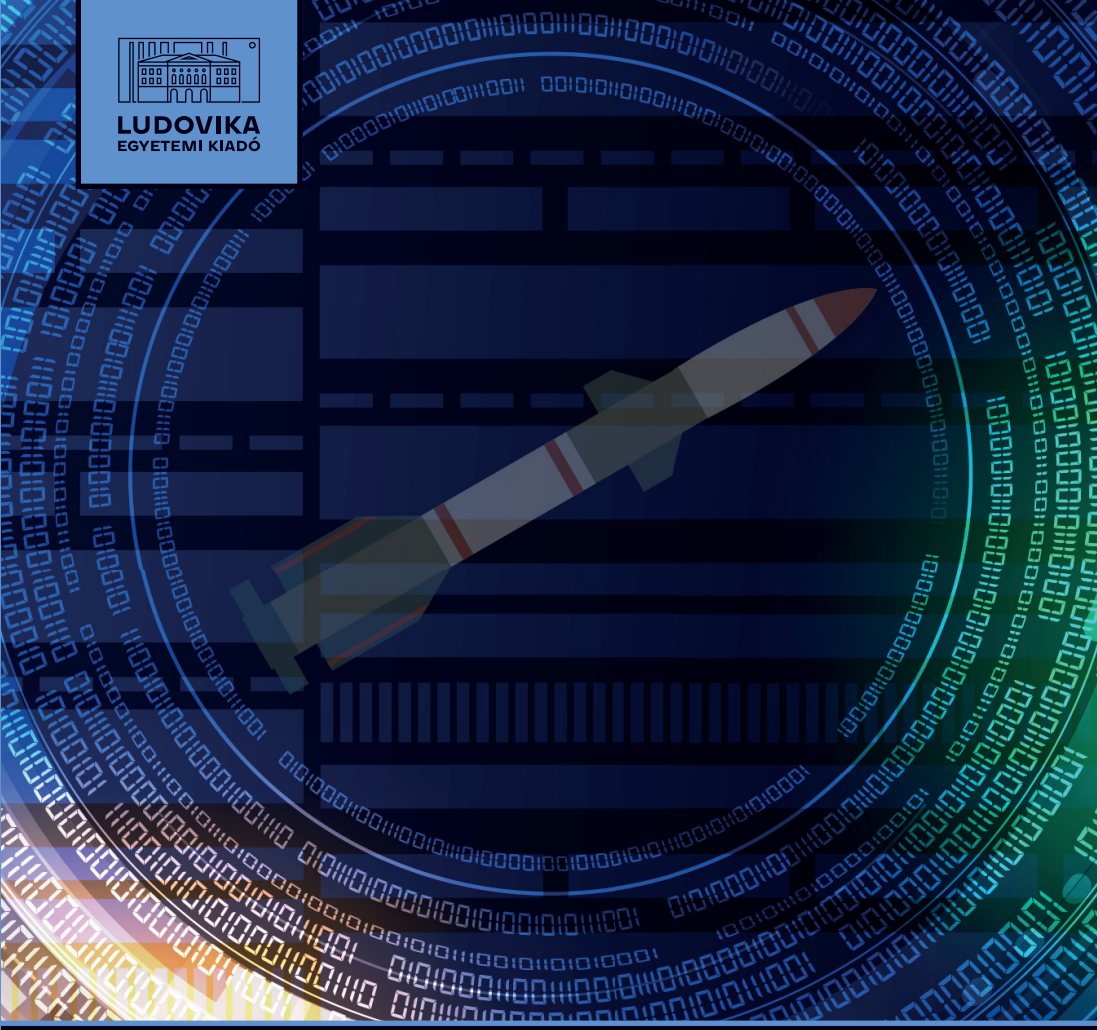
LUDOVIKA
EGYETEMI KIADÓ



Kovács László

Hadviselés a 21. században: kiberműveletek

Kovács László

Hadviselés a 21. században: kiberműveletek

Kovács László

Hadviselés a 21. században: kiberműveletek

LUDOVIKA
EGYETEMI KIADÓ
Budapest, 2023

Szerző
Kovács László

Szakmai lektor
Haig Zsolt

Kiadja a Nemzeti Közszolgálati Egyetem
Ludovika Egyetemi Kiadó
A kiadásért felel: Deli Gergely rektor

Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: kiadvanyok@uni-nke.hu

Felelős szerkesztő: Varga Zoltán
Olvasószerkesztő: Kalcsics Ildikó
Korrektor: György László
Tördelőszerkesztő: Stubnya Tibor

ISBN 978-963-531-765-3 (nyomtatott)
ISBN 978-963-531-954-1 (elektronikus PDF) | ISBN 978-963-531-955-8 (ePub)

© A szerző, 2023
© A kiadó, 2023

Minden jog védve.

Tartalom

Rövidítések jegyzéke

5G	5th generation	5. generációs (kommunikáció)
ACT	Allied Command of Transformation	Szövetséges Transzformációs Parancsnokság
AI	artificial intelligence	mesterséges intelligencia
APT	advanced persistent threat	folyamatosan fennálló, nagyon fejlett támadás
AR	augmented reality	kiterjesztett valóság
C2	command and control	vezetés és irányítás
C4ISR	command, control, communications, computers, intelligence, surveillance, reconnaissance	vezetés, irányítás, kommunikáció, számítógépek, hírszerzés, megfigyelés, felderítés
CCD	charge-coupled device	töltéscsatolt eszköz
CCDCOE	Cooperative Cyber Defence Centre of Excellence	Kibervédelmi Kiválósági Központ
CDC	Cyber Defence Committee	Kibervédelmi Bizottság
CDMB	Cyber Defence Management Board	Kibervédelmi Irányító Testület
CIMIC	civilian-military cooperation	civil-katonai együttműködés
CIS	communication and information system	kommunikációs és információs rendszer
CEPS	Centre for European Policy Studies	Európai Politikai Tanulmányok Központja
CMF	Cyber Mission Force	Kiberműveleti Erő
CNO	computer network operations	számítógép-hálózati műveletek
COTS	commercial off-the-shelves	polcról levehető termék
CyOC	Cyberspace Operation Center	Kibertérműveleti Központ
DoS	denial of service	túlterheléses támadás
DDoS	distributed denial of service	elosztott túlterheléses támadás
DESI	Digital Economy and Society Index	digitális gazdasági és társadalmi index
DNS	Domain Name Service	domainnév-szolgáltatás
DSTL	Defence Scientific and Technology Laboratory	Védelmi Tudományos és Technológiai Laboratórium
EBESZ		Európai Biztonsági és Együttműködési Szervezet
ENISA	European Union Agency for Cybersecurity	Európai Uniós Kiberbiztonsági Ügynökség
ENSZ		Egyesült Nemzetek Szervezete
EPCIP	European Programme for Critical Infrastructure Protection	Európai program a kritikus infrastruktúrák védelmére

EU	European Union	Európai Unió
EW	electronic warfare	elektronikai hadviselés
GCHQ	Government Communication Headquarters	Kormányzati Kommunikációs Főparancsnokág
GCI	Global Cybersecurity Index	globális kiberbiztonsági index
GIS	geoinformation system	geoinformációs rendszer
IoT	Internet of Things	a „dolgok internete”
IP	Internet Protocol	internetprotokoll
KLE	key leader engagement	kapcsolattartás kulcsvezetőkkel
LOIC	Low Orbit Ion Cannon	
MAC	Media Access Control	médiaelérés-vezérlés
MI		mesterséges intelligencia
MilCERT	Military Computer Emergency Response Team	Katonai Elektronikus Információbiztonsági Eseménykezelő Központ
MILDEC	military deception	katonai megtévesztés
MilPA	military public affairs	katonai tömegtájékoztatás
NAC	North Atlantic Council	Észak-atlanti Tanács
NATO	North Atlantic Treaty Organisation	Észak-atlanti Szerződés Szervezete
NC3	NATO Consultation, Control and Command	NATO Konzultációs, Irányítási és Vezetési Testület
NCIA	NATO Communication and Information Agency	NATO Kommunikációs és Információs Ügynökség
NCIRC	NATO Computer Incidence Response Team	NATO Számítógép-vészhelyzeti Reagálócsoport
NCF	National Cyber Force	Nemzeti Kibererő
NCW	network-centric warfare	hálózatközpontú hadviselés
NCSC	National Cyber Security Center	Nemzeti Kiberbiztonsági Központ
NCSI	National Cyber Security Index	nemzeti kiberbiztonsági index
NIS	network and information security	hálózati és információs rendszerek biztonsága
NSA	National Security Agency	Nemzetbiztonsági Ügynökség
OPSEC	operations security	műveleti biztonság
OSINT	open-source intelligence	nyílt forrású felderítés
PLC	programmable logic controller	programozható logikai vezérlő
PPP	presence, posture, profile	megjelenés, viselkedés, arculat
PSYOPS	psychological operations	lélektani műveletek
SA	Situational Awareness	helyzetérzékelés és -felismerés
SCADA	supervisory control and data acquisition	ipari rendszerirányító rendszer

SCEPVA	Sovereign Cyber Effects Provided Voluntarily by Allies	Szuverén kiberképességek önkéntes szövetségesi átadása
SDR	software defined radio	szoftverrádió
SHAPE	Supreme Headquarters Allied Powers Europe	Szövetséges Erők Európai Főparancsnoksága
SIGINT	signals intelligence	rádióelektronikai felderítés
SIM	Subscriber Identity Module	előfizető-azonosító modul
SOCMINT	social media intelligence	közösségimédia-felderítés
STEM	science, technology, engineering, and mathematics	természettudomány, technológia, mérnöki tudomány és matematika
UN ITU	United Nations International Telecommunication Unit	Egyesült Nemzetek Szervezete Távközlési Egyesülete
USCYBERCOM	United States Cyber Command	Egyesült Államok Kiberparancsnoksága
VR	virtual reality	virtuális valóság

Vákát

Képek jegyzéke

Vákát

Táblázatok jegyzéke

Vákát

Bevezetés

Az emberiség történetében ősidők óta jelen van a háborúskodás. A háborúk megvívásának módjai minden korban összefüggtek az adott kor technikai és technológiai színvonalával. A hadviselés mindig a technika és a technológia fejlődésével változott és változik ma is.

