HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

A KIBERBIZTONSÁGI INFORMÁCIÓCSERE INTEROPERABILITÁSI KÉRDÉSEI

INTEROPERABILITY QUESTIONS OF CYBERSECURITY INFORMATION EXCHANGE

MUNK Sándor

(ORCID: 0000-0001-8576-308X)

munk.sandor@uni-nke.hu

Absztrakt

Napjaink társadalmi, gazdasági, és mindennapi tevékenysége egyre növekvő mértékben függ a kiberteret alkotó, globálisan összekapcsolt, decentralizált informatikai rendszerek és hálózatok által nyújtott szolgáltatásoktól.
A kiberbiztonság megteremtése és fenntartása a kiberbiztonsági szervezetek, az informatikai rendszereket, hálózatokat működtető szervezetek, az állampolgárok, és a média kiemelt jelentőségű közös feladata, amely több szereplőre kiterjedő és széleskörű együttműködést igényel.
Jelen publikáció – egy háromrészes sorozat zárásaként - a kiberbiztonsági szervezetek közötti információcsere interoperabilitási problémáit, követelményeit mutatja be, elemzi, kiemelten a kiberbiztonsági eseményekre, sérülékenységekre vonatkozó információk cseréjéhez kapcsolódóan.
A publikáció a KÖFOP-2.1.2-VEKOP-15-2016-00001 'A jó kormányzást megalapozó közszolgálat-fejlesztés' projekt támogatásával, a Kiberbiztonsági Ludovika Kiemelt Kutató-műhely keretében készült.

Kulcsszavak: *kiberbiztonság, kiberbiztonsági szervezetek, kiberbiztonsági információcsere, interoperabilitás*

Abstract

Today's social, economic, and every-day activities are increasingly dependent on the services provided by globally interconnected, decentralized IT systems and networks, the cyberspace.
Ensuring cyber security is a common task of cybersecurity organisations, IT system-network operators, citizens, and media, which requires wide range, extensive cooperation of these actors.
Recent paper – as a closing part of a three-part series - presents and analyses interoperability problems and requirements for information exchange between cyber security organizations, especially for cyber security events and vulnerability information.

Keywords: *cybersecurity, cybersecurity organisations, cybersecurity information exchange, interoperability*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.03.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.20.

BEVEZETÉS

Napjaink társadalmi, gazdasági, és mindennapi tevékenysége egyre növekvő mértékben függ a kiberteret alkotó, globálisan összekapcsolt, decentralizált informatikai rendszerek és hálózatok által nyújtott szolgáltatásoktól. Az informatikai szolgáltatások egyre jelentősebb mértékben járulnak hozzá az állami működés hatékonyságának, a vállalkozások eredményességének és versenyképességének, valamint az állampolgárok életminőségének javításához. A növekvő függőség egyben növekvő kiszolgáltatottságot, kockázatot is jelent, mivel az informatikai rendszerek, hálózatok, és az általuk kezelt adatok, információk biztonságának (bizalmasságának, sértetlenségének, és rendelkezésre állásának) megsértése maga után vonja az informatikai szolgáltatásokra épülő rendszerek, folyamatok, szolgáltatások biztonságának sérülését is, ami jelentős kihatással lehet az átfogó biztonság politikai, katonai, gazdasági, pénzügyi, és társadalmi dimenzióira is.

A kibertérben világszerte növekvő mértékben jelentkező kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a nemzeti kritikus infrastruktúra működtetésének biztosítására minden államnak, így – Magyarország Nemzeti Biztonsági Stratégiájában megfogalmazottak szerint – hazánknak is készen kell állnia. A kiberbiztonság megteremtése és fenntartása nem csak a kiberbiztonsági (információbiztonsági, informatikai biztonsági) szervezetek, hanem az informatikai rendszereket, hálózatokat működtető szervezetek, az állampolgárok, és a média kiemelt jelentőségű feladata.

A kibertér informatikai rendszereinek, hálózatainak globális, szövevényes összekapcsolódása következtében az egyik rendszer biztonságának sérülése elvezethet egy másik (más országban, más ágazatban működő) rendszer biztonságának sérüléséhez. Egy magán vállalkozás által üzemeltetett informatikai infrastruktúra támadásával támadhatóvá válnak az infrastruktúra szolgáltatásait igénybevevő kormányzati, gazdasági, és más informatikai rendszerek is. Az Internet lényegében bárhonnan könnyű útvonalat biztosít kibertámadások, kiberbűncselekmények végrehajtásához. Mindebből következik, hogy a kiberbiztonság fenntartása több szereplőre kiterjedő és széleskörű együttműködést igényel.

Jelen publikáció egy szélesebb körű, a kiberbiztonsági szervezetek információcsere igényeit, és az ehhez kapcsolódó interoperabilitási követelményeket vizsgáló kutatás harmadik részét képezi. Az elsőben rendszerezésre kerültek a kiberbiztonsági szervezetek főbb típusai, és ezek funkciói, feladatai. A második pedig a kiberbiztonsági szervezetek által kezelt, illetve a köztük áramló információk, és az információcsere alapvető jellemzőit tárgyalta.

Ezen publikáció célja a kiberbiztonsági szervezetek közötti információcseréhez kapcsolódóan felmerülő interoperabilitási problémák, követelmények bemutatása, elemzése, annak vizsgálata, hogy az információcserében érintett felek között milyen területeken vannak eltérések, amelyek – megfelelő megoldás alkalmazása nélkül – megnehezítik, vagy lehetetlenné teszik a jelentésmegőrző információcserét. Ennek érdekében a következőkben:

- összegezzük az interoperabilitás alapjait, a jelen publikációban is felhasznált legfontosabb fogalmait, állításait, majd megvizsgáljuk ennek a kiberbiztonsági információcserére vonatkozó sajátosságait;
- röviden értékeljük az interoperabilitás helyzetét a kiberbiztonsági információcsere során, és meghatározzuk jövőbeni alakulásának néhány lehetséges irányát;
- végül általában, illetve a két kiemelt információkörre vonatkozóan elemezzük az interoperabilitási követelményeket és a legfontosabb, megoldásra váró problémákat.

