HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 1. szám 145–160.
DOI: 10.32567/hm.2021.1.9

Kralovánszky Kristóf[1]

A kibertér fejlődése (második rész) – Kiberműveletek és kritikus infrastruktúrák egyes kapcsolatai

The Evolution of Cyberspace, Part II Certain Connections between Cyber Operations and Critical Infrastructures

Az állami akaratérvényesítés eszközei között egyre hangsúlyosabb szerepet kapnak a kiberműveletek. Alkalmazásuk sokkal komolyabb körültekintést igényel, mint a hagyományos tartományokban végzett műveletek, mivel a megtámadott infrastruktúra nem kellően felmért interdependenciái hatalmas járulékos károkat okozhatnak a támadónak is. Jelen tanulmány ennek bizonyos kockázatait és összefüggéseit vizsgálja.

Kulcsszavak: **komplex küszöbérték, kiberműveletek, állami akaratérvényesítés, kritikus infrastruktúrák**

Cyber operations are becoming robust tools in a nation state's policy. The applications thereof require far more caution than the tools used in conventional domains. Inaccurately evaluated interdependencies of attacked infrastructures can cause substantial collateral damages to the attacker. This paper investigates certain aspects and connections of such interdependencies.

Keywords: **complex threshold, cyber operations, state policy tool, critical infrastructure**

[1] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Elektronikai Hadviselés Tanszék, egyetemi tanársegéd, e-mail: kralovanszky.kristof@uni-nke.hu, ORCID: https://orcid.org/0000-0002-5560-3525

1. Bevezetés

Jelen publikáció *A kibertér fejlődése* című tanulmány második része, így bizonyos fogalmi meghatározások magyarázatától eltekint, és az első részben használtakat kezeli irányadónak. A kibertér fogalmát azonban ismét definiálja, a következők szerint: elsődlegesen az ember által mesterségesen létrehozott, dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot.[2] A tanulmány célja, hogy a kiberműveletek egyes hadászati szintű kérdéseit és hadtudományi aspektusait előtérbe helyezve vizsgálja azok kapcsolatait, megtörtént kibertéri műveletek elemzésével és a különböző ágazati eredmények szintézisével.

2. A kritikus infrastruktúra fogalma[3]

A kritikus infrastruktúrák tartalmi meghatározása viszonylag kiforrott, függetlenül attól, hogy megfogalmazásában eltérések lehetnek. Több tudományos mű foglalkozik átfogóan a fogalmi definiálással,[4] amelyek jellemzően megfeleltethetők a 2012. évi CLXVI. törvényben foglalt meghatározásnak: kritikus infrastruktúra „[…] a meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna".[5]

A jogalkotó azonban külön szabályozza, hogy mely ágazatokat tekint kritikusnak és így a törvény hatálya alá tartozónak. Ebben a minősítésben azonban már jelentős eltérések vannak országok között.[6] Bizonyos (al)ágazatok,[7] mint például a villamosenergia-szolgáltatás (a hozzá kapcsolódó teherelosztással és elosztóhálózattal), illetve

[2] Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus Kiadó, 2018. A meghatározás Haig Zsolttól származik, csupán az elején az „elsődlegesen" szóval került kiegészítésre.

[3] Hatályos honi jogi szabályozás szerint (2012. évi CLXVI. törvény) a kritikus infrastruktúrák hivatalos megnevezése létfontosságú rendszerelem, amely nemzetközileg elfogadott elnevezés szerint: kritikus infrastruktúra. Jelen publikáció a két kifejezést egymás szinonimáiként használja.

[4] Kovács László: Kritikus információs infrastruktúrák Magyarországon. *Hadmérnök,* 1. (2007), Robothadviselés konferencia különszám. 1–20.; Haig Zsolt – Kovács László: *Kritikus infrastruktúrák és kritikus információs infrastruktúrái.* Budapest, Nemzeti Közszolgálati Egyetem, 2012.; Haig Zsolt – Hajnal Béla – Kovács László – Muha Lajos – Sik Zoltán Nándor: *A kritikus információs infrastrukturák meghatározásának módszertana.* ENO Avisory Kft., 2009.

[5] 2012. évi CLXVI. törvény 1. § f) bekezdés.

[6] Haig et alii (2009) i. m.

[7] Magyarországon az alágazati besorolást egy 2020. évi Kormány rendelet bővítette, és ezzel bevezette az „Alapvető szolgáltatások jegyzékét", amely jelenleg a 65/2013 Korm. rendelet (a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról) 3. számú melléklete.

a közcélú távközlési/adatátviteli hálózatok szinte minden fejlett országban a kritikus infrastruktúrák közé soroltak.[8]

Vannak ugyanakkor olyan országok, ahol például az ipari létesítmények, illetve a vegyipari létesítmények törvényi tekintetben nem tartoznak a kritikus infrastruktúrák közé.[9] Ezzel pedig megjelenik egy másik lehetséges csoportosítás: (1) törvény szerinti kritikus infrastruktúrák és (2) a valóban kritikus infrastruktúrák. Ideális esetben a két halmaz teljes mértékben fedné egymást, ám a gyakorlat ettől jelentősen eltérhet. Jogi besorolás alapján ugyanis a mérlegelésre kerülő feltételrendszer (általánosítva) az alábbi:

- országok saját meghatározása alapján,
- horizontális (ágazati) besorolás szerint,
- vertikális (hatás) besorolás szerint.

Ahogy az európai szabályozás is helyesen felismerte, illetve ahogy a honi szabályozásban is megjelenik, létezik az „európai létfontosságú rendszerelem" fogalma,[10] amelynek ilyenné történő kijelölését vagy az állam önmaga vagy egy másik Európai Gazdasági Térség (EGT) állam kezdeményezheti. Ezzel az európai jogalkotó elismeri, hogy egy kritikus infrastruktúrának lehetnek olyan súlyos hatásai, melyek nem csupán az üzemeltető államot érintik, hanem egy (vagy több) szomszédos államot is – tehát a kezelendő kockázatok az államok határainál nem állnak meg. Ki kell emelni ugyanakkor, hogy nem csupán környezeti hatásokról van szó, hanem ellátási, vagy társadalmi hatások is felmerülhetnek – tehát más megfogalmazásban megjelenik egy sajátos (nem technológiai) interdependencia mint besorolási feltétel. Ez, vagyis az egymástól függés, azonban rendkívül mély és szerteágazó – sokszor jóval nagyobb mértékű, mint a jogalkotó által meghatározott keretek. Bizonyos ágazatok kizárásával ugyanis a jogalkotó nem ismeri el, hogy abban az adott ágazatban lehet egy infrastruktúra kritikus.