A digitális korban a hadviselés célja már nem elsősorban az élőerő pusztítása, hanem a digitális technikára alapozott infokommunikációs rendszereken keresztül a hadseregek vezetési rendszereinek a bénítását vagy azok működésének korlátozását igyekszik elérni a támadó. Ugyanakkor a digitális rendszerek globalitásának köszönhetően a hadviselés ma már a mindennapjainkban is jelen lehet, ami nem elsősorban fegyveres konfliktusok formájában, hanem a befolyásolásban vagy a mindennapi élethez szükséges létfontosságú rendszerek támadásában jelentkezik.

Az azonban nagy bizonyossággal kijelenthető, hogy még jó ideig velünk lesznek a fizikai térben – a szárazföldön, a levegőben, a tengereken és talán egyre inkább az űrben is – folytatott fegyveres összecsapások is, de ezeket egyre inkább kiegészítik a kibertérben folytatott katonai célú műveletek. Ezek a műveletek a jövőben a fegyveres küzdelem szerves részét fogják képezni, mígnem egyszer csak átveszik a kinetikus energiájú fegyvereken alapuló harc szerepét.

A hadviselés tehát ma is változik, mint ahogy elvei és eszközei is. A mesterséges intelligencia vagy a robotok katonai alkalmazása, a számítógépes vezetés és fegyverirányítás, illetve éppen az ezek ellen intézett támadások egyre inkább a katonai gondolkodás és nem utolsósorban a katonai műveletek szerves részét képezik.

A hadviselés említett fejlődése azonban nem zajlik egyformán és egyszerre mindenhol. Ráadásul ez a fejlődés nem is zökkenőmentes minden országban. A nagy katonai-politikai szövetségekben, mint például a NATO, komoly diskurzusok folynak arról, hogy egyrészt hogyan tud a szervezet megfelelni a 21. század új típusú kihívásainak, illetve hogyan lehet a tagállamokat egységesen felkészíteni ezeknek a kihívásoknak a kezelésére, és így ütőképes, a kor kihívásainak megfelelni és egymással együttműködni képes hadseregeket építeni.

Az egységesítés mind technikai téren, mind az eljárásokban igen fontos, hiszen csak egymással interoperábilis rendszerekkel lehet biztosítani több

nemzet együttműködését, és ez az együttműködés csak akkor lehet sikeres, ha a műveleti eljárások a tervezéstől a logisztikán át a harci műveletekig – legalább részben – egységesek.

A kiberhadviselés a kinetikus műveletek támogatása mellett azonban egy másik területen is egyre inkább teret nyer. Ez pedig nem más, mint a szemben álló vagy potenciálisan szemben álló fél, illetve annak civil infokommunikációs rendszereinek kibertérből történő támadása. Ennek oka – mint ahogy látni fogjuk könyvünk első fejezeteiben – az, hogy a 21. század társadalmának egyik meghatározó eleme a digitális technika és technológia, amely azonban ma még rendkívül sérülékeny és sebezhető. Ezt a sérülékenységet kihasználva ma már jóval kisebb energiabefektetéssel jóval nagyobb kár okozható vagy befolyás szerezhető egy szemben álló országban, mint korábban.

A két fő irány – azaz a hagyományos katonai tevékenységek és az olyan új műveletek, mint a kibertéri akciók – egyidejű, jól meghatározott cél vagy célok elérése érdekében történő alkalmazását jelenti a hibrid hadviselés kifejezés. Ebben az új típusú hadviselésben az egyik legfontosabb elemnek a kibertérben megvalósított műveletek összessége tekinthető. Ezek a kiberműveletek azonban ma már nemcsak a kibertérre vannak hatással, hanem azon túlnyúló módon a fizikai térben is – többnyire negatív – hatásokat okoznak.

A jövő hadviselése rendkívül komplex környezetben fog zajlani. A lineáris katonai műveletek helyett egyre inkább az egyszerre több helyen és akár több dimenzióban vagy több műveleti térben végrehajtott katonai tevékenységek összessége lesz a jellemző. A több dimenzió miatt multitérműveletekről, a több helyszín miatt pedig elosztott műveletekről beszélünk. Ezek hatalmas kihívás elé állítják a hadseregeket, azok vezetését és a vezetéshez szükséges infokommunikációs rendszereket is. Ezek az infokommunikációs rendszerek azonban szintén a digitalizációra épülnek. Ennek megfelelően elengedhetetlen ezen rendszerek esetén a kiberbiztonság garantálása, fenntartása és folyamatos fejlesztése. Ugyanakkor, a másik oldalról tekintve minderre, a szemben álló fél infokommunikációs eszközeinek és rendszereinek támadása a mindennapok katonai tevékenységének része lett. Így a kiberhadviselés a hagyományosnak mondott katonai műveletek szerves részévé vált és válik folyamatosan. A kiberhadviselés azonban új filozófiát, új eljárásokat és nem utolsósorban új eszközöket, jól felkészült katonákat, valamint civil mérnököket is követel. Az ő felkészítésük nemcsak katonai feladatot jelent, hanem ebben a munkában nagy és elengedhetetlen szerepe van az akadémiai szférának, a kutatóintézeteknek, az egyetemeknek és a kiberbiztonság területén működő vállalatoknak.

Ez pedig kölcsönös és közös munkát jelent a civil társadalom és a hadsereg között.

Jelen könyv azt kívánja bemutatni és megvizsgálni, hogy a kiberműveleteknek és a tágabb értelemben vett kiberhadviselésnek, amely ma már nem is a 21. század jövőbe tekintő, jövőt jelentő futurisztikus jellemzője, hanem a mindennapok része, milyen összetevői, milyen eljárásai és várhatóan milyen eredményei, illetve hatásai vannak, illetve lehetnek.

Mindehhez megvizsgáljuk a hagyományos hadviselés és a kiberhadviselés kapcsolatát, elemezzük a legfontosabb kibertéri eseményeket, illetve górcső alá vesszük, hogy a hadseregek milyen szervezetekkel készülnek fel nemcsak a kibervédelem, hanem az offenzív kiberműveletek, azaz a támadó jellegű kibertevékenységek végrehajtására.

Könyvünk külön nem elemzi, de fontos megjegyezni, hogy a Covid–19-pandémia önmagában is felerősítette azokat a főleg rosszindulatú kiberműveleteket, amelyek egyébként a mindennapjainkban már régóta jelen vannak. A világjárvány következtében az otthoni online munkavégzés előtérbe kerülése, a vásárlási szokások megváltozása vagy éppen a vállalatok és egyéb szervezetek vezetésében bekövetkezett, egyre inkább az online térre áthelyeződött tevékenységei vonzották ezeket a műveleteket.

Ez a könyv elsősorban nem a szakembereknek szól, hanem azoknak az érdeklődőknek, egyetemi hallgatóknak, illetve más területen kutatóknak, akik szeretnének világosabb képet kapni napjaink és minden bizonnyal a jövő egyik legperspektivikusabb biztonsági és védelempolitikai kihívásáról, a kiberhadviselésről, benne a kiberműveletekről és azok összefüggéseiről.

A kézirat lezárásának ideje: 2022. február.

Vákát

A kiberhadviseléshez és a kiberműveletekhez kapcsolódó legfontosabb fogalmak gyűjteménye

A kiberműveletek és az ezek összességeként értelmezhető kiberhadviselés a hadtudomány rendkívül új területe. Jelenleg az a terminológia, amellyel a kiberműveleteket, illetve az ezekhez kapcsolódó egyes tevékenységeket vagy jellemzőket leírjuk, még csak kialakulóban van. Számos esetben még nincs meg a nemzetközileg egységesen elfogadott definíciós készlet, amely széles körben alkalmazható lenne. E munka elősegítése, valamint a jelen könyvben leírtak érthetősége érdekében néhány fogalom magyarázatát megadjuk. Ezek nem minden esetben általánosan elfogadott vagy hivatalos fogalmi meghatározások – többségük a szerző saját felfogását tükrözi, azonban a leírtak feldolgozásához, pontosabb megértéséheznagyban hozzájárulhat. Amennyiben valamely fogalomnak van hivatalos – jogszabályban, stratégiában, doktrínában stb. – rögzített meghatározása, ennek forrását feltüntetjük, illetve a magyar fogalom mellett megadjuk annak angol megfelelőjét is.

5G: az az 5. generációs, vezeték nélküli hálózat, illetve a kapcsolódó technológia, amely a mobilkommunikációban standarddá vált. Ma már ez a technológiai alapja számos infokommunikációs szolgáltatásnak.

Biztonság *(security):* az eszközök, rendszerek és hálózatok olyan megkívánt állapota, amelyben a veszélyek megfelelő szintű kezelése megtörténik.

Botnet (lásd zombihálózat): megfertőzött (kompromittált) internetre kötött számítógépek olyan hálózata, amelyet elsősorban rosszindulatú tevékenységre használnak a hálózatot létrehozók.

Digitális ökoszisztéma *(digital ecosystem):* nagy sávszélességű infrastruktúra, képzett felhasználók, digitális szolgáltatásokat használó és azokra épülő üzleti szféra, fejlett és intenzív K+F+I ipar, digitális szolgáltató állam, online elérhető kereskedelmi szolgáltatások, digitális archívumok olyan összessége, amely a tudásalapú társadalom meghatározó tényezőjeként értelmezhető.

DoS/DDoS *(denial of service / distributed denial of service):* túlterheléses / elosztott túlterheléses támadás, amely egy vagy több számítógépről a megtámadott,

azaz a célszámítógép felé érkező lekérdezést jelent. Amennyiben a lekérdezések száma meghaladja a célpont által kiszolgálni képes lekérdezésszámot, akkor működése korlátozott lesz vagy ellehetetlenül.

Elektronikus információbiztonság *(electronic information security):* az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.[1]

Infokommunikáció *(infocommunications):* az informatika és a kommunikáció konvergenciája révén létrejövő technológia, eszközök és rendszerek gyűjtőfogalma.

Információs műveletek *(information operations):* az a törzsfunkció, amelynek célja, hogy az információs környezet elemzése alapján megtervezze és integrálja, majd értékelje az információs tevékenységeket úgy, hogy azok végrehajtása a küldetés célkitűzéseinek elérése érdekében biztosítsa a kívánt hatást a célközönség akaratában, megértésében és képességeiben. A célközönséget a szemben álló felek, a lehetséges szemben álló felek és más, a politikai szint által jóváhagyott személyek és meghatározott csoportok alkotják.[2]

Infrastruktúra *(infrastructure):* létesítmények, hálózatok, rendszerek és üzemeltető szakemberek összessége, amelyek és akik hozzájárulnak a társadalom alapvető szükségleteinek kielégítéséhez.