AZ INTEROPERABILITÁS ALAPJAI

Az interoperabilitás korunk népszerű, megkerülhetetlen szakkifejezése, amelynek jelző nélküli és jelzős változataival széles körben találkozhatunk. Bár e kifejezések értelmezéseiben sok a

közös, de számos eltérés is tapasztalható. A következőkben bemutatjuk az interoperabilitás jelen publikációban alkalmazott fogalmi alapjait, amelyek alapvetően egy korábbi publikációnkban [1] foglaltakra épülnek.

Az ***interoperabilitás*** általános értelemben együttes tevékenységre (működésre) való kölcsönös képesség. Az együttes tevékenység (együttműködés) értelmezhető tudatosan tevékenykedő szereplők (emberek, szervezetek), vagy meghatározott rendeltetéssel működő technikai rendszerek (eszközök, részegységek) között. Az előbbihez kapcsolódik a szervezeti/működési interoperabilitás fogalma, ami egyeztetett cél megvalósítása érdekében együttműködő szereplők között fennálló viszony, az eredményes és hatékony együttműködést biztosító átfogó, kölcsönös képesség, míg az utóbbit technikai interoperabilitásnak nevezzük. A szervezeti/működési interoperabilitás megvalósítása számos részterületen fennálló interoperabilitást igényel, ezek egyike – mivel együttműködés nem lehetséges információcsere nélkül – az információs interoperabilitás.

Az *információs interoperabilitás* különböző szereplők kölcsönös képessége információk közös értelmezésen alapuló, a hatékony együttműködéshez szükséges cseréjére. A meghatározásból láthatóan az információs interoperabilitás két alapvető összetevője az információcserére való képesség, és a kicserélt információk közös értelmezésére való képesség. Ezekhez kapcsolhatóak a nyelvi interoperabilitás, fogalmi interoperabilitás, és szellemi interoperabilitás fogalmai is.

Az információk közös értelmezésén alapuló cseréjére vonatkozó képesség ***három, egymásra épülő információs interoperabilitási szintre*** tagolható, amelyek a következők:

- az anyagi (fizikai) információ reprezentációkhoz kapcsolódó technikai;
- a logikai információ reprezentációkhoz (adatokhoz) kapcsolódó szintaktikai;
- valamint az információ reprezentációk jelentéséhez kapcsolódó szemantikai.

A legalsó szintet a *technikai szintű információs interoperabilitás* képezi, amely az információt hordozó anyagi (fizikai) reprezentációk cseréjére – előállítására, továbbítására, fogadására, megjelenítésére – vonatkozó képességek összessége. Ennek feltétele az adott fizikai reprezentációnak megfelelő, egymással "interoperábilis" technikai eszközök[1] megléte és rendeltetésszerű működése.

A *szintaktikai szintű információs interoperabilitás* az információkat hordozó adatok cseréjére vonatkozó képességek összessége, amelynek lényege az alkalmazott adatcsere formátumok előírásainak megfelelő[2] adatok kezelésére – előállítására, a technikai szint szolgáltatásaira épülő továbbítására, fogadására, és formai feldolgozására – vonatkozó képesség.

Az informatikai eszközök segítségével történő információcsere esetében az információk reprezentációi (adatok) bonyolult, egymásra épülő struktúrát alkotnak, amelynek alapja, elemi szintje napjainkban a bitsorozat, bitfolyam. Erre épülnek – akár több szinten – az információcsere során alkalmazott adat- és üzenetformátumok. Ennek feltétele az alkalmazott formátumokat kezelni képes szoftver összetevők megléte, és rendeltetésszerű működése.

Végül a *szemantikai szintű információs interoperabilitás* a legfelső szint, amely különböző szereplők kölcsönös képessége a hatékony együttműködéshez szükséges információ-reprezentációk – esetleges átalakítások közbeiktatásával történő – jelentésmegőrző cseréjére. Az együttműködő felek közötti információcsere során az információkat egyezményes jelrendszernek

[1] Vezetékes, vagy vezetéknélküli adatátviteli eszközök, adathordozók előállítására (írására) és felhasználására (olvasására) alkalmas berendezések.

[2] Pld. bináris, vagy karakteres számformátumok; karakterkészletek; dokumentum formátumok; hang-, kép-, video formátumok; formatizált üzenetformátumok, stb.

megfelelő adatokká kell alakítani, így továbbíthatóak, és a fogadónál az adat értelmezése során áll elő a továbbítani szánt információ.

A szemantikai szint lényege az információcsere során használt adatokhoz rendelt jelentés együttműködéshez szükséges mértékben azonos értelmezése. Vagyis hogy ugyanazon adathoz minden szereplő ugyanazt a jelentést rendelje[3], és azonos információkat azonos adatok formájában jelenítsen meg. Az adatok szándékolt, egyeztetett jelentésének feltétele a felek fogalomrendszerének kellő szintű azonossága, legalább harmóniája, ami ki kell terjedjen az adatcsere során közvetlenül nem is használt fogalmakra, információkra (pld. incidens, káros, alárendeltje, stb.)

Érdemes kihangsúlyozni, hogy az információs interoperabilitás és különböző szintjei vizsgálatának igazából csak akkor van jelentősége, kialakítására és fenntartására akkor van csak szükség, ha az együttműködő szereplők között valamilyen szempontból ***heterogenitás (különbözőség)*** áll fenn. Szervezetek, emberek közötti információcsere esetében ez a heterogenitás – a szinteknek megfelelően – fennállhat a közös (azonos) értelmezés, az alkalmazott adatformátumok, vagy a rendelkezésre álló technikai adatcsere lehetőségek hiányában, vagy ezek együttműködés szempontjából nem elégséges minőségében, szintjében.

Az ***informatikai interoperabilitás*** az információs interoperabilitáshoz kapcsolódó sajátos, informatikai eszközök, rendszerek között fennálló, az általuk kezelt adatok szándékolt jelentésüket, értelmezésüket megőrző - esetleges átalakítások közbeiktatásával történő – cseréjére vonatkozó kölcsönös képesség. Szerepe azzal született meg, hogy a szereplők már nem feltétlenül (egyes körülmények között nem is elsősorban) közvetlenül cserélnek információt egymással, hanem közvetve, akár kezdeményezésük, tudomásuk nélkül informatikai eszközeiken, rendszereiken keresztül. Erre példa lehet közzétett információk lekérdezése egy szereplő informatikai rendszeréből, vagy informatikai rendszerek közötti automatizált – ütemezett, vagy feltételek bekövetkeztétől függő, kötött, vagy dinamikusan változó tartalmú – adatcsere.