Ezért lenne fontos egy más megközelítésből tekinteni a besorolási feltételekre és vizsgálni az alábbi főbb gyakorlati szempontokat, amely alapján egy adott infrastruktúra:

- Jelentősen átlép-e egy bizonyos küszöbértéket?[11]
- Átlép-e egy mátrixként kezelhető komplex küszöbérték rendszert?

[8] Ágazatként vagy alágazatként. Általában – de nem szükségszerűen – kritikus infrastruktúra ágazat jellemzően a vízügy (inkább az ivóvíz szegmensben), az élelmiszeripar, az egészségügy, a pénzügy és a szállítás.

[9] Magyarországon például az „ipari veszélyes anyagok előállítása, tárolása és feldolgozása" alágazatot (a nagyobb vegyipari gyártók döntő többsége idetartozik), illetve a gyógyszergyártás alágazatot a közigazgatási bürok- ráciacsökkentésről szóló 2015. évi CLXXXVI. törvény kivette a kritikus infrastruktúra alágazatok közül.

[10] 2012. évi CLXVI. törvény 3. §.

[11] A küszöbértékek meghatározása többek között ágazattól is függő, rendkívül összetett feladat, ezért meghatározása nem tárgya jelen tanulmánynak, ugyanakkor több hazai kutatás is részletesen foglalkozott a küszöbérték fogalmával és tágabb értelemben a kritikus infrastruktúrák meghatározásának módszertanával. Haig et alii (2009) i. m. Küszöbértéken – jelen írás – a létesítmény (infrastruktúra) valamely működési (vagy ahhoz kapcsolódó) paraméterét, míg küszöbérték rendszeren e paraméterek adott együttesét érti.

3. Komplex küszöbértékrendszer

A küszöbértékek elvileg már ágazatonként megállapíthatók, és szövetségi rendszer szintjén is kezelhetők, vagyis létrehozható lenne egy egységes európai normarendszer. Ehhez azonban egy olyan értékelési mátrix elkészítése szükséges, amely jelenleg nem áll még rendelkezésre.[12]

Le kell küzdeni továbbá az államok és adott esetben gazdasági szereplők[13] ellenérdekeltségét, hiszen a kritikus infrastruktúrává minősítés az adott gazdasági társaságra jelentős többletköltségeket ró, illetve az államnak is rendelkeznie kell azzal a szakértői gárdával és erőforrással, ami a megfelelő szakmai szintű ellenőrzéshez szükséges. Másik oldalról viszont mindkét félnek plusz garanciákat teremt, hiszen egy esetleges baleset (vagy szabotázs), vagy üzemi kiesésből származó elsődleges, másodlagos és harmadlagos károktól való mentesülés a védelmi bekerülési költségeket akár jelentősen (nagyságrendileg többszörösen) is meghaladó megtakarításokhoz vezethet.

A veszélyeztetettségek szintje – ágazattól függően – dinamikusan változó lehet. Különösen igaz ez a vegyiparra, ahol egy új receptúra vagy egy technológiai frissítés bizonyos összetevők vagy paraméterek olyan változását eredményezheti, amelytől jelentősen megnövekedhet egy adott küszöbérték meghaladása, vagy egy új, addig nem kezelt küszöbérték szerinti kockázat kezelése válhat szükségessé.[14]

Feltétel ezért, hogy az az értékelési keretrendszer, amelynek alapján a besorolás történik, kellően rugalmas tudjon lenni a változó technológiákkal szemben, és ne dogmatizálódott szabályok alapján kezelje a felmerülő kérdéseket. Ezzel párhuzamosan elengedhetetlen, hogy a hatósági oldalon is ugyanúgy és ugyanakkor álljon rendelkezésre mindaz a szaktudás és információ, ami alapján az értékelés elvégezhető.

Általában tehát nem fogadható el kielégítőnek a szolgáltató önbevallása – feltétlenül fontos a hatósági oldalról a bevallás realitásának ellenőrzése, amelyhez szintén jelentős szaktudásra van szükség. Fontos ugyanakkor az is, hogy az „ellenérdekeltség"[15] fennmaradjon az ellenőrző és az ellenőrzött között, hiszen ha az ellenőrzött egy ugyanazon állami szervezet által működtetett kritikus infrastruktúra, mint az ellenőrző másik állami intézménye, akkor könnyen előfordulhat, hogy maga az ellenőrzés jóval megengedőbb, mint egy ugyanolyan tevékenységet végző gazdasági szereplő

[12] Jelen publikáció kereteit többszörösen meghaladná egy ilyen új értékelési mátrix leírása, ezért ezzel itt érdemben foglalkozni nem lehetséges.

[13] A gazdasági szereplők ebben az esetben inkább multinacionális vagy globális vállalatok, igen jelentős politikai érdekérvényesítő képességgel.

[14] Ilyen lehet például egy hőmérséklet-kritikus technológia, ahol a folyamat csak meghatározott magas hőmérsékleten stabil. Egy esetleges áramszünet esetén (az abból következő hőmérséklet-csökkenés miatt) az előbbi folyamat pedig instabillá válik, és adott esetben kinetikus robbanást eredményezhet. Megoldásként tehát olyan szünetmentes áramellátásra van szükség, amely kontrollált keretek és stabil körülmények között csökkenti le a technológiai hőmérsékletet olyan szintre, amely azt követően már villamos energia nélkül is fenntarthatóan stabil.

[15] Az ellenérdekeltség semmiképpen sem negatívként értelmezendő, hanem legyenek garanciák arra, hogy a mindkét oldali állami tulajdonlás ténye az ellenőrzést megőrizze a segítő/támogató objektivitás szintjén. Ehhez viszont elengedhetetlen egy olyan transzparens keretrendszer létrehozása, amely szigorúan szakmai konszenzuson alapul, és amelynek kialakításában külső, független – célszerűen elismert külföldi is – szakértők vesznek részt. Adott szakmán belül pedig meg kell teremteni az auditok megismerhetőségét oly módon, hogy az adatok biztonsága ne kerüljön veszélybe, és nemzetbiztonsági érdekek ne sérüljenek. A fő cél ugyanis a biztonságos üzemeltetés gyakorlati megteremtése, és nem a csupán statisztikai megfelelőségre való törekvés.

esetén. Itt juthatnak kulcsszerephez a nemzetközi (szabványos) tanúsítási rendszerek és az akkreditált ellenőrző szervezetek.