Internet *(Internet):* olyan globális kiterjedésű számítógép-hálózat, amelyben számítógép-hálózati protokollok kapcsolják össze a felhasználókat és a szolgáltatásokat.

Katonai kibertérműveletek *(military cyberspace operations):* a kibertérben megvalósuló olyan katonai kibertevékenységek, amelyek a saját kibertéri

[1] Lásd 2013. évi L. tv. az állami és önkormányzati szervek elektronikus információbiztonságáról.
[2] Lásd Magyar Honvédség: *Információs műveletek doktrína* (2014). 1. kiadás. (Ált/57.)

rendszerek védelmére és/vagy a szemben álló fél kibertéri rendszereinek támadására irányulnak.

Kiberbiztonság *(cyber security):* a kibertérre értelmezett, annak biztonságát meghatározó eszközök, politikák, koncepciók, technológiák, irányelvek, kockázatkezelési módszerek, tevékenységek, képzések, valamint a legjobb gyakorlatok összessége. Mindezek célja, hogy megvédjék a számítógépes környezetet, az ezt használó szervezetek és felhasználók eszközeit, rendszereit.

Kiberbiztonsági esemény *(cyber security event):* nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

Kiberfelderítés *(cyber intelligence, surveillance and analysis):* a kibertérben folytatott hírszerzési, megfigyelési és felderítési célú adat- és információgyűjtés, valamint a szükséges adat- és információfeldolgozás együttese.

Kiberfenyegetés *(cyber threat):* a kibertérben megjelenő, a kiberteret alkotó infokommunikációs és más elektronikus rendszerek biztonságát veszélyeztető, sérülékenységét kihasználni képes potenciális (kölcsön)hatás.

Kiberhelyzetkép *(cyberspace operational picture):* a kibertéri helyzetre vonatkozó adatok gyűjtése, feldolgozása és értékelése, valamint az ezekből levont következtetések eredményeként létrejövő, a kialakult kiberhelyzetről alkotott kép és annak általában vizuális megjelenítése.

Kibertámadás *(cyber attack):* az offenzív kibertérműveletek részeként a szemben álló fél infokommunikációs vagy más elektronikus rendszereibe történő behatolást és ott káros hatások okozását jelenti ezen rendszerek működésének akadályozásával és/vagy az ezeken a rendszereken tárolt, feldolgozott vagy továbbított információk, illetve adatok módosításával, eltulajdonításával vagy azokhoz történő hozzáférés akadályozásával.

Kibertér *(cyberspace):* globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint a közvetítésükkel adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese. Más megfogalmazásban: felhasználók, eszközök, szoftverek, folyamatok, tárolt vagy átvitel alatt lévő információk, szolgáltatások és rendszerek gyűjtőfogalma, amelyek közvetlenül vagy közvetett módon számítógép-hálózathoz vannak kapcsolva.

Kibertérműveletek/kiberműveletek *(cyberspace operations):* a kibertérben vagy azon keresztül végzett olyan tevékenységek, amelyek célja, hogy a saját kibertéri és valós téri cselekvési szabadságát megőrizzék, és/vagy olyan hatásokat hozzanak létre, amelyek hozzájárulnak a saját célok eléréséhez.

Kibertérműveleti fellépés *(cyberspace operational action):* A kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelemre, az ezekre történő felkészülésre, a folyamatban lévők megszakításához szükséges reagálásra, valamint a kapcsolódó biztonsági feladatok ellátására irányuló passzív vagy aktív védelmi, illetve támadó jellegű beavatkozások, intézkedések összessége.

Kibervédelem *(cyber defence):* a kibertérből érkező fenyegetések elleni védelem, ideértve a saját kibertéri képességek megőrzését is.

Kritikus információs infrastruktúra *(critical information infrastructure):* olyan hálózatszerű fizikai vagy virtuális rendszereket, eszközöket és módszereket (eljárásokat, szolgáltatásokat) foglal magában, amelyek az információ folyamatos biztosításának és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban kritikus rendszerek vagy más azonosított kritikus rendszer működéséhez nélkülözhetetlenek. A fogalom hivatalos megnevezése létfontosságú információs rendszer, rendszerelemek.

Kritikus infrastruktúra *(critical infrastructure):* olyan eszköz, létesítmény vagy rendszer, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős negatív következményekkel járna. A fogalom hivatalos megnevezése létfontosságú rendszer, rendszerelemek.

Malware: rosszindulatú program, amely az angol Malicious Software, azaz rosszindulatú program szavakból alkotott mozaikszó. Azok a programok

tartoznak a malware-ek kategóriájába, amelyek engedély nélkül jutnak a megcélzott számítógépre, abból a célból, hogy annak működését akadályozzák vagy az abban kezelt adatokat manipuláljak, onnan kijuttassák.

Mesterséges intelligencia *(artifical intelligence):* gépi és/vagy szoftveres úton létrejövő intelligencia, amely képes emberi beavatkozás nélkül a változó környezettel interakciót folytatni, a természetes intelligenciához hasonló módon képes problémamegoldásra, valamint a tanulásra.

Nem kinetikus képességek *(non-kinetic capabilities):* nem kinetikus energián alapuló olyan képességek, amelyek közvetlen hatásaikat az információs, a kognitív és a kibertérben fejtik ki, de közvetett hatásaik a fizikai térben is jelentkezhetnek.

Nulladik napi sérülékenység *(zero-day exploit):* olyan szoftver- vagy hardversérülékenység, amelyre még nincs kiadva védelmi megoldás.

Offenzív kibertérművelet *(offensive cyberspace operation):* a kibertérben vagy azon keresztül kezdeményezett olyan tevékenység, amely a műveleti célból végzett kibertéri felderítés, információszerzés és -feldolgozás eredményeire építve a célkezelést, a kibertámadást és annak hatásainak elemzését foglalja magában.

Pszichológiai manipuláció *(social engineering):* az emberi hiszékenységet kihasználó olyan támadási technika, amely során a támadó megtévesztéssel vagy zsarolással jut a rendszerekhez hozzáférést nyújtó adatokhoz, információkhoz.

Sérülékenység *(vulnerability):* kiberteret alkotó infokommunikációs és más elektronikus rendszerek olyan tulajdonsága vagy gyengesége amelynek révén egy kiberfenyegetés érvényre juthat.

Védelem *(defence):* olyan tevékenységek összessége, amelyek a biztonság megteremtésére és fenntartására irányulnak.

Zombihálózat *(botnet):* olyan kompromittált számítógépek hálózata, amelyek a támadó szándéka szerinti rosszindulatú tevékenység végzésére utasíthatók a felhasználók tudta nélkül.

Zsarolóvírus *(ransomware):* olyan rosszindulatú program, amelyet arra terveztek, hogy titkosítsa az eszközön lévő fájlokat, használhatatlanná téve azokat és a rájuk támaszkodó rendszereket. Az elkövetők általában váltságdíjat követelnek a titkosítás visszafejtéséért cserébe.[3]

[3] CISA: Ransomware 101. *Stop Ransomware,* 2022.

1. fejezet

A digitális kor és hadviselése

1.1. Digitalizáció

1.1.1. Digitális társadalom és gazdaság

Manuel Castells szociológus szerint a ’90-es években megfogalmazott hálózatos társadalom elméletétől[4] a teljes digitális ökoszisztémáig nagyon rövid időn belül hatalmas változás állt be a világ működésében. Ez a változás azonban annyira természetes lett mára, hogy a hétköznapi életünkben sokszor már fel sem tűnik. Annyira hozzászoktunk az újabb és újabb információtechnológiai, azaz röviden csak IKT-eszközök[5] rendszeres megjelenéséhez, hogy már maga a folyamat is életünk szerves részét képezi. Napjainkban már nemcsak az új formájú és design-elemekkel díszített IKT-eszközök megjelenése a fontos, hanem funkcionalitásuk és minél előnyösebb, könnyebb és egyszerűbb, ugyanakkor minél sokoldalúbb használatuk is. Azok az infokommunikációs eszközök jellemzik igazán a 21. századot, amelyeknek egyik legszemléletesebb példái az okostelefon vagy a mobilizálható számítógépek – tabletek, laptopok –, illetve az ezek működését lehetővé tevő forradalmi technológiák, mint például az 5G mobilkommunikáció, továbbá ezeknek az okoseszközöknek a háztartásokban való megjelenése.

Az infokommunikációs technológia komplett digitális ökoszisztémává fejlődött napjainkra. Maga a digitális ökoszisztéma egyfajta meghatározás szerint nem más, mint „nagy sávszélességű infrastruktúra, képzett felhasználók, digitális szolgáltatásokat használó és azokra épülő üzleti szféra, fejlett és intenzív K+F+I ipar, digitális szolgáltató állam, online elérhető kereskedelmi szolgáltatások, digitális archívumok olyan összessége, amely a tudásalapú társadalom

[4] Manuel Castells: *A hálózati társadalom kialakulása. Az információ kora.* I. kötet. Budapest, Gondolat–Infonia, 2005.

[5] Az IKT rövidítést az információtechnológia, a kommunikáció, valamint a médiatechnológia konvergenciájaként létrejött infokommunikációs technológia leírására alkalmazzuk.

meghatározó tényezőjeként értelmezhető".[6] Ez ma már nemcsak össztársadalmi szinten értelmezhető kifejezés, hanem akár szervezeti, vállalati szinten is egyre gyakrabban használatos, amely az adott cég vagy vállalat tevékenységének teljes spektrumában megjelenő digitális eszközök, rendszerek és szolgáltatások összességét jelenti, kezdve a tervezéstől a gyártáson át a vállalat termékeinek vagy szolgáltatásainak az értékesítéséig.