Az informatikai interoperabilitás alapja az informatikai rendszerek által kezelt adatok szándékolt jelentése, aminek megőrzése, átvitele a cél. Ez azonban a szemantikus technológiák, az információk (adatok) jelentésére vonatkozó meta-információk (meta-adatok) alacsonyabb elterjedtsége miatt napjainkban még nem könnyen adható meg, ismerhető meg[4]. Azonban a gyakorlatban, az együttműködés során az eltérő értelmezések jó része napvilágra kerül.

Az együttműködő, információt cserélő felek közötti információs heterogenitás, eltérések interoperabilitási problémákként merülnek, merülhetnek fel[5], amelyekre ***interoperabilitási megoldást*** kell találni. Az interoperabilitási problémák egyik lehetséges, napjainkban leggyakrabban alkalmazott megoldása a *szabványosítás*: a széles körben, vagy egy adott alkalmazási körben elfogadott szabványos megoldások alkalmazása. Ez kiküszöböli a különbözőségeket, minden fél a szabványos megoldást (pld. besorolási rend, kódrendszer, mértékegységek, stb.) alkalmazza. A megoldás feltétele a szabvány megléte, a teendő a szabvány alkalmazása a saját tevékenység során, a saját informatikai rendszerben.

A szabványosítás azonban nem minden esetben jelent megoldást, a heterogenitás nem mindig küszöbölhető ki, vagy nem célszerű kiküszöbölni. Ebben szerepet játszhat a szabványosítás,

---

[3] A gyakorlatban a fogadó félnél a kapott adat értelmezésével általában nem pontosan a küldött információ, a szándékolt jelentés áll elő, de erre nincs is szükség, mert elegendő az együttműködéshez elegendően pontos értelmezés, tartalom.

[4] Mindenkinek lehetnek személyes tapasztalatai egy adatbázisban, vagy formatizált üzenetben szereplő adatok értelmezési problémáiról (pld. a hőmérséklet Fahrenheit, vagy Celsius, a név tartalmazza-e valamennyi utónevet, stb.).

[5] Annak eldöntése, hogy ezek a különbözőségek, eltérések az együttműködést, és az ahhoz szükséges tartalmú és minőségű információcserét akadályozó, nehezítő jellegűek-e, az érintett felek joga, lehetősége.

illetve a szabvány szükséges módosításainak előzetes egyeztetés- és időigénye, illetve a szabvány, vagy annak változásai átvezetésének feladata a már meglévő informatikai rendszerekben. Az információs interoperabilitás esetében a szabványosítás sokkal könnyebben valósítható (és ahogy látható valósul is meg) a technikai és a szintaktikai szinten, mivel az alkalmazás szintjét ez – amennyiben korlátozásokkal nem jár – közvetlenül nem érinti.

Jóval nehezebb a szabványosítás, esetenként nem is kivitelezhető a szemantikai szinten. Ehhez ugyanis az szükséges, hogy az információcsere során alkalmazott fogalomrendszer minden szereplő számára egységesen elfogadható, alkalmazható legyen. Értelemszerűen a szabványosítás könnyebb tartós együttműködésben álló, azonos, vagy hasonló jellegű szereplők között, mint lazább együttműködésben lévő, eltérő szakterületekhez tartozó szereplők között. Az egyes szereplők fogalomrendszere ugyanis a szakterületük, feladataik igényeihez igazodó, amely általában szerves fejlődés eredményeként alakult ki, és megváltoztatása csak alapvető körülmények módosulása esetében és akkor is csak hosszabb idő alatt lehetséges.

Amennyiben a szabványosításra teljes körben nincs lehetőség, az interoperabilitás megvalósítására a közbenső átalakítások, *egyeztetett (adatszintű) közvetítő reprezentáció alkalmazása* ad lehetőséget. Ennek lényege, hogy minden együttműködő fél megtartja a saját (belső) fogalomrendszerét, adat-, esetleg üzenetformátumait, azonban ezeket információ küldése során átalakítja az egyeztetett közvetítő reprezentációra, illetve információ fogadása esetén az egyeztetett közvetítő reprezentációból átalakítja a saját belső formátumára. Ezzel az interoperabilitás – a tartalmi feltételek megléte esetén (pld. a továbbítandó információ valamilyen formában rendelkezésre áll a rendszerben) – az informatikai rendszerek módosítása nélkül is megvalósítható.

A KIBERBIZTONSÁGI INFORMÁCIÓCSERE INTEROPERABILITÁSÁNAKALAPJAI

Az interoperabilitási kérdések, problémák, követelmények, megoldások minden olyan területen vizsgálhatóak, ahol az együttműködő felek egymással információt cserélnek, nincs ez máshogy a kiberbiztonsági szervezetek közötti információcsere esetében sem. Alkalmazási területenként, szakterületenként, vagy információkörönként is eltérhet azonban az interoperabilitási kérdések szerepe, jelentősége, és eltérhetnek az interoperabilitási problémák, az elért interoperabilitási szintek következményei. A következőkben ezeket a kérdéseket elemezzük a kiberbiztonsági szervezetek közötti információcseréhez kapcsolódóan.

Az ***interoperabilitás szerepe, jelentősége a kiberbiztonsági szervezetek közötti információcserében*** ezen szervezetek rendeltetéséből, jellegéből vezethető le. A kiberbiztonsági eseménykezelő központok egy nézőpontból olyan tudás-intenzív szervezeteknek tekinthetőek, amelyek az ügyfélkörükbe tartozó szervezetek terheit csökkentik, az ügyfeleik által üzemeltetett informatikai rendszerek, hálózatok biztonsága megőrzésének eredményességét és hatékonyságát növelik.

Elvileg az egyes üzemeltető szervezetek informatikai és hálózatbiztonsági szerveinek önállóan is képesnek kell lenniük a biztonság fenntartására, a sérülékenységekre, és bekövetkezett incidensekre vonatkozó információk begyűjtésére, és ennek alapján a szükséges tevékenységek rendszabályok megvalósítására (akkor is, ha nincs őket támogató kormányzati, ágazati, vagy más kiberbiztonsági eseménykezelő központ), azonban ehhez jellemzően korlátozottabbak a kapacitásaik, illetve az információhoz jutási lehetőségeik.