Ha elfogadjuk a szolgáltatói oldalon az interdependencia jelentőségét, akkor felismerhetjük, hogy a nemzeti hatóságok között[16] (illetve főként országok hatóságai között nemzetközi viszonylatban) ugyanennyire fontos az információk megosztása – nem csupán a gyorsriasztási rendszerekben, hanem az ellenőrzési eljárásokban és a technológiai változások megfelelő követésében. Az ágazatok egy része ugyanis hasonló vagy közel megegyező technológiát és gépeket használ egy földrajzi régióban,[17] amelyből fakadóan a vizsgálati eljárások és a felmerülő kockázatok is hasonlóak lesznek. Ugyanígy nagyfokú egyezés lesz tapasztalható az interdependenciák logikájában is, ám annak konkrét szereplői már nyilvánvalóan az adott ország nemzetgazdasága szerint különbözni fognak.

Jelentős szimmetria figyelhető tehát meg mind a gazdasági szereplők, mind a hatóságok oldalán az elvárások mértéke és azok teljesítése vonatkozásában, amiből következik az is, hogy nem lehet sem tudásban, sem tapasztalatban szakadék a két fél között. Ellenkező esetben ugyanis az előbbiekben említett dinamikus környezet működési egyensúlya fog sérülni – vagy teljesen – felborulni, ami jelentős többletkockázatként jelentkezik.

4. Műveletek a kibertérben

A kritikus infrastruktúrák zökkenőmentes működése – beleértve ebbe az interdependenciáik folyamatos és stabil üzemét is – létfeltétele egy ország stabilitásának (nemzetbiztonsági tekintetben is). Önmagában tehát a létfontosságú rendszerelemek egy részének (tartozzanak ugyanazon vagy eltérő ágazatba) hetekig tartó vagy azt meghaladó működési zavarai szinte garantált instabilitást fognak eredményezni, úgy gazdasági, mint belpolitikai vonatkozásaiban. Főként ez az oka annak, hogy a kritikus infrastruktúrák célponti értéke – egy támadó szemszögéből – rendkívül magas.[18] Következésképp a károkozási célú kiberműveletek elsődleges célpontjai jellemzően a kritikus infrastruktúrák.

Kritikus infrastruktúrákkal szembeni támadások különböző végrehajtási módozatokban tudnak megtörténni, amelyek közös célja, hogy az adott infrastruktúra működését megzavarják vagy korlátozzák – ideiglenesen vagy véglegesen. Kézenfekvő módszer lehet tehát:

- a fizikai károkozás, amely valamilyen kinetikus (be)hatás segítségével jöhet létre;[19]

[16] Országon belül.

[17] Például a villamosenergia-ellátás SCADA (Supervisory Control and Data Acquisition – felügyeleti irányító és adatgyűjtő) rendszereinek érzékelői és szoftverei. Az egyező (konkrét) rendszerek a részes országok nemzetbiztonsági érdekei miatt minősített adatok.

[18] Haig (2018) i. m.

[19] Hubbard, Ben – Palko Karasz – Stanley Reed: Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran. *The New York Times,* 2019. szeptember 14.

- az adott infrastruktúrán belüli – egymással interdependenciában lévő – alrendszerek közötti kommunikáció manipulálása vagy blokkolása;[20]
- egy vagy több alrendszerben történő belső, fizikai károkozás.[21]

Mindhárom módozat kivitelezhető kiberműveletek segítségével,[22] amelyeknek az elkövető számára nagyon komoly előnyei vannak: távolról végrehajtható ezért nincs szükség hozzá helyszíni erőre, így olcsóbb, kockázatmentesebb és elkövetőre nehezebben bizonyítható.[23] E bizonyíthatóság nehézsége teszi még vonzóbbá a kiberműveleteket az elkövető számára.

Egymással szemben álló érdek érvényesítése vagy (relatív) erőfölény megszerzése szinte folyamatos célja a különböző államoknak, ám legalább ennyire fontos, hogy a meglévő együttműködések mellett ezek végrehajthatók legyenek, vagyis egymással szemben ne járjanak politikai arcvesztéssel. Ennek egyik legfőbb oka, hogy az egymás közötti főbb gazdasági érdekek, amelyek értelem szerint politikai eredővel rendelkeznek, prioritással bírnak – ezek azonban csak nagy vonalakban jelölik ki az érdekszférák határvonalait. A „finomabb" körülhatárolások eszközei tudnak lenni azok az egyéb – szintén politikai eredővel rendelkező – műveletek, amelyek a kibertérben végrehajthatók, és a szereplők számára is világosak, ugyanakkor nem igényelnek nyílt konfliktust.

Hatékonyságában és alacsony bekerülési költségében ilyen eszközök a történelemben eddig nem álltak rendelkezésre, ezért szokásjogon alapuló elfogadott használati mérték is nehezen határozható meg. Más megfogalmazásban: rendkívül széles az a szürke zóna, amelyben a kiberműveletek sikerrel alkalmazhatók. Itt tehát szintén értelmezhetővé válik a küszöbérték fogalma, amely már a szürke zóna felső (határ) értékét jelenti, definitív kimondása viszont szinte minden esetben politikai kérdés. Nem meghatározható az az időben független, abszolút érték (határvonal), ahol egy kiberművelettel megtámadott országnál már nyílt támadásként értelmeznek egy eseménysort. Ebben a vonatkozásában a küszöbérték tehát ugyanúgy viselkedik, mint a kritikus infrastruktúrák meghatározásánál: vagy egy komplex feltételrendszernek kell megfelelnie a támadásnak, vagy egy ingerértéket kell nagyon jelentősen túllépnie.

A politikai döntéseknek van ugyanakkor egy másik jellemzőjük is: a külső és belső környezettől való jelentős függésük és azok alapján történő dinamikus módosulásaik – akár napon belül is. Elenyészően kevés az a helyzet, amiről időtől függetlenül, abszolút módon meghatározhatóan kimondható, hogy mindig túl fogja lépni a politikai küszöbértéket.

Annak deklarálása tehát, hogy egy ország kijelentse önmagáról, hogy kibertámadás érte, gyakorlatilag minden esetben politikai döntés – hiszen ezzel annak kijelentése is

[20] Norsk Hydro Unit Begins Operating at 50% of Capacity After Cyber Attack. *Insurance Journal,* 2019. március 21.
[21] Daniel Terdiman: Stuxnet delivered to Iranian nuclear plant on thumb drive. *Cnet,* 2012. április 12.
[22] A kinetikus károkozás kivételével (amennyiben a Stuxnet támadást nem kívülről irányítottként, hanem belül telepítettként tekintjük) a jelölt hivatkozások mind sikeres kibertámadások voltak. A kívülről vezérelt, nem célirányos, hanem kárérték-maximalizálásra törekvő támadásra eddig csak sikertelen kísérlet volt. (Pierluigi Paganini: Triton Malware Hits Critical Infrastructure in Saudi Arabia. *Infosec,* 2017. december 18.) A támadásokkal egy korábbi publikációban a szerző részletesen foglalkozott. Kralovánszky Kristóf: A villamosenergia-rendszer kiber- és nemzetbiztonsági kockázatai (1. rész). *Nemzetbiztonsági Szemle,* 7. (2019), 3. 18.
[23] Az elkövetés bizonyítását és az elkövető (igazolt) azonosítását nevezzük attribúciónak (angol szaknyelven: attribution), amely rendkívül összetett és nehéz folyamat lehet.

megtörténne, hogy az adott ország nem volt képes önmagát a kibertérben megvédeni. Így lehetséges az is, hogy ugyanazon művelet egyszer küszöbérték alattinak, máskor nyílt támadásnak minősül.