A fentiekből következően a digitális ökoszisztéma kialakítása, fenntartása és nem utolsósorban fejlesztése 21. századi életünk minden területén elengedhetetlen. Digitális rendszerek szövik át a társadalom legtöbb funkcióját, kezdve az oktatástól az egészségügyön át a védelmi szféráig. Ma a digitális technológia, a digitális technológiára épülő infokommunikációs eszközök és rendszerek segítségével megvalósuló szolgáltatások nélkül nagyon nehéz lenne elképzelni a mindennapi életünket. A digitális ökoszisztéma a kutatás-fejlesztéstől a gyártáson át minden olyan digitális technikát és technológiát magában foglal, amely a 21. század sajátja.

Az Európai Unió külön mérőszámrendszert alkotott arra, hogy az egyes tagországok digitális fejlettségét össze lehessen hasonlítani. Ez az úgynevezett digitális gazdasági és társadalmi index, amely az angol megnevezésből – *Digital Economy and Society Index* – származó DESI-index elnevezést viseli. A DESI az adott ország digitális gazdasági és társadalmi fejlettségét méri. 5 fő és több mint 30 kisebb indikátora képes mérhetővé tenni, hogy hol tart az adott ország a digitális technológia fejlettségében,[7] és ez milyen hatással van magára az országra, annak állampolgáraira, vállalkozásaira, azok fejlettségére.[8]

A 21. század digitális ökoszisztémája azonban nem nélkülözheti a biztonság, esetünkben – nem elhanyagolva számos más terület biztonságát sem – elsősorban a digitális biztonság megteremtését, illetve jelenti az annak folyamatos fejlesztését érintő kérdések vizsgálatát. Ez a digitális biztonság ma a kiberbiztonságban manifesztálódik. A kiberbiztonság összefoglalja azokat a részterületeket, amelyek a teljes és komplex módon értelmezett biztonság megteremtéséhez szükségesek. A kiberbiztonság fejlettségi szintjének megítélését segítik azok a külön mérőszámrendszerek, amelyek a digitális technológia e meghatározó szegmensének az összehasonlítására alkalmasak. Ilyen mérőszámrendszer például

[6] Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018b. 17.

[7] Magyarország 2020-ban az európai uniós tagországok között a 21. helyet foglalta el a DESI alapján, 2019-ben pedig a 23. helyen állt.

[8] Kovács (2018b): i. m. 27.

az ENSZ Távközlési Egyesületének (UN International Telecommunication Unit, ITU) globális kiberbiztonsági indexe (*Global Cybersecurity Index,* GCI)[9] vagy az úgynevezett nemzeti kiberbiztonsági index (*National Cyber Security Index,* NCSI),[10] amelyet észt kezdeményezésre ma már egy nemzetközi csapat fejleszt.[11]

Persze ez a digitális társadalom és a hozzá kapcsolódó infrastruktúrák nem egyik napról a másikra alakultak ki. Az 1960-as években megszületettek az elosztott számítógép-hálózatok, majd az ezt követő – az 1970-es évek elején kezdődő, de az 1980-as évek elejétől robbanásszerűen bekövetkező – forradalom a személyi számítógépek elterjedése terén ma már azt jelenti, hogy több milliárd számítógép van hálózatba kötve. Ezek a számítógépek ma már nemcsak a klasszikus személyi számítógépeket jelentik, hanem a mindennapi élet legapróbb szegmensében is jelen lévő, a hálózaton kommunikálni képes intelligens eszközöket is magában foglaló rendszerek együtteséről beszélhetünk. Az úgynevezett „dolgok internete", azaz angol megnevezéssel az *Internet of Things*- vagy csak röviden IoT-eszközök ma már saját meghatározást is kaptak. A már említett ITU még 2012-ben egyik ajánlásában az IoT-t a következőképpen definiálta: „A dolgok internete az információs társadalom globális infrastruktúrája, amely lehetővé teszi a fejlett szolgáltatások összekapcsolását (fizikai és virtuális értelemben egyaránt), a már meglévő és a fejlesztés alatt lévő interoperábilis infokommunikációs technológiákra építve."[12]

Az IoT-eszközök valóban ott vannak a nappalinktól kezdve az autónkig az élet minden területén. Ma már okosvárosokról, okosotthonokról beszélünk, amelyeknek legfontosabb eszközei az említett IoT-eszközök. Ezek képesek a hálózaton áramló adatokat akár a fizikai térben megvalósuló különböző tevékenységgé lefordítani vagy átváltani, és így képesek az okosotthonokat vezérelni vagy akár az önvezető okosgépjárműveinket egyik pontról a másikra elvezetni.

A számítógép-hálózatok és kimondottan az internet egyik legfontosabb problémája a 21. században a mérhetetlen mennyiségű információ, illetve az ebből a számunkra releváns és fontos információ kinyerése, valamint lehető leggyorsabb és leghatékonyabb felhasználása. Erre a munkára persze létrejöttek a nagy

[9] Magyarország az ITU globális kiberbiztonsági indexén 2020-ban az európai országok összehasonlításában a 22. helyen állt, míg világviszonylatban a 35. helyezést szerezte meg.

[10] Hazánk az NCSI-indexen 2021-ben a 30. helyen állt globális összehasonlításban.

[11] Kovács László: *A kiberbiztonság stratégiai megközelítése.* Doktori értekezés. Budapest, Magyar Tudományos Akadémia, 2018a. 33.

[12] ITU: *ITU-T Recommendations* (2012. június 15.).

keresőgépek, amelyek hatalmas fejlődésen mentek keresztül az elmúlt kettő, kettő és fél évtizedben. Ugyanakkor a felszín alatt az úgynevezett szürke vagy – angol terminológiával élve – *deep web*et találjuk, amely keresőgépekkel még csak nem is indexált tartalommal van jelen. A hálózat ezen része így az átlagos felhasználó számára láthatatlan módon, de mégis létezik.

A digitalizáció nem hagyta érintetlenül az ipart sem. Az ipar digitalizálása és az úgynevezett negyedik ipari forradalom – vagy egyes szakértők szerint másként megfogalmazva az ipari forradalom negyedik szakaszának – beköszöntével egy olyan új korszak hajnalán vagyunk, amely eddig az emberi történelem során még a gépi ipari korszak korábbi vívmányait is felülmúló módon alakítja át világunkat.

A digitalizáció, benne a számítógépek és nem utolsósorban az internet fejlődése – összehasonlítva az emberiség technikai-technológiai fejlődésével – rendkívül gyorsan és dinamikusan, mondhatni forradalmi változásokat okozva ment végbe. Ez igaz is, hiszen a digitalizáció története csak néhány évtizedet ölel fel, amely azonban mégis gyökeresen átalakította világunkat.

Van azonban egy hatalmas probléma, amely komplex biztonsági kihívást jelent a digitális 21. században. Ez nem más, mint a digitális rendszerek sebezhetősége, illetve sérülékenysége. A kiberhadviselésnek egyik legfontosabb célja – és így eszköze is – ezeknek a sebezhetőségeknek a kihasználása. Erről a későbbiekben a kiberhadviselés tárgyalásánál részletesen szót ejtünk.

Ugyanakkor a digitális fejlődés nem állt meg, és jelenleg is zajlik. Ez a fejlődés naponta jelenti olyan új technológiák megjelenését, mint például a mesterséges intelligencia, a blokklánc-technológia vagy a kvantum-számítástechnika, amelyek azonban nemcsak forradalmian új előnyöket, hanem egyben számos biztonsági kihívást is hordoznak.

1.1.2. A digitális társadalom kritikus (létfontosságú) rendszerei

A fentiekben körülírt digitális társadalom esetében világosan látszik, hogy ma már erősen függ azoktól a működését segítő infokommunikációs eszközöktől és rendszerektől. Más szóval, ezek a rendszerek fontosságukat tekintve elérték azt a szintet, amikortól létfontosságúvá, meglétükben és működésükben kritikussá váltak. Ezért ezeket a rendszereket kritikus infrastruktúráknak, illetve kritikus információs infrastruktúráknak hívjuk. Az ezek ellen intézett rosszindulatú támadások már az európai unió 2020 végén megjelent új

kiberbiztonsági stratégiája szerint is az egyik legfontosabb veszélyforrásnak tekinthetők.[13] Ez az egyszerűnek tűnő megállapítás azonban rávilágít egy nagyon komoly tényre, amely könyvünk szempontjából kiemelkedően fontos. Mivel ezek az infrastruktúrák alapvetően hálózatos informatikai eszközök, az ellenük intézett támadások volumene, nagysága és nem utolsósorban ezek következményei elérhetik azt a szintet, amikortól már kiberhadviselésről kell beszélnünk.

A kritikus struktúrák védelmének hazai, illetve európai uniós történetének vizsgálatához egészen 2005-ig kell visszamennünk az időben. Az Európai Unióban ekkor született meg az úgynevezett zöld könyv, amely az európai kritikus infrastruktúrák védelméről szólt, bár akkor még csak koncepcionális szinten.[14] Erre a dokumentumra építve született meg 2006-ban az Európai Unió kritikusinfrastruktúra-védelmi programja (*European Programme for Critical Infrastructure Protection,* EPCIP),[15] amely sok európai ország, így Magyarország azonos célú programjának alapjaként is szolgált. Azt már a szabályozás korai szakaszában, tehát a kétezres évek közepén sikerült rögzíteni, hogy melyek azok a legfontosabb ágazatok, illetve ezeken belül a legfontosabb alágazatok, amelyek kritikus, más szóval létfontosságú rendszernek vagy rendszerelemnek tekinthetők. Ezt követően megszülettek azok az eljárások, amelyek alapján ezek az infrastruktúrák, illetve egyes elemeik kritikusként, azaz létfontosságúként besorolhatók.

A kritikus infrastruktúrák védelmének hazai szabályozása 2008-ban kezdődött, ám ekkor még csak egy kormányhatározat[16] definiálta a szabályokat, illetve sorolta fel a legfontosabb ágazatokat. A hazai törvényi szabályozásra egészen 2012-ig kellett várni, amikor is megszületett a hazai kritikus infrastruktúra védelméről szóló törvény. A törvény címe a létfontosságú rendszerekre és rendszerelemekre utal, amely az addig a szaknyelvben „kritikus"-nak nevezett rendszereket fedi le.[17] Az azonban nyugodtan kijelenthető, hogy ez a törvényi

[13] Európai Bizottság: *Közös közlemény az Európai Parlamentnek és a Tanácsnak. Az EU kiberbiztonsági stratégiája a digitális évtizedre.* JOIN(2020) 18 final (2020. december 16.).