A kiberbiztonsági eseménykezelő központok tevékenységüket – elsősorban a biztonsági események kezelése területén – eredményesen csak *egy eseménykezelő központ hálózat részeként,* a hálózat többi elemeivel szoros együttműködésben, egymás kölcsönös informálásával képesek végezni. Ennek hiányában csak a támogatott szervezeteikre vonatkozó eseményinformációkra támaszkodhatnának, azonban a globálisan összekapcsolt kibertérben a kiberbiztonsági fenyegetések számára a szervezeti határok nem léteznek, és a hálózati határok (még elkülönült hálózatok esetében) sem átjárhatatlanok.

A kiberbiztonsági eseménykezelő szervezetek szerepe azonban *nem elsősorban az egyszerű információ elosztás, továbbítás* (nem lehetnek kéretlen levélküldők). Ezzel kibővítik ugyan a támogatott szervezetek információs lehetőségeit, de nem vesznek le terheket a vállukról, sőt növelik azokat. Alapvető szerepük a beérkező – akár incidensekre, akár sérülékenységekre vonatkozó – információk szűrése, ellenőrzése, összevetése, szintetizálása, majd ezt követően az érintett támogatott szervezetek kiválasztása, és azok közvetlenül felhasználható, tevékenységet igénylő (az ENISA szóhasználatával 'actionable') információkkal történő ellátása.

Mindezen feladatok ellátásához a kiberbiztonsági eseménykezelő szervezeteknek széleskörű, megbízható, és egyértelműen értelmezhető információkra van szükségük. És bár új kiberbiztonsági információkat esetenként – például lefolytatott sérülékenység vizsgálatok, vagy tárgyi leletek vizsgálatának eredményeképpen – maguk is állíthatnak elő, tevékenységük alapját a szervezeten kívülről érkező információk, bejelentések, tájékoztatások, riasztások adják. Ebből következően az információk együttműködő partnereikkel, támogatott szervezeteikkel közös értelmezésen alapuló cseréjére vonatkozó képességeik, a velük fennálló információs interoperabilitásuk szerepe, jelentősége kiemelkedő.

Az ***információs interoperabilitás hiányának, alacsonyabb szintjének következményei*** számos formában megjelenhetnek, amelyeket az interoperabilitási követelmények meghatározása során, elsősorban az információkat fogadó fél szempontjából, figyelembe kell venni. Amennyiben egy adott információkörre vonatkozóan, vagy adott együttműködő partnerekkel egyáltalán nem biztosítható az interoperabilitás, az azt jelenti, hogy bár rendelkezésre állnak elvileg elérhető információk, azok nem férhetőek hozzá a fogadó számára, vagyis tevékenységét *kevesebb információ* birtokában képes végezni.

Az alacsonyabb szintű interoperabilitás, amikor az információ forrásától kapott, vagy az általa megosztott, hozzáférhetővé tett információt hordozó adatok formátuma eltér a fogadó fél által alkalmazott formátumtól (legyen ez elektronikus, vagy hagyományos), vagy amikor az információ értelmezése tér el a fogadó fél értelmezésétől, mindenképpen *többletmunkát* igényel: az eltérő formátumot át kell alakítani, az értelmezési különbségeket fel kell oldani.

Azon túl, hogy a többletmunka nem gazdaságos, okozhat *időbeniségi problémát* is. A beérkező információk lassabb feldolgozása egyes esetekben beleférhet a kiberbiztonsági szervezetek előírt minőségű eljárásrendjébe, azonban más esetekben – például súlyos minősítésű biztonsági események kezelése, vagy súlyos fenyegetésekről történő értesítések kiadása során – a tevékenység kicsúszhat az elvárt időkeretekből, amelynek következménye több károkozás is lehet.

Az interoperabilitás alacsonyabb szintje járhat olyan következménnyel, hogy az információk tartalma, teljessége, pontossága sérül. Ennek káros volta nem igényel különösebb indoklást, kiemelendő azonban a több szereplőn keresztül áramló információk minőségének folyamatos romlása, akár az egyes szereplők számára releváns érdemi információtartalom elvesztése is. Incidens bejelentések esetében ennek egy megoldási lehetősége lehet például a kiberbiztonsági szervezet által alkalmazott formátum mellett az eredeti bejelentés továbbítása is.

A KIBERBIZTONSÁGI INFORMÁCIÓCSERE INTEROPERABILITÁSÁNAK HELYZETE, JÖVŐJE

A kiberbiztonsági szervezetek között történő információcsere megvalósítási módjait folyamatos változások, új megoldások megjelenése és elterjedése jellemzik. Ez a folyamat még csak a fejlődési pálya kezdeti szakaszában van, amely a 'hagyományos' információcsere megoldásoktól a kiberbiztonsági szervezetek által alkalmazott informatikai rendszerek közötti automatizált információcseréig terjedhet. Természetesen ez utóbbira csak a biztonsági szempontok, a minősített információk kezelésére vonatkozó szabályok, a szervezeti információ-megosztási politikák keretei között, az adott szervezet mindenkori felügyelete alatt kerülhet majd sor.

A következőkben röviden összegezzük, elemezzük a kiberbiztonsági szervezetek közötti információcsere interoperabilitásának jelenlegi helyzetét, és tervezett, vagy várható jövőbeni irányait. A helyzet értékelése során csak röviden, szemléltetésképpen mutatjuk be a kapcsolódó interoperabilitási megoldásokat, mert ezek részletes vizsgálata egy későbbi kutatás tárgyát képezi. A helyzet, és a jövőbeni irányok vizsgálatát az információs interoperabilitás 'könnyebben megvalósítható' technikai és szintaktikai, illetve 'jelentősebb feladatot képező' szemantikai szintjére tagoljuk.

Előzetesen szükséges kiemelnünk azt a tényt, hogy az interoperabilitás, és annak bármely szintje kölcsönös – két, vagy több fél között fennálló (vagy hiányzó) – képesség, vagyis egy kiberbiztonsági szervezet interoperabilitásának helyzete csak a partnereivel fennálló információcsere kapcsolatok konkrét interoperabilitási viszonyainak együtteseként értékelhető. Egyes szervezetekkel magas szintű, másokkal közepes, vagy alacsony szintű lehet az interoperabilitás[6], amiből előállítható egy összegzett interoperabilitási értékelés is.