Kiberműveletek során – amennyiben állami megrendelésre vagy állam által kerül végrehajtásra – állami akaratérvényesítésről beszélhetünk, amelynek számos végrehajtó szerve lehet. Egy adott ország állami szervezetei közül többen is alkalmasak lehetnek ezek kivitelezésére: lehet akár rendvédelmi, honvédelmi vagy állambiztonsági (nemzetbiztonsági) szereplő (illetve ezek valamilyen kombinációja). Fedett műveletek esetében pedig az előző három csoport valamely tagjából önmaga szakosodott szolgálata és/vagy vele kapcsolatban álló egyéb gazdasági vagy civil szereplő (csoport). Egyáltalán nem szükségszerű tehát, hogy egy kiberműveletet egy adott ország fegyveres ereje hajtson végre, vagy abban egyáltalán részt vegyen.

5. Az állam kiberképességeinek jelentősége

Egy állam minden esetben igyekszik a saját akaratát érvényesíteni és a saját céljait megvalósítani – de teszi ezt egy dinamikusan változó nemzetközi környezetben, amelyben az erőviszonyok is folyamatos változásban vannak. Ebből eredően minden pillanatban törekedni fog arra, hogy az adott helyzetben legjobb pozíciót érje el, és sok esetben más államok szuverenitásának részleges megsértését is meg fogja engedni magának, hiszen a szuverenitás nem abszolút fogalom, és értelmezése ugyanúgy a politikai környezet változásait követi.[24]

Ahogy a konvencionális hadviselésben is, az államok többségének a szuverenitása korlátozott, illetve behatárolt, és e szuverenitásukat az érdekszférájukba tartozó nagyhatalom (jellemzően ENSZ Biztonsági Tanács valamely állandó tagállama) viszonyrendszerében képesek csak gyakorolni. A nagyhatalmak erőterét pedig akár jelentősen is kiterjesztheti egy vele nyílt vagy korlátozott szövetségi rendszerben működő másik állam.[25] A kibertérben ez egyszerűsödhet, hiszen létrejöhetnek olyan alkalmi szövetségek (akár hosszabb időtartamra is), amelyek eltérnek a hagyományos kapcsolatrendszer szereplőitől, de a kibertér szürkezónájának köszönhetően titokban tarthatók, vagy nehezen bizonyíthatók.[26]

Más megközelítésből, egy állam – a lehetőségeihez mérten – igyekszik magának maximális mozgásteret[27] létrehozni, és azt folyamatosan és dinamikusan kitölteni, nyílt vagy fedett módon.

[24] Varga Gergely: A szuverenitás különböző megközelítései és jelentéstartalma. *Nemzet és biztonság,* (2015), 1. 30–38.

[25] Államok önrendelkezési joga – egy bizonyos kockázati szint felett nem értelmezhető, mert automatikusan sérteni fogja egy másik állam szuverenitását, de politikai okok miatt időlegesen (és sokszor színleg) csökken a jelentősége.
A háttérben, a fentiekkel párhuzamosan pedig jelentősen nő az állampolgárok kitettsége a kritikus infrastruktúráknak – a meghatározó államokban is.

[26] Gary Corn: Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace. In *Complex Battlespaces.* Oxford University Press, 2019.

[27] Az esetek döntő többségében nem földrajzi értelemben.

Ezt a törekvést az állam mint akaratának érvényesítését végzi, ugyanakkor nem önállóan katonai kérdésként tekinti, hanem komplex feladatként, de amelyben a fegyveres ereje valamilyen formában általában részt vállal. Ugyanígy igaz az is, hogy az adott állam nem csupán egy fronton vívja e küzdelmét, hanem él a rendelkezésére álló valamennyi lehetőségével. Racionális esetben igyekszik ugyanígy tenni a vele szomszédos állam is, tehát minden állam törekszik arra, hogy az őt potenciálisan támadó államok elkövetési eszközeivel szemben védekezni tudjon.[28]

Miért fontosak a kiberképességek egy országnak? Ha az állam oldaláról keressük a választ, akkor két fő irányban indulhatunk:

- nagyon sok másik ország is rendelkezik valamilyen szintű kiberképességgel, így amennyiben egy adott államnál ez hiányzik, úgy sérülékenyebb és kitettebb lesz ilyen támadásoknak;
- az állami akaratérvényesítés legolcsóbb változata az okozható kár (elrettentési képesség) arányában.

Tovább vizsgálva a támadó által elérendő célt, és összehasonlítva az azonos politikai eredménnyel kecsegtető, de más tartományt alkalmazó megoldásokkal, kézenfekvő lehet a kibertér – mint hadviselési tartomány – használata. A harc sikeres megvívásának azonban alapfeltétele a fegyelmezettség és a nagyon tiszta alá-fölé rendeltségi rendszer, amely rendvédelmi vagy fegyveres erő bevonásával tud igazán megvalósulni. Többek között ezért is fontos, hogy a hadsereg a kiberműveletek[29] szerves része legyen és maradjon. Ne feledkezzünk meg arról, hogy jellemzően nem egy hadsereg fog önmagában (és önmagáért) harcot vívni a vele szemben álló féllel, hanem azt az állam akaratának érvényesítése céljából – vagy eszközeként – fogja tenni.

6. A kibertér – mint tartomány – műveleti sajátosságai

A kibertér egyik legfőbb összehasonlítási alapja más hadviselési tartományokkal a kinetikus eszközökkel történő rombolás képessége. Egy szerencsére meghiúsult példa jól mutatja, hogy a kibertéren keresztül megvalósuló kinetikus pusztító erő igen jelentős lehet. 2017-ben a szaúd-arábiai Petro Rabigh kőolajfinomítót [30] azzal a céllal támadták a kibertérből, hogy az üzemben robbanást érjenek el, ezzel megsemmisítve a gyár minél nagyobb részét, és másodlagosan jelentős termelési kiesést okozzanak.[31]

A cél elérhető lett volna rakétákkal okozott fizikai pusztítással is – amennyiben feltétel a távolról történő végrehajtás – de ez azonnal és egyértelműen azonosította volna a támadót is. Ilyen rakétát pedig szinte csak állam képes indítani,[32] így annak szaúdi légtérbe való behatolása már önmagában is háborús okot eredményezett volna.