[14] Európai Közösségek Bizottsága: *Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról.* COM(2005) 576 végleges (2005. november 17.).

[15] Európai Közösségek Bizottsága: *A Bizottság közleménye a létfontosságú infrastruktúrák védelmére vonatkozó európai programról.* COM(2006) 786 végleges (2006. december 12.).

[16] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról [sic!].

[17] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

szabályozás sem rendezte mindazokat a kérdéseket, amelyek a digitális rendszerek, azaz a kritikus információs infrastruktúrák védelmének kérdéseivel függnek össze. A kritikus információs infrastruktúrák védelmére csak egy későbbi jogi szabályozás adott részben eligazítást. Ez akár a hazai, de akár az európai uniós szabályozás kritikájaként is felfogható, bár a későbbiekben látni fogjuk, hogy nem sokkal ezt követően az európai uniós szabályozással harmóniában megszületett az a hazai stratégia, amely a hálózati és információs rendszerek biztonsági kérdéseinek egységes megválaszolását jelentette. Persze kérdés, hogy egy stratégia milyen eredményt is ér el, azaz mennyiben hajtják végre, vagy éppen a végrehajtás mennyire hatékony. Az mindenesetre tény, hogy a kritikus infrastruktúrák és kritikus információs infrastruktúrák védelmének állami szabályozása az elmúlt másfél évtizedben hatalmasat lépett előre. Talán ez az egyik oka annak, hogy azok a létfontosságú rendszerek, amelyek valóban elengedhetetlenek mindennapi életünk során, folyamatosan működnek, és bár természetesen nem 100%-os a védelmük, de a működésük mégis megbízható.

A kritikus információs infrastruktúrák fogalmát tehát csak egy későbbi, az említett törvény végrehajtási rendeleteként megjelent kormányrendelet adja meg, amely szerint a kritikus információs rendszerek és létesítmények „a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek”.[18] Ez a meghatározás nagyon jól összefoglalja, hogy ma már nemcsak a hagyományos értelemben vett infrastruktúrák, hanem az ezek vezérlését, működtetését ellátó információs rendszerek közül önmagában is nagyon sok kritikus infrastruktúrának minősül.

Maga a törvény természetesen a kritikus (eredeti megfogalmazásában: létfontosságú) infrastruktúra fogalmát meghatározza. E szerint a kritikus infrastruktúra „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 –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya

[18] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról, 1. § 3. pont.

miatt jelentős következményekkel járna".[19] Ki kell emelni, hogy a törvény a hazai kritikus infrastruktúra meghatározása mellett definiálja az európai kritikus infrastruktúra fogalmát is, a következőképpen: „a törvény alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése jelentős hatással lenne – az ágazatokon átnyúló kölcsönös függőségből következő hatásokat is ideértve – legalább két EGT-államra."[20] Ez a definíció nagyon jól rávilágít arra, hogy a fizikai infrastruktúrák és a digitális rendszerek ma már számtalan helyen összekapcsoltak. Ez egy nagyon fontos tény, hiszen – ahogy a későbbiekben szintén elemezni fogjuk – ez jelenti majd a kiberhadviselés egyik legnagyobb és legfontosabb kérdését is. Ez pedig nem más, mint annak meghatározása, hogy egy-egy kibertámadás vagy egyéb kibertéri művelet milyen kihatással van akár a fizikai infrastruktúrákra is – hiszen ne feledjük: a kibertámadások nemcsak a kibertérben fejtik ki hatásukat, hanem ma már a fizikai térben is (a későbbiekben ezt szintén elemezni is fogjuk). Ráadásul ezek a hatások más, akár az országhatárokon kívüli infrastruktúrákra, az azokon megvalósuló szolgáltatásokra, illetve közvetve az emberek mindennapi tevékenységeire is komoly kihatással lehetnek.

Maga a hazai kritikusinfrastruktúra-védelmi törvény 10 ágazatban és több mint 30 alágazatban rögzíti, hogy Magyarország vonatkozásában melyek a létfontosságú infrastruktúrák.[21] Ezeken belül természetszerűleg megtalálhatók az infokommunikációs rendszerek, illetve az azokon keresztül megvalósuló szolgáltatások is, ugyanakkor ezek elvi védelme nem egy egységes törvényi szabályozásban, hanem a fentiekben is említett különböző jogszabályokban leírt módon valósult meg idehaza. Ezeken túl az egyik legfontosabb, a hazai digitális rendszerek biztonságát meghatározó jogi szabályozás az úgynevezett információbiztonsági törvény, vagy rövidítve az Ibtv. Ez a törvény – hivatalos megnevezésével élve a 2013. évi L. törvény – az állami és önkormányzati szervezetek elektronikus információbiztonságát szabályozza. Azt mélyebb elemzés nélkül is megállapíthatjuk, hogy ez a törvény Magyarország vonatkozásában, de nemzetközi téren is egyaránt korszakalkotó volt, hiszen komplex módon szabályozza az elektronikus információbiztonság és így közvetve a kiberbiztonság különböző kérdéseit. Ez még akkor is igaz, ha kötelező módon csak a közigazgatási szereplőkre vonatkozó jogszabályról beszélhetünk.

[19] 2012. évi CLXVI. tv. 1. § *f)* pont.
[20] 2012. évi CLXVI. tv. 1. § *c)* pont.
[21] 1. melléklet a 2012. évi CLXVI. törvényhez.

A kritikus információs infrastruktúrák európai szabályozásának egyik legfontosabb, fentebb már említett alappillére a 2016-ban született úgynevezett uniós NIS-direktíva. A NIS egy mozaikszó, amely az Európai Parlament és az Európai Tanács hálózati és információs rendszerek biztonságáról szóló közös irányelvének angol címéből *(Network and Information Security)* ered.

A direktíva közel 3 éves komoly jogalkotási-előkészítő munka után született meg 2016-ban, és csak 2018 májusában lépett életbe. Mivel azonban az Európai Parlament és az Európai Tanács közös rendelete, kötelező érvényű az összes európai uniós tagországra nézve. A NIS egyik legfontosabb filozófiai irányelve, hogy egységes követelményrendszert határoz meg a tagországok számára a hálózati és információbiztonság területén. Ez egy olyan nemzetközi szervezet esetében, mint az Európai Unió, nem egyszerű feladat, több oknál fogva sem. Ezek közül az egyik a 28 tagállam (mára 27, de a NIS elfogadásakor, majd életbelépésekor még 28 tagállama volt az EU-nak) már önmagában is nagyon sok ahhoz, hogy viszonylag egységes szabályozást lehessen bevezetni, illetve azt folyamatosan fenntartani, hiszen az országok többsége korábban nemzeti szinten igyekezett ezeket a biztonsági kérdéseket kezelni, amelyeknek most egy külső – uniós – erő hatására meg kellett változniuk. Egy másik, ennél sokkal nyomósabb ok az, hogy az EU-tagországok eltérő digitális fejlettséggel és információbiztonsági szinttel rendelkeznek. Ez azt is jelenti, hogy a kevésbé fejlett infrastruktúrával vagy biztonsági szinttel rendelkező országok kockázatokat hordozhatnak magukban az Unió egészére nézve, hiszen a digitális szolgáltatások jelentős része összekapcsolt az országok között. A NIS-direktíva tehát rákényszerítheti az országokat arra, hogy digitális fejlettségüket, illetve ezzel párhuzamosan a digitális rendszereik biztonságát egyre magasabb szintre emeljék. Ezzel elérhető lehet, hogy egységes legyen a tagországok hálózati és információs rendszereinek biztonsága. A NIS azt is elrendelte, hogy minden országnak stratégiai szinten kell erről a területről döntést hoznia, azaz rendelkeznie kell nemzeti hálózat- és információbiztonsági, illetve kiberbiztonsági stratégiával. Magyarország korábbról már rendelkezik nemzeti kiberbiztonsági stratégiával, bár meg kell jegyezni, hogy az még 2013-ban született.[22] A NIS-direktívának megfelelően tehát ezt egészítette ki egy nemzeti hálózat- és információbiztonsági stratégia hazánkban 2018 végén.

A NIS a kritikus információs infrastruktúrák védelmének európai uniós szintű megvalósítása területén szintén hatalmas előrelépés, mert meghatározza azokat a legfontosabb ágazatokat, amelyek védelme minden tagország számára

[22] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

kiemelt fontosságú kell hogy legyen. Ezek az infrastruktúra-ágazatok felsorolásszerűen: az energia, a közlekedés, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, az ivóvízellátás és -elosztás, valamint a digitális infrastruktúra.

A felsorolt ágazatokból – fentebb tett megállapításainknak megfelelően – szintén nagyon jól látszik, hogy ma már nehezen vagy egyáltalán nem választhatók szét a létfontosságú hagyományos, illetve információs jellegű infrastruktúra-ágazatok. Ez nagyon jól rávilágít arra, hogy gyakorlatilag minden kritikus infrastruktúra tartalmaz kritikus információs infrastruktúrát vagy legalábbis annak egyes elemeit. Így van ez még az internet mint kritikus információs infrastruktúra vonatkozásában is, hiszen ez is tartalmaz olyan szolgáltatásokat vagy olyan elemeket, amelyek nélkülözhetetlenek a működés szempontjából. Az internet vonatkozásában ilyen kritikus rendszerelem például a DNS *(Domain Name Service),* azaz a domainnév-szolgáltatás. Ez az a szolgáltatás, amely nélkül ugyan ideig-óráig még működik az, amit internetnek hívunk, ugyanakkor egy idő után a domainnevek feloldásának hiányában egyre kisebb hatékonysággal tudják a felhasználók vagy akár a különböző szolgáltatások a hálózatot használni.

A kiberhadviselés szempontjából így a DNS-szolgáltatás is kiemelt célpont lehet. Bár a 2000-es évek elején még nem kiberhadviselés-mértékű, de különböző intenzitású kibertámadások több alkalommal is érték a DNS-szolgáltatásokat nyújtó rendszereket – több kísérlet is történt arra, hogy az úgynevezett legfelsőbb szintű DNS-szerverek működését bénítsák meg. Ezek a támadások azonban nem jártak sikerrel.[23] Ezt követően az egyik legnagyobb hasonló támadás 2016-ban történt, amikor az Egyesült Államok nagy DNS-szolgáltató cégét, a Dyn nevű vállalatot érte DDoS- (*Distributed Denial of Service,* azaz elosztott túlterheléses) támadás. Ebben az esetben a Dyn szervereit több hullámban támadták, aminek következtében a cég szolgáltatásai fokozatosan leálltak, s ez nemcsak az Egyesült Államokban, hanem közvetve Ázsia egyes részein is komoly internetkiesést jelentett:[24] a bekövetkezett szolgáltatáskiesés messze túlmutatott az Egyesült Államok határain,[25] mert számos ázsiai IP-cím-tartomány névfeloldása is ezeken

[23] Gyányi Sándor: DDOS-támadások veszélyei és az ellenük való védekezés. *Hadmérnök,* (2007), különszám.