A kiberbiztonsági információcsere technikai és szintaktikai interoperabilitási kérdései az alkalmazott fizikai adatátviteli megoldásokhoz, valamint adatcsere formátumokhoz kapcsolódnak. A – változatlanul szerepet játszó – hagyományos információcsere megoldásokkal jelen publikációban nem foglalkozva a ***technikai interoperabilitás*** megítélésének alapja napjainkban az, hogy van-e adatátvitelt biztosító hálózati kapcsolat az információcserében érintett felek között, vagy csak adathordozók cseréjével oldható meg az információcsere. A hálózati kapcsolat ugyanis gyakorlatilag egyet jelent a szinte kizárólagos szerepet betöltő IP-alapú kapcsolattal, ami minden informatikai eszköz képességei között megtalálható. Így a technikai interoperabilitás általában minden partnerrel alapszinten biztosított.

A technikai interoperabilitás körébe tartozik megítélésünk szerint a *védett adatátvitel* képessége is, mivel a kiberbiztonsági információk (az ezeket hordozó adatok) nyilvánossága lehet korlátozott, illetve ezek az információk lehetnek minősítettek is. Ennek megfelelően két fél között, vagy felek egy együttműködő körén belül a technikai interoperabilitás helyzete lehet: nincs közvetlen adatátviteli lehetőség, nyílt adatátviteli lehetőség van, nyílt és védett adatátviteli lehetőség is van.[7]

Összességében megállapítható, hogy a kiberbiztonsági szervezetek közötti technikai interoperabilitás – a védett összeköttetés esetleges problémáitól eltekintve – napjainkban alapvetően adott, nem jelent problémát, és ilyen a jövőben sem várható. A technikai interoperabilitás kialakítása és fenntartása – nevének megfelelően – a kiberbiztonsági szakterülettől független, technikai kérdés.

A ***szintaktikai interoperabilitás*** megítélésének alapja a különböző adatformátumok fogadására, hasznosítására, illetve előállítására való képesség. Ezen belül jelentős csoportot képeznek – és várhatóan a jövőben sem tűnnek el – a *strukturálatlan (jellemzően szabad szöveges) adatok*, amelyek kezelése bonyolult szintaktikai feladatot nem igényel. Ezekhez kapcsolódóan interoperabilitási kérdésként egyrészt az alkalmazott karakterkészlet, másrészt az alkalmazott nyelv merül fel. Az eltérő karakterkészletek kezelése az alkalmazott alap- és alkalmazói szoftverek szolgáltatása kell legyen. A Unicode karakterkészlet elterjedésével ennek az interoperabilitási problémának a jelentősége folyamatosan csökken.

A nyelvi interoperabilitás megvalósítása napjainkban még alapvetően felhasználói, humán feladat, de a jövőben várhatóan megjelennek majd gépi fordítási megoldások. Megjegyzésre

[6] Az interoperabilitás szintjének meghatározására, értékelésére különböző interoperabilitási érettségi modellek, interoperabilitási skálák léteznek (lásd pld. [2])

[7] Ez a besorolás nem kiberbiztonsági szervezetek közötti információcserére specifikus.

érdemes, hogy a gépi fordítás az emberi "fordításhoz" hasonlóan lehetséges azonos nyelv, de eltérő szakmai, kiberbiztonsági terminológia – eltérő szaknyelvek (?) – esetében is.

A strukturálatlan adatok hasznosítása során a jövőben megjelenhet a természetes nyelvi feldolgozás eszköztára is, amely a szabad szövegből (például egy incidens bejelentésből), strukturált adatok együttese formájában képes kiemelni a kiberbiztonsági szervezet számára fontos információkat, sőt ezekre építve besorolásokat is készíthet, jelzéseket, riasztásokat is kiadhat.

A szintaktikai interoperabilitás szempontjából köztes csoportot képeznek a *félig strukturált adatok*, amelyek meghatározott struktúrába rendezett szabad, vagy bizonyos szabályoknak eleget tevő szöveges összetevőkből épülnek fel. Ilyen például szinte valamennyi sérülékenység leírás[8]. Nyilvánvalóan a szintaktikai interoperabilitás eltérő szintjét jelenti az, ha az adott kiberbiztonsági szervezet ezeket a leírásokat 'olvasni' és szövegként 'írni' tudja, vagy ha ezeket képes feldolgozni, strukturált (adatbázisba tárolásra alkalmas, vagy formatizált üzenet) formába alakítani, illetve strukturált formából a félig strukturált formátumot automatizáltan előállítani.

A szintaktikai interoperabilitás *strukturált adatok* esetében a formatizált üzenetekben, valamint az adatbázisokban tárolt információkhoz, illetve az ezeket kezelni képes szoftver megoldásokhoz kapcsolódik.[9] Az interoperabilitás fennállásáról akkor beszélhetünk, ha az adott szervezet megfelelő informatikai rendszere, alkalmazása képes:

- meghatározott formátumú üzeneteket fogadni, formai szempontból feldolgozni, a benne szereplő adatokat szükség esetén a szervezet által alkalmazott formára átalakítani, és ilyen üzeneteket a rendelkezésére álló adatok alapján előállítani;
- illetve kiberbiztonsági információkat együttműködő felek által hozzáférhetővé tett adatbázisból lekérdezni, a lekérdezett adatokat szükség esetén a szervezet által alkalmazott formára átalakítani, és kiberbiztonsági információkat meghatározott felépítésű, tartalmú adatbázisban mások számára hozzáférhetővé tenni.

A kiberbiztonsági információcsere szintaktikai kérdéseinek legnagyobb része a különböző egyeztetett, *szabványos üzenetformátumokhoz*[10] kapcsolódik. Az üzenetformátumok kezelésére vonatkozó képességek két szintre bonthatóak: a keretet képező általános adatcsere formátum, valamint az erre épülő kiberbiztonsági üzenetformátum kezelésének képessége. Az előbbi területén napjainkra egyeduralkodóvá vált az XML[11] formátum, amelynek kezelése a fizikai adatátvitel IP megoldásához hasonlóan az informatikai rendszerek, eszközök képességei között megtalálható, így ennek alkalmazása esetén interoperabilitási probléma jellemzően nem merül fel.