[28] Vagy legalább megkísérelje a védekezést.
[29] Támadó vagy védekező egyaránt.
[30] The Highly Dangerous 'Triton' Hackers Have Probed the US Grid. *Wired,* Elérés 2019. június 14.
[31] Kralovánszky (2019) i. m. 18.
[32] Feltételezve egy legalább 500 km-es hatótávolságot és az indítást sikeresként értelmezve, vagyis az ahhoz szükséges minden infrastruktúra (indítóállvány, hajtóanyaggal való feltöltés stb.) működőképességét is.

Ugyanez a teljes megsemmisítés drónokra erősített robbanószerkezetekkel lényegesen nehezebben érhető el,[33] de hasonlóra is történt már kísérlet 2019-ben, szintén Szaúd-Arábiában.[34] Humán erőforrás – helyszínen történő fegyveres erő (akár konspiráltan is) – használatával pedig pont a távoli végrehajtás lehetősége vész el.

A pusztítás új elvi lehetőségei némileg hasonlatosak az 1940-es évek második felében megjelent atomfegyverek által nyújtottakhoz, azzal, hogy az új fegyverrel – addig megszokott kijuttatási módszerekhez képest – dimenziókkal nagyobb megsemmisítő erő vált elérhetővé.[35] Valami hasonló történik a kibertérben is, azzal, hogy a nem nukleáris eszköztárral megegyező[36] vagy azt akár jelentősen meghaladó kinetikus pusztítás és/vagy fenyegetettség valósítható meg egy másik országgal szemben.

A nukleáris és a kiberképességekkel való rendelkezés sokban ugyanazt a célt szolgálják; első és legfontosabb az elrettentés, illetve ennek magasabb harmonikusa, a kölcsönös elrettentés. A fő elrettentő erő pedig abban van, hogy (1) nehéz tudni, mikor és hol fog támadni az elkövető, (2) mekkora pusztítást lesz képes okozni. Sem nukleáris, sem kiberfegyver esetén nem szükségesek a támadás helyszínén a támadó ország katonái, mert a támadás akár több ezer kilométerről elindítható, végrehajtható és befejezhető.

Mind kiber-, mind nukleáris fegyver alkalmazásánál az alábbi fő részek mérlegelése elengedhetetlen a csapásmérés tervezésében és kivitelezésében:

- elérni kívánt hatás;
- egyéb másodlagos, többedleges hatások;
- fegyver kiválasztása;
- célbajuttatás módja.

A csak nukleáris világban a helyzet egyszerűbb volt: a politikai döntéshozóknak nem nagyon kellett foglalkozni az alkalmazott eszköz technológiai részével, hiszen bombáról vagy robbanófejről volt szó, amely egy viszonylag jól becsülhető környezetben kinetikus pusztítást volt képes végezni. Az egyéb hatásokkal (radiológiai, biológiai stb.) kevéssé foglalkoztak.[37]

Ma a helyzet a kibertérben ennél jóval bonyolultabb: a politikai döntéshozóknak érteniük kellene a különböző technológiák támadásával elérhető (okozható) károk nagyságát és mértékét, különös hangsúllyal a kiiktatni kívánt technológiák interdependenciáinak részleges vagy teljes kiesése esetén létrejövő kumulációs hatást. Mint mindent, nyilván ezt a kérdést is le lehet nyelvtanilag egyszerűsíteni – tartalmilag azonban már jóval kevésbé: ma sokkal hangsúlyosabban (szerteágazóbban) jelenik meg a másodlagos hatás kérdése, mint a nukleáris kor hajnalán.

[33] A szállítható viszonylag kevés robbanóanyag és a pontos célterületre (3-5 méteres pontossággal egy komplex ipari létesítmény belsejében) juttathatóság korlátozottsága miatt.

[34] UN Cannot Confirm Iran behind Saudi Oil Attacks. *BBC News,* 2019. december 11.

[35] Vonatkoztassunk el rövid időre a radioaktivitás által okozott hatásoktól, és csak a rombolási képességet vizsgáljuk.

[36] A világban fellelhető nukleáris eszközök összesített csapásmérő képességét (vagyis a Föld többszörös elpusztításának képességét) ne vizsgáljuk.

[37] Ha mélyebben foglalkoztak volna ezen aspektusokkal is, akkor a nukleáris fegyverek fejlesztése vélhetően másként alakul, de ez a gondolat hamar ahhoz a kérdéshez vezet, hogy összességében megnyerhető-e egy nukleáris háború? E kérdés megválaszolásával pedig jelen írás nem kíván foglalkozni.

Két fontos kiegészítést is kell tenni a nukleáris és a kiberműveletek összehasonlításában. Az egyik, hogy nukleáris eszközök – különösen urbanizált területeken történő – alkalmazása rendkívül komoly, százezres vagy milliós nagyságrendű emberélet kioltásával és egy jelentős földrajzi terület használhatatlanná válásával járhat.

Az ötvenes évek elején ugyanakkor nem volt a társadalom ilyen magas szinten kitett a kritikus infrastruktúráknak. Ma is vannak (Magyarországon is) olyan létfontosságú rendszerelemek, amelyekben egy bekövetkező kinetikus robbanás – megfelelően sajátos időjárási körülmények esetén – tízezres nagyságrendben okozná emberek halálát néhány napon belül. Ezzel párhuzamosan, mivel Magyarországon csak egy van belőle, és Európában sincs csak néhány másik, a gazdaság ellátás nélkül maradása is hatalmas károkat okozna.[38]

Az egyre növekvő interdependenciák miatt ugyanakkor egy csapás stratégiai minősége nem a támadás elsődleges méretében, hanem az okozott kár nagyságában lesz mérhető (akár egyetlen, jól kiválasztott célpont támadásával).[39] Más megközelítésben, egy rosszul felmért (másodlagos hatásokkal nem megfelelően számoló) taktikai méretű kibertámadás könnyen stratégiai szintűvé (eredményűvé) válhat.

A kiberképességek és -módszerek nagyfokú titkolásának a legfőbb oka pedig, hogy a kibercsapásmérés egyik legfontosabb értéke (és elrettentő ereje), hogy nem ismert, mi az a sérülékenység, amelyet a támadó ki fog használni.[40] Sokszor nem ismert továbbá az a dominóhatás sem, amelyet a támadás okozni fog, vagyis a támadó rendelkezhet olyan további információval, amelynek segítségével tud olyan másodlagos hatásról, amelyről a megtámadott nem tud – így nem is számít annak hatásaira.[41]

7. A kibertér mint megoldási tartomány

A nukleáris eszközök és az azokkal történő összehasonlítás a kibertér súlyára kíván rámutatni, vagyis a károkozási képesség lehetőségeire. Egy másik példán keresztül a konvencionális hadviselés kiberműveletekkel való kiválthatóságát vizsgáljuk meg.