[24] Kovács (2018b): i. m. 92.

[25] Lily Hay Newman: What We Know About Friday's Massive East Coast Internet Outage. *Wired.com,* 2016. október 21.

a megtámadott szervereken keresztül valósult meg, így azok a szolgáltatások is elérhetetlenné váltak.[26]

A későbbi vizsgálatok bizonyították, hogy az úgynevezett Mirai vírus állt a támadások hátterében, amely elsősorban az IoT-eszközöket fertőzte meg.[27] A jól kivitelezett támadássorozat rávilágított arra, hogy az internet gerincét alkotó és egyben az egyik legfontosabb szolgáltatását jelentő domainnév-szolgáltatást bizony sikeresen is lehet támadni, aminek következményei viszont beláthatatlanok lehetnek.

Az internet esetében további kritikus szolgáltatást jelentenek azok a felhőszolgáltatások, amelyek például a nagy közösségi médiumok számára végeznek különböző háttértevékenységeket. 2021 májusában a Fastly nevű felhőszolgáltató rendszerei egy egyébként legitim rendszerfrissítést és a hozzá kapcsolódó beállítást követően összeomlottak.[28] Ennek következtében sok felhasználó rendszerkiesést tapasztalhatott az olyan szolgáltatások esetében, mint például a Reddit, az Amazon, illetve jó néhány közösségimédia-szolgáltatás, hiszen ezek a platformok is a Fastly felhőszolgáltatását használták és használják részben ma is háttértevékenységeikhez.

Ez az eset jól mutatja, hogy az említett szolgáltatásokon belül (legyen szó akár az Amazonról vagy bármelyik nagy közösségi médiumról) szintén létfontosságú információs – vagy ha tetszik, létfontosságú internetes – szolgáltatásokról kell beszélnünk. Azaz ma már léteznek olyan kritikus rendszerek, amelyeken belül egyes rész-szolgáltatások, illetve rendszerelemek is kritikusnak minősülnek.

A kiberműveletek kontextusában, illetve a kiberhadviselés célpontjainak szemszögéből vizsgálva természetszerűleg ezek a rendszerek vagy rendszerelemek lesznek az első számú célpontok, amelyek védelme – csakúgy, mint általánosságban a kritikus információs infrastruktúrák védelme – ennek megfelelően kiemelten fontos. Mivel ezek a szolgáltatások határokon átnyúló szolgáltatásokat is jelentenek egyben, ma már egy-egy ország különálló védelme sem stratégiai, sem technikai szinten nem elégséges. Olyan átfogó, akár globális védelmi megoldásokra és stratégiákra van szükség, amelyek ha nem is 100%-osan, de a lehető legmagasabb szinten garantálják ezeknek a rendszereknek a biztonságát, függetlenül attól, hogy fizikailag melyik országban helyezkednek el azok az eszközök, amelyek ezeket a szolgáltatásokat lehetővé teszik.

[26] Kovács (2018b): i. m. 92.
[27] Kovács (2018b): i. m. 92.
[28] Jane Wakefield: One Fastly Customer Triggered Internet Meltdown. *BBC News,* 2021. június 9.

Ugyanakkor szót kell ejtenünk még a digitalizáció egyik legújabb területéről is: a háztartásokról. Az otthonainkba beköltöző digitális technika révén okosotthonokról, angol kifejezéssel élve *smart home*-okról beszélhetünk, amelyek létrejöttét a már említett *Internet of Things*-eszközök robbanásszerű elterjedése tette lehetővé. Mindez azt is jelenti, hogy „[a]z okosotthonok funkcionalitásához természetszerűleg tartozik hozzá a távvezérlés, illetve a távoli elérés és ellenőrizhetőség lehetősége. A különböző mobilalkalmazásokkal egyre nő azoknak az eszközöknek és rendszereknek a száma, amelyek távolról elérhetőek és vezérelhetők. Ráadásul sok gyártó kínál olyan eszközt, amelyek integráló és funkcióelosztó eszközként működnek. Ezek az eszközök a lakáson belül lévő különböző okoseszközökkel kapcsolatba lépnek, és képesek azokat vezérelni."[29]

Az okosotthonokban alkalmazott IoT-eszközök biztonsága azonban nem követte ezek robbanásszerű fejlődését és mindennapi életünkben való elterjedését. A távoli, hálózatos elérés pedig tovább növeli ezeknek a rendszereknek a sérülékenységét. Kiberműveleti és kiberhadviselési szempontból mindezek rendkívül megkönnyítik a célpontok kiválasztását. A sérülékeny IoT-eszközök kompromittálása útján, azokba behatolva nagyon sok információ szerezhető a felhasználók szokásairól, mindennapi tevékenységeiről, és így nem utolsósorban maguk az adott rendszerek is viszonylag egyszerű felszereltséggel és megoldásokkal támadhatókká válnak. Ami még bonyolultabbá teszi a kérdést, hogy ezeken az eszközökön keresztül, ezek felhasználásával további komoly támadások indíthatók – erre jó példa a már említett Dyn DNS-szolgáltató elleni támadássorozat, amely pont az IoT-eszközök kompromittálásával és felhasználásával következett be.

A későbbiekben még elemezni fogjuk, de már ezen a helyen is utalnunk kell arra a tényre, amely közvetett módon a kritikus infrastruktúrákkal, illetve a kritikus információs infrastruktúrákkal kapcsolatos. Ez pedig nem más, mint a beszállítói vagy ellátási lánc (angol megnevezéssel: *supply chain*) biztonsága. A létfontosságú infrastruktúrák már azelőtt a kiberműveletek célpontjai lehetnek, hogy egyáltalán elkészülnének vagy működnének. Azok a számítógépek, hálózatok és rendszerek, de akár az összetettebb szoftverek, amelyeket a későbbiekben a kritikus infrastruktúrák, illetve a kritikus információs infrastruktúrák kialakítása során beépítenek, már a gyártás folyamán olyan előre definiált sérülékenységeket kaphatnak, amelyek később kihasználhatóvá válnak. Ennek megfelelően a kritikus infrastruktúrák rendszereit szállító, tervező,

[29] Kovács (2018b): i. m. 114.

kivitelező és összeszerelő vállalatok esetében is fontos a teljes körű biztonság megteremtése és folyamatos fenntartása. Az úgynevezett kommersz vagy polcról levehető (angol megnevezéssel *commercial off-the-shelves,* COTS) termékek felhasználása és alkalmazása a fentiekből következően kiemelt figyelmet követel. Az ilyen termékekben meglévő akár szándékosan beépített, de akár nem szándékosan meglévő sérülékenységek azokra a kritikus infrastruktúrákra fognak komoly veszélyt jelenteni, amelyekben ezeket majd alkalmazzák.

Ugyanakkor a teljes ellátási vagy beszállítói lánc biztonságán belül kiemelt szerepet kap a digitális technológia biztonsága. Így a digitális ellátási lánc biztonsága az információtechnológiai rendszerek, ezen belül például a szoftverek, hardverek és hálózati elemek kiberbiztonsági követelményeit egységesen kezelve fókuszál az olyan fenyegetések kivédésére, mint például a rosszindulatú programok, az adatlopás vagy akár az APT (angol megnevezéssel: *advanced persistent threat*), azaz a folyamatosan fennálló, fejlett technológiákat alkalmazó veszélyek jelentette fenyegetések.

Persze a beszállítói lánc biztonságának megteremtése rendkívül összetett feladat, hiszen maga a beszállítói lánc számos szervezetet, tevékenységet, információt, erőforrást, illetve szakembert foglal magában. A beszállítói lánc minden eleme közreműködik a termékek és/vagy szolgáltatások előállításában vagy létrejöttében, olyan komplex rendszert alkotva, amely gyakran nehezen átlátható, amihez hozzájönnek még az esetlegesen földrajzilag is elkülönült helyeken, eltérő biztonságfelfogással létrejövő részegységek vagy résztermékek. Ugyanakkor mindezek biztonsági szempontból történő egységes kezelése elengedhetetlen, hiszen ebben a komplex rendszerben számtalan helyen ott van az információtechnológia, illetve a kibertér. A beszállítói lánc egyes számítógépeinek vagy számítógép-hálózatainak sérülékenysége az azokat kihasználó rosszindulatú tevékenységek révén hatalmas kockázatot jelent a teljes ellátási lánc egészére nézve.

Mindezek szintén rávilágítanak arra, hogy a kiberhadviselés nem egy elvont kérdés, amely csak a hadseregeket érintené, hanem ennél nagyságrendekkel nagyobb problémát – más olvasatban lehetőséget – jelent, hiszen a társadalom minden rétegét és minden funkcióját átszövő digitalizáció miatt a mindennapjaink részévé válik.

1.1.3. Digitális hadsereg

A digitalizáció megjelenése a hadseregekben sem új keletű. A hadseregek a vezetés és irányítás – angolul *command and control* (C2) – különböző funkcióinak támogatására már közel három évtizede alkalmazzák a digitális technológiát. Ez a legelső időkben, azaz az 1990-es években a digitális technika megjelenésével, annak elsősorban kommunikációs célokra történő alkalmazását jelentette. Ugyanakkor már az 1990-es évek legelején megjelent a digitalizáció az olyan katonai területeken is, mint a navigáció, hiszen az első Öböl-háborúban, 1991-ben debütált éles körülmények között az a globális műholdas navigációs rendszer, amelyet egyébként ma már civil navigációs rendszerként is használunk nap mint nap. Ezzel egy időben jelent meg a saját erők követését lehetővé tevő rendszerek első változata, és ekkor kezdődött egyre szélesebb körben a digitális felderítő rendszerek alkalmazása is.