A kiberbiztonsági információcserében azonban léteznek jelentős üzenetszabványok, amelyek nem XML alapra, hanem például JavaScript-hez kapcsolódó JSON adatcsere formátumra[12] épülnek. Ebben az esetben természetesen biztosítani kell az ezen formátum kezeléséhez szükséges szoftver összetevőket is (ami ebben az esetben szintén általában infrastrukturális szinten rendelkezésre áll).

A speciális kiberbiztonsági üzenetformátumokhoz kapcsolódó szintaktikai interoperabilitási képesség, amennyiben az alapját képező általános adatcsere formátum kezelésének képessége

[8] Lásd például a MITRE cég, vagy a Kormányzati Eseménykezelő Központ által közreadott sérülékenység listákat.
[9] Sok esetben szintaktikai interoperabilitásról erre az értelmezésre leszűkítve beszélnek.
[10] Ezek az üzenetformátumok a kiberbiztonsági információcsere esetében szinte kizárólag karakteres típusúak.
[11] Az eXtensible Markup Language, Kiterjeszthető Jelölő Nyelv.
[12] JavaScript Object Notation (JSON), amelyre épül például a fenyegetések, leírására alkalmas nyelv (Structured Threat Information Expression, STIX).

meg van, viszonylag egyszerűnek nevezhető szoftver fejlesztési feladat. Az adott üzenetformátumhoz így kialakítható egy olyan interfész, amely az üzenetből további feldolgozásra, tárolásra, megjelenítésre alkalmas formában képes kiemelni a kiberbiztonsági információkat hordozó egyes adatelemeket, illetve a rendelkezésre álló adatokból képes összeállítani az üzenetformátum szabványnak megfelelő üzenetet.

A ***szemantikai interoperabilitás*** a kiberbiztonság területén is az interoperabilitás kialakításának és fenntartásának, a jelentésmegőrző információcsere biztosításának kulcskérdése. Az együttműködő feleket nem a kiberbiztonsági információk cseréje során alkalmazott fizikai, és adatformátumok érdeklik, érintik, hanem az ezek segítségével továbbított, ezek által hordozott információk. Szemantikai interoperabilitási feladat akkor jelentkezik, amikor az információt cserélő felek eltérő fogalomrendszereket használnak, eltérés van köztük az adatok értelmezésében, vagy a közös környezet ugyanazon dolgait különböző módon modellezik. Amennyiben ugyanis ezek megegyeznek, a technikai és szintaktikai megoldások könnyen megtalálhatók, az alkalmazói szintet érdemben nem is befolyásolják.

A szemantikai interoperabilitás megvalósításának kiinduló feltétele az egyes felek által használt fogalmak pontos definiálása, ami magában foglalja az érdeklődésre számot tartó dolgokra, a dolgokat leíró tulajdonságokra, valamint a dolgok között fennálló kapcsolatokra vonatkozó fogalmak definiálását. Együttműködés esetében meg kell állapodni az információcsere hátterében álló, egyeztetett, egyértelműen definiált fogalomrendszerben, ami kisebb, vagy nagyobb mértékben eltérhet az egyes felek saját fogalomrendszerétől. Ebben az esetben az érintett felek feladata a saját fogalomrendszerről a közvetítő (információcsere) fogalomrendszerre történő, illetve az ellenkező irányú átalakítás megvalósítása. A feladatot nehezíti, hogy egy szereplő több együttműködési kör része is lehet, így többféle átalakítást kell biztosítania.

Az együttműködő felek, vagy a felek és a közvetítő fogalomrendszer közötti *szemantikai eltérések típusai* között kiemelt szerepet játszhatnak a következők:

- terminológiai eltérések (azonos dolgok eltérő módon, különböző dolgok azonos módon történő megnevezése);
- alapfogalmak tartalmának eltérései (ugyanazon dolgokhoz pld. biztonsági eseményhez szűkebb, vagy tágabb tartalom rendelése);
- kategorizációs eltérések (dolgok kategóriákba sorolása eltérő részletességgel, vagy egymással nem teljes mértékben összehangolható módon);
- értékkészlet eltérések (dolgok ugyanazon tulajdonságának leírása eltérő módon);
- kapcsolatok eltérései (dolgok közötti kapcsolatok leírása eltérő módon, vagy eltérő részletezettséggel).

A szemantikai interoperabilitási problémák és megoldásaik a kiberbiztonságban az eseménykezelő szervezetek közötti szervezettebb együttműködés, információcsere kialakulásához kapcsolódóan már megjelentek. Elsőként, és azóta is elsősorban a kategorizációs, besorolási eltérések feloldását szolgáló *kötött értékkészletek, taxonómiák* kialakítása jelentette és jelenti a szemantikai interoperabilitás megvalósításának eszközét. A 2000-es évek elején már megjelentek javaslatok szabványos kiberbiztonsági információcsere formátumokra, azonban ahogy azt egy 2006-os ENISA tanulmány is megfogalmazta, a legnagyobb információ megosztási problémát a felek által alkalmazott eltérő taxonómiák, osztályozási rendszerek képezték. [3, 28. o.] Azóta különböző célú taxonómiák, kötött értékkészlet listák sora jelent meg, amelyek közül egyesek szélesebb, mások szűkebb körben kerülnek alkalmazásra.

A jövőben is várhatóan több kiberbiztonsági besorolási rend marad alkalmazásban, így a feladat ezek lehetséges mértékű összehangolása, illetve a jelentésmegőrző átalakítás biztosítása köztük. Az 'egyszerű' taxonómiák mellett várhatóan megjelennek, és előtérbe kerülnek a fogalomrendszerek formalizált leírását biztosító ontológiák, valamint az ezekre épülő szemantikus szolgáltatások, funkciók (pld. automatikus átalakítás fogalomrendszerek között).

KIBERBIZTONSÁGI ESEMÉNYEKHEZ KAPCSOLÓDÓ INTEROPERABILITÁSI KÖVETELMÉNYEK, PROBLÉMÁK

Mint azt egy előző publikációban már tárgyaltuk, a kiberbiztonsági szervezetek információkat tárolnak, kezelnek, és használnak fel a felügyeletük alá tartozó, általuk támogatott szervezetek kiberbiztonsági eseményeiről. Ezen információk egy részét különböző együttműködő partnereknek is továbbítják jelentési/tájékoztatási kötelezettség, figyelmeztetés, további teendők végrehajtása céljából, illetve ilyen információkat fogadnak együttműködő partnerektől hasonló okokból.