A koreai háború során, 1953-ban, amikor a béketárgyalások már javában zajlottak, az Egyesült Államok továbbra is hatékony és erős csapásokkal kívánta folytatni műveleteit. Ennek keretében az alapvető elképzelés az északi élelmiszer-termelési képesség jelentős csökkentése és ezzel az élelmezésben történő súlyos zavarok okozása

[38] E tanulmány nem kíván tippet adni senkinek, így szándékosan nem nevez meg konkrét helyszínt és ágazatot. A szerző a saját munkái során több ilyen infrastruktúrát ismert meg gyakorlati oldalról is.

[39] A 2019 szeptemberében a szaúdi olajfinomítók elleni, drónokkal elkövetett támadás elérhető lett volna megfelelően végrehajtott kibertámadással is, bár a drónos támadás elkövetőinek sem anyagi, sem technikai, sem információs erőforrásaik nem lettek volna elégségesek hozzá. Vannak ugyanakkor olyan szervezetek, amelyek már rendelkeznek ilyen lehetőségekkel. Charlie Osborne: Hackers use Triton malware to shut down plant, industrial systems. *ZDNet.com,* 2017. december 15.; Nicole Periroth – Clifford Krauss: A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try. *The New York Times,* 2018.

[40] Nyilvánvaló, hogy sérülékenységekkel szemben lehet védekezni, ám a sérülékenység fokának csökkentése egyenes arányban áll a védekezésre fordított költségek nagyságával és a védekezéshez igénybe vett szakemberek tudásának és tapasztalatának kiterjedtségével.

[41] Például egy vízerőmű valamely túlhevülést felügyelő rendszerének kiiktatásával (annak az üzemeltető számára nem ismert infokommunikációs sérülékenységét kihasználva), utána a felügyelet nélkül maradt és túlterhelődött rendszer robbanásával, majd ezt követően az erőmű gát részének mechanikai sérülésével.

volt, amely az akkori tervezők véleménye szerint jogilag is elfogadható katonai cél lett volna – különösen azért, mert az északi területeken megtermelt 283 000 tonnát meghaladó rizs nagyobb része az északi katonák élelmezésére fordítódott.[42]

Az Egyesült Államok két opciót mérlegelt: (1) a megtermelt rizskészletek pusztítása a raktárak bombázásával; (2) a rizstermelés lehetőségeinek korlátozása. Mindkét koncepció elfogadható volt a stratégiai tervezők részére és a második megoldás részletes kivitelezésére az északi öntözőrendszer gátjainak felrobbantása látszott célszerű választásnak. Mai kifejezéssel ezt a stratégiai célt interdependenciáinak támadásaként írnánk le – amely természetéből fakadóan másodlagos hatásként[43] eléri a kívánt eredményt.

A katonai parancsnokok ugyan elvetették a gátak lerombolásának komplex tervét, de három gát felrobbantására mégis parancsot kapott az Egyesült Államok légiereje.[44]

A 2017-es Petro Rabigh finomító elleni kibertámadással párhuzamba állítva a támadó céljai sokban megegyeztek: kritikus infrastruktúrát támadni és annak rombolásával az adott infrastruktúra által kiszolgált gazdasági szereplőket korlátozni, illetve a támadott ország működésében jelentős fennakadást okozni. Nyilvánvaló különbség van a két művelet dinamikájában, hiszen a hagyományos bombázás végrehajtása a parancs kiadásától számítva 4–36 órán belül végrehajtható volt, és nem igényelt többéves előkészítést. Ugyanígy egyértelmű különbség van a két támadás költségében is, hiszen a repülőgépekkel és bombákkal végrehajtott támadás lényegesen magasabb költséggel jár.[45] Az óriási különbség azonban az, hogy kibertérben végrehajtott támadáshoz elsődlegesen infokommunikációs eszközökre van csak szükség,[46] amelyek nem számítanak katonai szakanyagnak, illetve a végrehajtói állomány komoly programozói és egyéb informatikai tudással rendelkező személyei esetében sem feltétel, hogy fegyveres testület hivatásos állományú tagjai legyenek.

8. Kibertámadás előjelzése

Konvencionális tartományokban végrehajtott katonai műveletek esetében az előjelzési képesség jelentősen eltér a kibertér műveleteinek ugyanilyen lehetőségeitől. Egy stratégiai[47] nukleáris csapás valamennyire előjelezhető volt a triád mindhárom aspektusában:

- földi indításnál: megfigyelt helyszínről történő indítás, röppályaelemzés;

[42] Robert Futrell: *The United States Air Force in Korea, 1950-1953*. 2. kiadás. Washington, D. C., Office of Air Force History, 1983.

[43] Az elsődleges hatás a gátak fizikai pusztítása lett volna, de mivel annak eredménye az öntözés ellehetetlenülése, így a rizstermesztés is komoly akadályokba ütközött volna.

[44] A ledobott több tonnányi robbanóanyag a háromból csak két gátat tudott felrobbantani, és azokat is csak indirekt módon, mert a gátak órákkal a légi csapásokat követően a robbanások okozta szerkezeti gyengülés következtében omlottak le.

[45] A költségek elemzése természetesen ennél jóval összetettebb, hiszen nagyon komoly szakállomány szükséges a háttérben mindkét típusú támadás kivitelezéséhez.

[46] Természetesen a támadást előkészítő hírszerzési adatok nem mellőzhetők, ahogy a végrehajtás kivitelezési módjához és időzítéséhez is jellemzően titkosszolgálati forrásokból származó információk szükségesek.

[47] Hangsúlyozottan stratégiai és nem taktikai csapásról van szó, amely nem 1-2 rakéta indítását jelenti. Földi indításnál nem tekintendő e kategóriába tartozónak például a vonatról vagy az önjáró állványról való indítást.

- tengeri indításnál: a helyszín nehezebben volt készenléti állapotában figyelhető, de az indításra használt eszközök közelítő helyszínei nagyságrendileg ismertek voltak;
- légi indításnál a légi jármű követhető volt, és ismerhető volt a típusa, így a feladata is.

A példákat követve, hagyományos bombázás esetében például a légijárművek radarral követhetők – feltételezve, hogy a támadó a megtámadott légvédelmi képességeit nem semmisítette meg.