Ez a digitalizáció ma már nemcsak stratégiai szinten, hanem a legfelsőbb szinttől egészen az egyes katonáig a digitális eszközök összekapcsolását és hálózatba szervezését is jelenti. Az egyes katona vonatkozásában egyre inkább digitális katonáról beszélünk, akinek az egyéni felszerelésében olyan infokommunikációs eszközök találhatók, amelyek korábban egészen elképzelhetetlenek voltak. Ezek az eszközök bekapcsolják a katonát abba az egységes hálózatba – vagy különálló hálózatok egységes rendszerébe –, amelyek révén nemcsak az információáramlás gyorsul fel, hanem a döntéshozatal mechanizmusa is. Ráadásul így a valós időben rendelkezésre álló, reális döntéstámogató információknak köszönhetően sokkal pontosabb és relevánsabb lesz maga a döntés. A katonán elhelyezett digitális eszközök közül csak néhányat említünk: a katona sisakján vagy fegyverén rögzített infra- vagy nappali videókamera, de akár a széles sávú adatátvitelt lehetővé tevő rádióján keresztül a digitális térkép, illetve domborzati modell megjelenítését lehetővé tevő, alapvetően kisméretű számítógép ma már mind-mind az egyes katona alapvető felszereléséhez tartozik.

A hálózatos kialakítás 2000-es évek elején kezdődött nagyarányú fejlesztése miatt akkor hálózatos vagy hálózatalapú hadviselésről beszéltünk, hiszen a végrehajtó, azaz a fegyvert kezelő állománytól egészen a döntéshozó tábornokig egy egységes hálózatban kellett és lehetett elképzelni a különböző műveletek végrehajtását.

Ugyanakkor ezek a digitális infokommunikációs eszközök nemcsak előnyt, hanem – a civil rendszerekhez hasonlóan – sérülékenységeik révén komoly veszélyt is hordoznak magukban. A kiberhadviselés egyik célja pedig pont

az, hogy ezeket az infokommunikációs rendszereket támadja, azokból információkat szerezzen, vagy azok működését akadályozza, illetve szükség esetén ellehetetlenítse.

Ma a korszerű digitális hadseregek robusztus digitális architektúrára, digitális kommunikációs és számítógép-hálózatokra épülnek. Ugyanakkor a hadsereg működőképessége csak akkor biztosítható, ha a különböző hálózatok és digitális eszközök képesek egymással együttműködni. Ez nagyon komoly interoperabilitási feladatot jelent, amely a hadseregek analóg rendszerekről digitális vezetési és irányítás, illetve fegyverirányítási rendszerekre történő átállásától kezdve, azaz az 1990-es évek második felétől kezdődően a mai napig komoly kihívás elé állítja nemcsak a mérnököket, hanem a rendszerek felhasználóit is.

A hadseregekben végbement digitalizáció egyik legfontosabb előnye a vezetés és irányítás hatékonyabbá tétele mellett az, hogy ennek hatására egy ellenálló, gyorsan reagálni képes, megfelelő információkkal a legalacsonyabb szinttől a legmagasabb szintig rendelkező, ütőképes haderő jön létre. Természetszerűleg ezeknek az infokommunikációs eszközöknek és számítógép-hálózatoknak az alkalmazására fel kell készíteni a katonákat, megismertetve velük azok biztonságos használatának szabályait. A harcmező digitálissá válik, ami azt is jelenti, hogy számos számítógép-hálózat, infokommunikációs, illetve elektronikai eszköz egymással való párhuzamos működésével kell számolni, így ezeknek a biztonsága kiemelt fontosságú. A digitális eszközök alkalmazása gyakran felveti azt a kérdést, hogy a 21. század katonájának csak ezeknek vagy az olyan hagyományos eszközöknek és eljárásoknak a használatát is ismernie kell-e, mint például a papíralapú térképek és az ezek segítségével való tájékozódás, navigáció, vagy éppen ezek alapján a pontos tűzcsapások vezetése. Az igazság nyilvánvalóan a két gondolatiság között van, azaz a digitális technika és technológia készségszintű ismerete és alkalmazása mellett bizonyos szinten a hagyományos eljárások és megoldások ismeretére is szükség van a jövőben is.

Természetesen a digitális hadsereg kialakítása hatalmas tudományos és katonaszakmai vitákat generált. E diszkussziók során olyan alapvető – nem csak technikai és technológiai – kérdésekre kellett választ adni, mint hogy egyszerre cseréljük-e le a régi, hagyományos, analóg technikai eszközöket új, digitális eszközökre, vagy a régi és az új rendszerek és eszközök egymás melletti, egymással párhuzamos működtetését biztosítsuk-e inkább. Egy másik nagyon nehéz kérdés az, hogy ha a régi technológiát le is cseréljük újra, az folyamatos, ráadásul gyors ütemű fejlesztést is igényel. Ez a fejlesztés, illetve a fejlesztési lehetőség már integrálva kell hogy megjelenjen az új technikai eszközökben, hiszen azok

teljes cseréje – legalábbis olyan rövid időintervallumban, ahogy azt a civil rendszereknél megszoktuk – a hadseregekben gazdaságilag nem lehetséges. Így meg kell teremteni annak a lehetőségét, hogy bizonyos fokú szoftveres fejlesztés az alaphardverekben, azaz platformokon vagy hordozóeszközökön – legyenek azok nehéz-haditechnikai eszközök vagy akár repülő eszközök – elvégezhető legyen.

Egy másik, nem egyértelműen csak pozitív hozadékkal járó, hanem nagyon komoly biztonsági aggályokat felvető kérdés az olyan új technológiák megjelenése, mint a mesterséges intelligencia. Mielőtt ezt nagyon röviden elemeznénk, célszerű a mesterséges intelligencia, illetve annak kibertérben való – akár támadó, akár védelmi jellegű – felhasználásának bemutatása. A mesterséges intelligencia, röviden MI (avagy angol megnevezéssel *artificial intelligence,* AI) rohamléptekben fejlődik, és azonnal be is épül a mindennapjainkban használt technikai eszközökbe és szolgáltatásokba. A mesterséges intelligencia ma már ott van a mobilkommunikációs eszközeinktől kezdve az okosotthonainkig az életünk számos területén. Bár nincs egységesen elfogadott meghatározása, definíciószerűen megfogalmazva az MI alapvetően szoftveres úton létrejövő intelligenciát jelent, amely képes lehet emberi beavatkozás nélkül reagálni a változó környezetre, a természetes intelligenciához hasonló módon a problémamegoldásra, valamint a tanulásra. Ez azt is jelenti, hogy az MI át is alakítja a világunkat, hiszen számos olyan helyen nyer teret, ahol eddig csak az emberi – intelligens – interakció és feladat-végrehajtás volt lehetséges. Talán az önvezető járművek és az iparban a robotika[30] a legjobb példák erre,[31] de ott van az egészségügyben, valamint a kibervédelemben is. Az MI a nagy mennyiségű adatok gyors és intelligens feldolgozásával a jövő kibervédelmi megoldásainak egyik pillérét fogja képezni. A megszokottól eltérő hálózati forgalom vagy akár a szokatlan felhasználói aktivitás ma már valós időben is kiszűrhető MI-megoldásokkal, sőt egyes esetekben ennek segítségével olyan előrejelzések is készíthetők, amelyek a kibertámadások bekövetkezését képesek prognosztizálni. Ezt erősíti a brit Nemzeti Kiberbiztonsági Központ egyik kiadványa: „Ha nagy léptékben szeret-

[30] Ma már az ipar 4.0 kifejezés írja le talán a legjobban az ipari vagy termelési folyamatoknak azt a futurisztikus együttesét, amelyben az egyes eszközök vagy rendszerek – legyenek azok a gyártásban vagy a szállításban, anyagmozgatásban valamely munkafázist ellátók – önállóan kommunikálnak egymással, sőt a kommunikáció mellett részben vagy teljesen önálló döntéseket hoznak, majd azokat a fizikai térben végre is hajtják.

[31] NIST: *Artificial Intelligence* (2022).

nénk automatizálni a kiberbiztonsági feladatokat, akkor az emberi képességeket meghaladó mennyiségben kell feldolgoznunk az adatokat. Ehhez számos eszköz áll rendelkezésünkre, például antivírusszoftverek és tűzfalak. A közelmúltig azonban ezek manuálisan fejlesztett szabályokon alapulva működtek. Mostanra az eszközök egyre inkább saját maguk tanulják meg a szabályokat, és intelligens algoritmusokat használnak arra, hogy ezeket a szabályokat közvetlenül az adatainkból származtassák. Ezek az új szabályok nagyon erőssé tehetik az eszközt, ugyanakkor kevésbé kiszámíthatóvá is teszik őket."[32]

A fentiekkel összhangban azt is figyelembe kell vennünk, hogy önmagában az MI valamilyen eszközbe vagy szolgáltatásba történő beépítése, illetve alkalmazása is jelenthet potenciális támadási célpontot. Erre utal az Európai Biztonsági Tanulmányok Központjának (Centre for European Policy Studies, CEPS) egyik tanulmánya: „Ahogy az MI-alapú rendszerek egyre általánosabbakká válnak, az ellenfelek ösztönzést kapnak arra, hogy megtanulják, hogyan támadják meg őket. A versenyképesség megőrzése érdekében a vállalatok vagy szervezetek veszélyesen figyelmen kívül hagyhatják a biztonsági kérdéseket, kisebbítik a már azonosított kockázatokat, vagy felhagynak a robusztussági irányelvekkel, hogy kitágítsák munkájuk határait, vagy hogy egy terméket a versenytársak előtt leszállítsanak."[33] Mindezek mellett, ahogy azt az IoT-eszközöknél is látjuk, a hatalmas és kiélezett piaci verseny, azaz a termékek kifejlesztése után a lehető leggyorsabb piacra dobás elve nagy kockázattal jár az MI esetében is. A fenti tanulmány is utal erre a negatív trendre: „Ez a gyenge minőség és gyors piacra kerülés irányába ható tendencia már uralkodóvá vált a »dolgok internete« iparágában, és a legtöbb kiberbiztonsági szakember rendkívül problematikusnak tartja. Hasonló meggondolatlanság a mesterséges intelligencia területén is ugyanilyen negatív következményekkel járhat. Ennek megfelelően az MI-kutatóknak és -mérnököknek tisztában kell lenniük azzal, hogy milyen jellegű etikai kérdések merülhetnek fel a munkájuk során, s hogy ezekre milyen választ kell adniuk."[34]

Visszatérve a hadviselés vonalára, a mesterséges intelligencia kontroll nélküli beépítése és felhasználása haditechnikai eszközökben – főleg a fegyverrendszerekben – számos esetben szintén komoly etikai kérdéseket vet fel. Ezek a kérdések

[32] National Cyber Security Centre: *Defining Artificial Intelligence* (2019. április 18.).