A kiberbiztonsági szervezetek eredményes és hatékony működésének alapvető feltétele, ***általános interoperabilitási követelménye***, hogy az együttműködő partnereknek képesek legyenek kiberbiztonsági eseményekre vonatkozó információkat megküldeni az előírt/egyeztetett formában és tartalommal, illetve a partnerektől képesek legyenek ilyen információkat fogadni, megfelelő módon értelmezni, és feldolgozni, hasznosítani. Mindez kiterjedt együttműködési kapcsolatokkal rendelkező szervezet számára – eltérő adatcsere formátumok esetében – több önálló interoperabilitási követelményt jelent.

A kiberbiztonsági eseményekhez kapcsolódó ***információk az interoperabilitási eltérések szempontjából*** három csoportba oszthatóak. Az első azon információk csoportja, amelyeknek az együttműködő felek által használt *tartalma és formátuma érdemben nem tér el*.[13] A korábbi publikációban bemutatott információk közül ilyenek a következők:

- bejelentő neve, elérhetőségei, képviselt szervezete;
- észlelés, bekövetkezés, befejeződés (stb.) időpontja, helyreállítás várható időtartama;
- hálózati azonosítók (IP címek, nevek);
- hatások mennyiségi jellemzői, a kár becsült összege.

A második csoportot azon szakterület, kiberbiztonság specifikus információk alkotják, amelyek *tartalma, értelmezése azonos, de formája eltér*. Ide a kiberbiztonsági események információi közül a földrajzi helyek, valamint az operációs rendszer platform, és alkalmazott javítócsomagok azonosítása tartoznak.

Végül a harmadik csoportba azon információkat sorolhatjuk, amelyek esetében az együttműködő felek között *szemantikai, értelmezési eltérések* állnak fent. Ezek elsősorban: az esemény osztályozása; az esemény által érintett összetevő típusa; az érintett összetevő rendeltetése; és az esemény hatásának mértéke (a szolgáltatásokra, illetve a kezelt információkra).

A következőkben sorra vesszük a harmadik csoportba tartozó ***információk interoperabilitási problémáit***. Ezek között kiemelt szerepet *a kiberbiztonsági esemény osztályozása* játszik. A kiberbiztonsági szervezetek ezen információ alapján döntenek arról, hogy az adott esemény milyen prioritással tart (egyáltalán tart-e) számot érdeklődésükre; kiknek kell információkat továbbítaniuk az eseményről; és ezt is felhasználva készítenek helyzetértékelő statisztikákat. Mivel napjainkban egységesen elfogadott osztályozási rendszer (taxonómia) nem létezik, alapvető interoperabilitás feladat a különböző rendszerek közötti jelentésmegőrző átalakítás biztosítása.

A kiberbiztonsági esemény által érintett ('áldozat', 'sérült') informatikai rendszer *összetevő típusa* szintén fontos szerepet játszik a kiberbiztonsági tevékenységben. A szervezetek ez alapján kereshetnek sérülékenységeket az esemény következményeinek elhárítása során; ez alapján; figyelmeztethetik a felügyeletük alá tartozó, támogatott szervezeteket a fennálló fenyegetésre;

[13] Ebben az értelmezésben nem tekintjük érdemi eltérésnek pld. a szöveges adatok karakterkészletében, mennyiségi adatok mértékegységében, vagy a dátum- és időadatok formátumában fennálló különbözőségeket, amelyekre a tartalomtól független átalakítási eljárások állnak rendelkezésre.

és értesíthetik az érintett gyártót; illetve ez az információ is fontos csoportosító tényező a kiberbiztonsági helyzetértékelő statisztikák elkészítése során. Mivel napjainkban még nincs széles körben elterjedt besorolási rendszer, sőt gyakran ez az információ kötetlen szöveges formájú, fontos interoperabilitási feladat annak átalakítása egy kötött értékkészletű saját besorolási rendszerre.

Az érintett *összetevő rendeltetés szerinti besorolása* (pld. kiszolgáló eszköz, munkaállomás, hálózati kapcsoló eszköz, vagy ennél részletesebb besorolás) az esemény értékelése, súlyossága, az események közötti prioritások meghatározásának egyik fontos kiinduló alapja. Ez az információ elsősorban a kiberbiztonsági eseménykezelő központ, és az eseményt elszenvedett, ügyfélkörébe tartozó szervezet között áramlik, azonban továbbításra kerülhet jelentések, tájékoztatások részeként is. A rendeltetés szerinti besorolásra sincs széles körben alkalmazott osztályozási rendszer, a különböző rendszerek közötti átalakítás mellett itt is felmerül a kötetlen szöveges formáról történő átalakítás feladata.

Végül *a kiberbiztonsági esemény hatásainak besorolása* – amennyiben nem más, mérhető jellemzők alapján kerül meghatározásra – szintén jelentős információ a különböző szintű kiberbiztonsági szervezetek számára feladataik prioritásának meghatározásához. A gyakorlatban 3-5 szintű skálák kerülnek alkalmazásra, amelyek között biztosítani kell a lehető legjobban jelentésmegőrző átalakítást, illetve speciális interoperabilitási feladatként merülhet fel a hatás súlyosságának besorolásából, az eredetileg alkalmazott besorolási feltételek esetén (visszakövetkeztetés alapján) egyes mennyiségi jellemzők, vagy azok értéktartományai meghatározására.

SÉRÜLÉKENYSÉGEKHEZ KAPCSOLÓDÓ INTEROPERABILITÁSI KÖVETELMÉNYEK, PROBLÉMÁK

A kiberbiztonsági szervezetek által kezelt információk között jelentős szerepet töltenek be a sérülékenységekre vonatkozóak is. A kiberbiztonságot megsértő események a legtöbb esetben az érintett informatikai rendszer összetevőiben megtalálható sérülékenységeket kihasználva következnek be. Emiatt a sérülékenységekre vonatkozó információk kezelése minden kiberbiztonsági szervezet alapvető feladata. A kapcsolódó információk általában az érintett rendszer összetevők gyártóitól, bejelentésekből, illetve más kiberbiztonsági szervezettől érkeznek, de keletkezhetnek az adott szervezetnél is.