Kiberhadviselés esetében az előjelzésnek két fő módozata lehet. Az első a hírszerzés,[48] mivel stratégiai szintű kibercsapásméréshez rendkívül komoly előkészületek szükségesek, amelyek részleteit nagyon nehéz titokban tartani – így egy jól működő (különösen szövetségi rendszerben üzemelő) hírszerzési rendszer bizonyos részeit fel fogja fedni. Ez különösen igaz akkor, ha az adott támadó fegyveres erején kívül az adott ország más kormányzati szerveit is (részlegesen) be kell vonni. Más a helyzet, ha a stratégiai szintű kiberműveletet egy stratégiai szintű össztartományi (szárazföldi, légi, kiber- [adott esetben tengeri] tartományokkal is kiegészítve) komplex műveletként hajtják végre.

A második előjelzési mód a saját infokommunikációs rendszerek megfigyelése és elemzése.[49] Egy nem fertőzött, normál működésű hálózatban a felhasználói szokások alapján viszonylag jól feltérképezhető az átlagos működés, amely jellemző arra az adott hálózatra. Az ettől való eltérések vizsgálatával (bármilyen irányban) általában megállapítható, hogy az kockázatot/fenyegetettséget jelent-e, vagy normál használatból eredő, indokolt eltérés.[50] Ez az elemzés értelmezhető egy pár tucat eszközből álló hálózaton ugyanúgy, mint egy több tízezer hálózati végponttal rendelkező nagyvállalati hálózaton vagy komplex kormányzati infokommunikációs rendszeren.[51] Az ilyen folyamatos elemzés rendkívül jó kiindulási alapot biztosíthat, ám egyáltalán nem biztos, hogy választ ad a támadást elkövetni szándékozó személyére. Indirekt módon szolgálhat ugyanakkor információval, mert az elkövetési módok vagy az azokhoz alkalmazott kártevők lehetnek jellemzőek egy-egy elkövetői csoportra.[52]

Ennek a megfigyelő-elemző munkának egyik alapfeltétele a lehető legnagyobb elemzési tartomány rendelkezésre állása, vagyis a hálózati forgalom offline (nem

[48] A hírszerzés mint előjelzési mód minden tartományra igaz. Megvalósulási formája tartományonként és haderőnemenként jelentősen eltér, de közös alapokon nyugszik. Jellemzően minden támadásnak vagy oka, vagy célja van. Ha oka van, akkor valamilyen előzménye is van, amely elvileg megismerhető. Egy komplex nemzetközi politikai/katonai környezetben ezek az okok roppant szerteágazók lehetnek, és egyáltalán nem biztos, hogy észszerű időn vagy racionális kereteken belül megismerhetők. Amikor az okokhoz elhatározás és tevőleges szándék kapcsolódik, akkor lesz belőlük fenyegetettség, amelyek bekövetkezésének egyik előjelzési módja a hírszerzés: a fenti fenyegetettségeket, okokat, célokat és azok hátterét fogja felderíteni, elemezni és értékelni.

[49] Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018. Az így elemzett adatok felhasználásával történik a korai előrejelzés, angol elnevezéssel: Early Warning System (EWS).

[50] Malik Shahzad Kaleem Awan – Pete Burnap – Omer Rana: Identifying Cyber Risk Hotspots: A Framework for Measuring Temporal Variance in Computer Network Risk. *Computers & Security,* 57. (2016), 31–46.

[51] Természetesen jelentős eltérések lesznek az alkalmazott elemző rendszerben, azok kapacitásában és elemzési komplexitásában.

[52] Itt kapcsolódik a tanulmány első részében részletezett bizonyíthatóság és az állami szereplők. (Kralovánszky Kristóf: A kibertér fejlődése. *Hadmérnök,* 14. (2019), 4. 197–212.)

valós idejű) elemezhetősége, amelyhez a hálózat méretének növekedésével rendkívül komoly méretű tárkapacitásra és feldolgozási sebességre van szükség.

Hasonló elemzésnek kell(ene) történnie[53] egy bekövetkezett támadást követően is, amikor az elkövető személyének a megállapítására van szükség.[54] Az óriási különbség az, hogy egy támadást követően sokkal jobban ismerhető, hogy mit kellett volna keresni, míg egy támadás előtt ez az információ a legritkább esetben áll csak rendelkezésre.[55]

9. Összegzés, következtetések

A kibertérben a klasszikus értelemben vett támadás és az azzal szembeni elsődleges védekezés szereplői ma már általában ugyanabból a körből kerülnek ki, mint a hagyományos hadviselés esetében, ahol a légitámadásra jellemzően a katonai légvédelem válaszolt, vagy ahol a tüzérségi tüzet a szemben álló oldal tüzérsége – esetleg valamely más katonai csapásmérő egysége hajtotta végre. Ennek elsődleges oka, hogy az állami akarat- és érdekérvényesítés ezköztárának továbbra is egyik fontos része a hadviselés (vagy az azzal történő elrettentés), amelyben tartományként a kibertér szerepe és hangsúlya folyamatosan növekszik.

Kibertámadások és az azokra adott válaszok esetében a támadó és védekező erők gyökeresen eltérőek lehetnek, különösen akkor, ha az adott válasz nem az elektromágneses spektrumban történik, hanem kinetikus eszközökkel valósul meg.

Visszatekintve az elmúlt 20 évre, a kiberműveletek[56] egy alapvetően egzotikus minőségből (mint izgalmas, de nem meghatározó lehetőség) fejlődtek a modern hadviselés meghatározó és megkerülhetetlen részévé, amelyek hadászati, hadműveleti és harcászati szinteken egyaránt számításba veendők, és támadásként történő bekövetkezésüket (támadás lehetséges elszenvedését) szinte minden más hadviselési módozatot megelőzően mérlegelni kell, illetve az arra történő felkészülést körültekintően és széles körű, szakértő szakmai alapokon el kell végezni, úgy nagyvállalati, mint nemzeti szinten – vagyis polgári és katonai tekintetben egyaránt.

Kiberműveletek alkalmazása a támadói oldalon egyre komolyabb felelősség főként azért, mert nehéz előre tudni, hogy egy támadásra hol és milyen formában fog érkezni a válasz – hiszen a válaszban egy sérülékenységet fognak viszont támadni, amely sérülékenységről egyáltalán nem biztos, hogy az eredeti agresszor tud. A támadó számára pedig azért is hatalmas a kockázat, mert a számára ismeretlen interdependenciákon keresztül olyan, nem szándékos károkozást is elérhet, amely az eredeti csapásmérési

[53] Az angol szakirodalom ezt a folyamatot hívja IT forensics-nek, vagyis digitális nyomkeresésnek.

[54] Simson Garfinkel: Digital Forensics Research: The next 10 years. *Digital Investigation,* 7. (2010), 64–73.

