: www.afcea.org/signal-media/cyber-edge/cisa-views-critical-infrastructure-and-cybersecurity-through-global-lens
- The MITRE Corporation (2012): *Cyber Information-Sharing Models. An Overview*. Online: www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf
- TOSH, Deepak K. et al. (2015): Cyber-Investment and Cyberinformation Exchange Decision Modeling. In *17th IEEE International Conference on High Performance Computing and Communications, HPCC 2015, 7th IEEE International Symposium on Cyberspace Safety and Security, CSS 2015, and 12th IEEE International Conference on Embedded Software and Systems, ICESS 2015, New York, NY, USA, August 24–26,*

2015. 1219–1224. Online: www.cse.unr.edu/~shamik/research/papers/CSS-2015-CyberInfoSharingGame-accepted.pdf
- TURETSKY, David – NUSSBAUM, Brian – TATAR, Unul (2020): Cybersecurity Information Sharing Success Stories. *Lawfare*, 2020. július 15. Online: www.lawfaremedia.org/article/cybersecurity-information-sharing-success-stories
- WEISS, Errol (2025): Why a Government-Led AI-ISAC Is a Missed Opportunity. *LinkedIn*, 2025. július 24. Online: www.linkedin.com/pulse/why-government-led-ai-isac-missed-opportunity-errol-weiss-2wake/
- World Economic Forum (2023): *Response to the White House's Request on Harmonizing Cybersecurity Regulations*. Online: https://www3.weforum.org/docs/WEF_Response_to_the_White_House's_Request_on_Harmonizing_Cybersecurity_Regulations_2023.pdf