A kiberbiztonsági szervezetek eredményes és hatékony működésének – az előző pontban foglaltak mellett – alapvető feltétele, ***általános interoperabilitási követelménye*** az is, hogy képesek legyenek együttműködő felek által küldött, vagy hozzáférhetővé tett sérülékenység információkat fogadni, átvenni, megfelelő módon értelmezni, és hasznosítani, illetve együttműködő partnereknek, támogatott szervezeteknek egyeztetett formában átadni, mivel a sérülékenységekre, illetve az elhárításukra vonatkozó információk nélkül nem lehet hatékony eseménykezelést megvalósítani.

A sérülékenységekhez kapcsolódó ***információk az interoperabilitási eltérések szempontjából*** szintén az előző pontban már meghatározott három csoportba oszthatóak. Azon információk közé, amelyeknek az együttműködő felek által használt *tartalma és formátuma érdemben nem tér el*, a következők tartoznak: sérülékenység azonosítók; az érintett összetevő megnevezése; valamint verziószáma, módosítása, kiadása. Sérülékenységekhez kapcsolódó *azonos tartalmú, de eltérő formátumú információnak* minősíthető az érintett összetevő gyártójának megnevezése.

A témánk szempontjából legfontosabb, *szemantikai, értelmezési eltérésekkel bíró információk* csoportja a következőket foglalja magában: a sérülékenység típusa, az érintett összetevő típusa; a sérülékenység potenciális következményeinek minősítése; illetve a sérülékenység súlyossága. Ezek közül több is megegyezik az eseményekre vonatkozó információkkal, hiszen az eseménykezelés és a sérülékenység nyilvántartás egymással szoros együttműködésben vannak.

A ***szemantikus interoperabilitási problémákat hordozó információk*** közül a *sérülékenységek osztályozása* rendszerező szerepet játszik a sérülékenységek nyilvántartásában, a különböző forrásokból származó sérülékenység információk összevetésében, sérülékenységek azonosságának, viszonyának feltárásában. Bár ezen a területen a Gyengeségek Felsorolása (CWE) lista alkalmazása széleskörű, de mellette léteznek más – az összetevők teljes körére, vagy csak egyes csoportjaira (pld. JAVA kódolási sérülékenységekre) kiterjedő – osztályozások, besorolások is.

Az *érintett összetevő típusa* kiemelt szerepet játszik a sérülékenység kezelésben. Ez segít a más forrásokból kiszűrni az adott kiberbiztonsági szervezet számára jelentőséggel bíró sérülékenységeket. Ez utóbbiak közé csak azok tartoznak, amelyek által érintett összetevők léteznek az eseménykezelő szervezet által támogatott szervezetek informatikai rendszereiben. A hatékony működés érdekében az összetevő típusának a sérülékenység nyilvántartásban szereplővel interoperábilis módon kell szerepelnie az informatikai erőforrások nyilvántartásában is.

A *sérülékenység következményeinek minősítése* a minden kiberbiztonsági szervezet által elvégzendő kockázatelemzés kiinduló adata. Ennek meghatározása az érintett szervezet feladata, ehhez azonban felhasználhatja a más szervezetek által megadott besorolásokat. Ehhez megfelelően értelmezni kell tudni az eltérő skálán meghatározott hatásszinteket, és átalakítani a saját skálára.

Végül *a sérülékenység súlyosságának besorolására* szintén nincs egységesen elfogadott skála és besorolási rendszer. A kapcsolódó interoperabilitási feladatok hasonlóak, mint amit a sérülékenység hatásának minősítésénél, illetve a kiberbiztonsági események hatásainak besorolásának bemutattunk.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Összegzésképpen megállapíthatjuk, hogy a kiberbiztonsági szervezetek közötti interoperabilitási problémák alapját az együttműködő felek közötti eltérések képezik, amelyek megnehezítik, vagy lehetetlenné teszik a jelentésmegőrző információcserét. Az információcserét befolyásoló, akadályozó eltérések megjelenhetnek a fizikai kapcsolatok technikai szintjén, az adatformátumok szintaktikai szintjén, valamint az adatok által hordozott jelentés szemantikai szintjén. Az interoperabilitási problémák egyik lehetséges, napjainkban leggyakrabban alkalmazott megoldása a szabványosítás, ami azonban nem minden esetben jelent megoldást, a heterogenitás nem mindig küszöbölhető ki, vagy nem célszerű kiküszöbölni.

A kiberbiztonsági eseménykezelő központok nézőpontjából az interoperábilis információcsere alapvető jelentőségű, tevékenységüket – elsősorban a biztonsági események kezelése területén – eredményesen csak egy eseménykezelő központ hálózat részeként, a hálózat többi elemeivel szoros együttműködésben, egymás kölcsönös informálásával képesek végezni. Az interoperabilitás hiánya azt jelenti, hogy az érintett szervezet tevékenységét csak kevesebb információ birtokában tudja végezni, vagy az átvett információk feldolgozása többletmunkát igényel, és több időt vesz igénybe.

Az interoperabilitási problémák a technikai és szintaktikai szinteken alapvetően megoldottak, vagy megoldhatóak, ezzel szemben a szemantikai szinten jelentős megoldatlan problémák állnak fent. A kiberbiztonsági szakterületen különböző célú taxonómiák, kötött értékkészlet listák sora jelent meg, amelyek közül egyesek szélesebb, mások szűkebb körben kerülnek alkalmazásra. A jövőben is várhatóan több kiberbiztonsági besorolási rend marad alkalmazásban, így a feladat ezek lehetséges mértékű összehangolása, illetve a jelentésmegőrző átalakítás biztosítása köztük.

FELHASZNÁLT IRODALOM

[1] MUNK S.: *Katonai informatikai rendszerek interoperabilitásának aktuális hadtudományi kérdései. MTA doktori értekezés.* – Magyar Tudományos Akadémia, 2007

[2] SARANTIS, D.-CHARALABIDIS, Y.-PSARRASM, J. Towards Standardising Interoperability Levels for Information Systems of Public Administrations. – In. Charalabidis, Y.-Panetto, H.-Loukis, E.-Mertins, K. (szerk): *eJETA Special Issue on "Interoperability for Enterprises and Administrations Worldwide"*, Athens, 2008

[3] *CERT cooperation and its further facilitation by relevant stakeholders.* – European Union Agency for Network and Information Security, 2006.