[55] Az előbbiek inkább a technikai felderítési csoportba tartoztak, ám ugyanennyire fontos a kiberteret érintő kereskedelmi típusú hírszerzés egyik klasszikus példája a „Threat Intelligence", amelyet a vezető kiberbiztonsági cégek szolgáltatásként értékesítenek. (Aviram Zrahia: Threat Intelligence Sharing between Cybersecurity Vendors: Network, Dyadic, and Agent Views. *Journal of Cybersecurity,* 4. (2018), 1.; Jori Pascal Kalkman – Lotte Wieskamp: Cyber Intelligence Networks: A Typology. *The International Journal of Intelligence, Security, and Public Affairs,* 21. (2019), 1. 4–24.) Ennek egyik alapja ugyanúgy technikai hírszerzés, a fent leírt módon, csak a saját eszközeik és szoftvereik által védett hálózatokból beérkező anonimizált információkból.

[56] Hangsúlyosan különbséget téve a tisztán elektronikai hadviselés és a kiberműveletek között.

szándékhoz képest jelentős eszkalációt eredményezhet – és amely a kibertéren messze túlmutathat.

A kibertér műveleteinek jelentős felértékelődése gyökeres paradigmaváltást jelent, amelynek alapjai az információs társadalom rohamos térnyerésében keresendők, és a mögötte lévő exponenciális technológiai fejlődésnek az eredményei. Korunk világpolitikájának meghatározó részei és egyensúlyi tényezői lettek az államok kiberképességei és az azokkal történő részleges akaratérvényesítés. Nem opció egy fejlett országnak vagy fejlett országok stratégiai szövetsége tagállamának,[57] hogy a kiberteret és az abban végzett műveleteket ne sorolja legalább azonos szintre a többi hadműveleti tartomány képességi elvárásával. Meg kell teremtenie, üzemeltetnie kell, és folyamatosan naprakészen rendelkezésre állón kell tartania továbbá mindazt a saját tudást és technológiát, amely segítségével a kibertérben a felkészültsége nagyságrendileg egyezni tud a vele – mint állammal – közel azonos méretű és/vagy geopolitikai státuszú más államok hasonló képességével. Ugyanakkor meg kell védenie saját szuverenitását a kibertérben, megőrizve ezzel az állam ilyen értelmű stabilitását. A kritikus infrastruktúrák kibervédelmén keresztül pedig a gazdasági szolgáltatások és a lakosság alapvető ellátásához szükséges erőforrások is biztonságban megőrizhetők.

Felhasznált irodalom

Awan, Malik Shahzad Kaleem – Pete Burnap – Omer Rana: Identifying Cyber Risk Hotspots: A Framework for Measuring Temporal Variance in Computer Network Risk. *Computers & Security,* 57. (2016), 31–46. Online: https://doi.org/10.1016/j.cose.2015.11.003.

Corn, Gary: Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace. In *Complex Battlespaces.* Oxford University Press, 2019. Online: https://doi.org/10.1093/oso/9780190915360.003.0012

Futrell, Robert: *The United States Air Force in Korea, 1950-1953*. 2. kiadás. Washington, D. C., Office of Air Force History, 1983. Online: https://media.defense.gov/2010/Dec/02/2001329903/-1/-1/0/AFD-101202-022.pdf

Garfinkel, Simson: Digital Forensics Research: The next 10 years. *Digital Investigation,* 7. (2010), 64–73. Online: https://doi.org/10.1016/j.diin.2010.05.009

Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus Kiadó, 2018.

Haig Zsolt – Hajnal Béla – Kovács László – Muha Lajos – Sik Zoltán Nándor: *A kritikus információs infrastrukturák meghatározásának módszertana.* ENO Avisory Kft., 2009. Online: https://nki.gov.hu/wp-content/uploads/2009/10/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf

Haig Zsolt – Kovács László: *Kritikus infrastruktúrák és kritikus információs infrastruktúrái.* Budapest, Nemzeti Közszolgálati Egyetem, 2012.

[57] Természetesen a szövetségi rendszernek önmagának is rendelkeznie kell koordinált kiberképességekkel, amely azonban a tagállamok hasonló képességén nyugszik.

Hubbard, Ben – Palko Karasz – Stanley Reed: Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran. *The New York Times,* 2019. szeptember 14. Online: www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html

Paganini, Pierluigi: Triton Malware Hits Critical Infrastructure in Saudi Arabia. *Infosec,* 2017. december 18. Online: https://resources.infosecinstitute.com/triton-malware-hits-critical-infrastructure-saudi-arabia/#gref

Kalkman, Jori Pascal – Lotte Wieskamp: Cyber Intelligence Networks: A Typology. *The International Journal of Intelligence, Security, and Public Affairs,* 21. (2019), 1. 4–24. Online: https://doi.org/10.1080/23800992.2019.1598092.

Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018.

Kovács László: Kritikus információs infrastruktúrák Magyarországon. *Hadmérnök,* 1. (2007), Robothadviselés konferencia különszám. 1–20.

Kralovánszky Kristóf: A kibertér fejlődése. *Hadmérnök,* 14. (2019), 4. 197–212. Online: https://doi.org/10.32567/hm.2019.4.13.

Kralovánszky Kristóf: A villamosenergia-rendszer kiber- és nemzetbiztonsági kockázatai (1. rész). *Nemzetbiztonsági Szemle,* 7. (2019), 3. 40–57. Online: https://doi.org/10.32561/nsz.2019.3.4

Osborne, Charlie: Hackers use Triton malware to shut down plant, industrial systems. *ZDNet.com,* 2017. december 15. Online: www.zdnet.com/article/hackers-use-triton-malware-to-shut-down-plant-industrial-systems/

Periroth, Nicole – Clifford Krauss: A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try. *The New York Times,* 2018. Online: www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

Norsk Hydro Unit Begins Operating at 50% of Capacity After Cyber Attack. *Insurance Journal,* 2019. március 21. Online: www.insurancejournal.com/news/international/2019/03/21/521324.htm

Terdiman, Daniel: Stuxnet delivered to Iranian nuclear plant on thumb drive. *Cnet,* 2012. április 12. Online: www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/

The Highly Dangerous 'Triton' Hackers Have Probed the US Grid. *Wired,* Elérés 2019. június 14. Online: www.wired.com/story/triton-hackers-scan-us-power-grid/

UN Cannot Confirm Iran behind Saudi Oil Attacks. *BBC News,* 2019. december 11. Online: www.bbc.com/news/world-middle-east-50742224

Varga Gergely: A szuverenitás különböző megközelítései és jelentéstartalma. *Nemzet és biztonság,* (2015), 1. 30–38.

Zrahia, Aviram: Threat Intelligence Sharing between Cybersecurity Vendors: Network, Dyadic, and Agent Views. *Journal of Cybersecurity,* 4. (2018), 1. Online: https://doi.org/10.1093/cybsec/tyy008