[33] Lorenzo Pupillo – Afonzo Ferreira – Stefano Fantin: *Artificial Intelligence and Cybersecurity.* Brussels, CEPS, 2020. 7.

[34] Pupillo–Ferreira–Fantin (2020): i. m. 7.

alapvetően az önálló döntéshozatallal kapcsolatban és elsősorban az emberi élet kioltására alkalmas fegyverek esetében jelentkeznek. A legfontosabb kérdés az, hogy rábízhatjuk-e egy fegyverrendszert kezelő mesterséges intelligenciára annak eldöntését, hogy adott esetben emberi életet, életeket oltson ki. Emellett nagyon komoly vitaalap ezen rendszerek biztonságának, elsősorban kiberbiztonságának a kérdése is, hiszen a távoli elérésű, mesterséges intelligencia által vezérelt fegyverekhez való illetéktelen hozzáférés lehetőségét nem lehet kizárni, ami így komoly kockázatot jelenthet az egyébként esetleg megbízható döntéshozatali mechanizmussal rendelkező, mesterséges intelligencia által irányított fegyverrendszerek esetében is.

A hadseregek digitalizációja a katonai információs rendszerek fejlődésén mérhető talán a leginkább. Ezek angol terminológiával élve a C4ISR-rendszerek, amely a benne szereplő négy „C" – *command, control, communications, computers* (azaz vezetés, irányítás, kommunikáció, számítógépek) –, valamint az *intelligence, surveillance, reconnaissance* (azaz hírszerzés, megfigyelés, felderítés) angol szavak kezdőbetűiből alkotott mozaikszó.

Ezekben a számítógépekre, számítógép-hálózatokra alapozott információs és vezetés-irányítási rendszerekben megjelennek a különböző felderítési szintek (stratégiai, hadműveleti, harcászati) feldolgozott és értékelt adatai, információi, valamint a különböző vezetési szintek jelentései, parancsai. Ezeknek a C4ISR-rendszereknek, amelyek a NATO terminológiájában a CIS (*communication and information systems,* kommunikációs és információs rendszerek) nevet viselik, legfontosabb funkciója a vezetéshez szükséges információ automatizált összegyűjtése, feldolgozása és a felhasználóhoz való eljuttatása. Ebben a munkában a digitális technológia megjelenése hatalmas lökést adott a C4ISR-rendszereknek, amelyek ma a katonai vezetés-irányítás technikai gerincét képezik. Ezek a rendszerek kapcsolják össze a végrehajtó elemeket, legyen szó egy lövész katonáról vagy akár egy harckocsiról, illetve az adott műveletet vezető parancsnokot. A fő funkció végrehajtása érdekében értelemszerűen a katonánál meg kell hogy jelenjenek azok az eszközök, amelyek egyrészt a felderítést, információszerzést (természetesen az adott szintnek megfelelően), másrészt az információk előzetes feldolgozását és esetleges megjelenítését, valamint továbbítását teszik lehetővé. Ugyanakkor a C4ISR-rendszerek nem statikusak, mert a vezetési szinttől függően gyorsan mobilizálhatóknak vagy akár átalakíthatóknak kell lenniük. Így alapvetően nemcsak statikus beépített állomásokból és eszközökből épülnek fel, hanem a terepen a végrehajtó alegységekkel közösen mozogva, sokszor azok technikai eszközeibe

integrálva jelennek meg, és a feladattól függően akár hardveresen, akár szoftveresen dinamikusan átkonfigurálhatók.

Meg kell jegyzeni, hogy ma már az egyszerűnek tűnő rádiók is nagyon gyakran számítógépek. Ezért is hívják ezeket az eszközöket szoftverrádióknak, angol megnevezéssel élve SDR- *(software defined radio)* technológián alapuló eszközöknek. Ezekben az SDR-rádiókban az azt kezelő beavatkozása nélkül, adott esetben az előre meghatározott üzemmódok, frekvencia és akár modulációs mód alapján a szoftvervezérlés dönti el, hogy a jelátvitel, azaz a kommunikáció módjai közül – legyen szó hang vagy adatátvitelről – melyik a leghatékonyabb. Ez a megoldás a mesterséges vagy természetes – az átvitelt nehezítő vagy akár lehetetlenné tevő – zajforrások ellenére biztosítja a lehető leghatékonyabb működést.[35]

Visszatérve a katonai információs rendszerekre, azt ma már nyugodtan kijelenthetjük, hogy a katonai harcászati számítógép-hálózatokban a korszerű harckocsik, páncélozott szállító járművek vagy akár a tüzérségi eszközök is számítógép-hálózatok végpontjait jelentik. Az adatok és az információk feldolgozását automatikus számítóközpontok végzik, és ezek mellett a különböző szintű vezetési pontok különböző munkaállomásai is megjelennek. A C4ISR legfontosabb funkciója tehát, hogy összekapcsolja a végrehajtót *(shooter)* és azt a parancsnokot *(commander),* aki a végrehajtó számára a feladatokat szabja, illetve az adott műveletet vezeti.

A C4ISR-rendszerek egyik alappillére a felderítés. A katonai felderítés, ahogy a fentiekben említettük, a katonai tevékenységek minden szintjén, tehát a stratégiai, a hadműveleti és a harcászati szinten egyaránt jelen van. Ugyanakkor a technológia változása miatt egyre korszerűbb és egyre inkább digitális eszközök szükségesek a felderítés elvégzéséhez is. Ma azonban már nem elsősorban az információk megszerzése, hanem az információk és adatok feldolgozása a legnagyobb kihívás. Ez azért jelent nehézséget, mert ahogy a civil rendszerek esetében már láthattuk, rendkívül sok és változatos formátumú információ áll rendelkezésre. Ebből a releváns, döntéstámogató információ lehető legrövidebb időn belüli kiválasztása és ezek összegzése, majd belőlük minőségében új felderítési információ előállítása a legfontosabb feladat. Az elérhető legtöbb forrás felhasználásával végzett felderítést összadatforrású felderítésnek hívjuk, amely

[35] Ványa László: Út a szoftverrádiók és szoftverrádió-zavaró állomások felé. In Rajnai Zoltán (szerk.): *Kommunikáció – Communications, 2006.* Konferenciakötet. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2006. 76.

a fentiekben említett rendkívül sok és nagy mennyiségű információ rendelkezésre állása miatt nem képzelhető el, csak számítógépes adatfeldolgozással. Definícószerűen megfogalmazva „az összadatforrású felderítés különböző fajtájú, önálló felderítő rendszereket, valamint változást érzékelő adatgyűjtő szenzorrendszereket integrál magába. Feladata, hogy az ellenségről és a hadszíntéri környezet változásairól minden lényeges és fontos adatot, információt időben összegyűjtsön, és az illetékesek számára átadja. Az összadatforrású felderítő rendszer tehát fontos információátalakítási műveletet végez, vagyis a nyers adatokból és a nyers információkból felhasználható információkat hoz létre. Működése azon az elven alapszik, hogy a különböző felderítő és adatgyűjtő rendszerektől folyamatosan érkező részadatokat, paramétereket idő, hely és fontosság szerint rendezi, adott célobjektumokra összegyűjti. Ezt a folyamatot adat- és információösszeolvasztásnak, idegen kifejezéssel adat- és információfúziónak nevezik."[36]

Ez utóbbi példán is jól látszik, hogy a számítógépek, a számítógép-hálózatok és maga az információtechnológia átalakította, illetve folyamatosan átalakítja a hadviselést. A hálózatok miatt így akár hálózatközpontú hadviselésnek is hívhatjuk napjaink hadviselését. A hálózatközpontú hadviselés – angol megnevezéssel *network-centric warfare* (NCW) – lehetővé teszi az egy időben több helyen történő feladat végrehajtását, illetve ezen műveletek egyidejű vezetését. A digitális technológia azt is lehetővé teszi tehát, hogy a parancsnok olyan helyzetkép – ismét csak angol terminológiával élve: *situational awareness* (SA) – birtokában legyen, amely alapján reális döntéseket tud hozni, továbbá hogy ezek a döntések a lehető legrövidebb időn belül el is jussanak a végrehajtókig. A folyamat itt nem ér véget, hiszen a parancsnok a hálózatokon visszakapott információk alapján látja a feladat-végrehajtás eredményét, annak következményeit, illetve hatásait, és ennek megfelelően akár menet közben be tud avatkozni egy-egy műveletbe. Mindezek oda vezetnek, hogy információs fölény jön vagy jöhet létre, amely nagymértékben az információtechnológiára alapozott vezetésnek köszönhető. Ezzel látszólag el is jutottunk az információs műveletekhez, amelyekről a későbbiekben még többször és több kontextusban is szót ejtünk, sőt röviden elemezzük is ezek szerepét a mai hadviselésben, elsősorban annak kiberhadviseléssel kapcsolatos vetületeit.

[36] Haig Zsolt et al.: *Felderítési és zavarási technikák vizsgálata. Tanulmány a Jedlik Ányos Program – 2. alprogram: Versenyképes Ipar NKFP_07_2-HT28_SAJ program keretében kidolgozásra tervezett integrált elektronikai felderítő és zavaró rendszerhez.* Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2008. 35.

A digitális technológia lehetővé teszi a különböző haderőnemek és ezeken belül a különböző fegyvernemek folyamatos és kölcsönös együttműködését, ami korábban számos nehézségbe ütközött. Az ezt biztosító rendszereknek azonban, ahogy korábban utaltunk rá, alapvetően interoperábilisnak kell lenniük, mert csak így lehetséges az említett folyamatos és zökkenőmentes együttműködés.

A katonai feladat-végrehajtás természetesen mást jelent a szárazföldön, és mást a levegőben, ugyanakkor akár a szárazföldi erők, akár a légierő eszközeiben a számítógép-hálózatok, illetve a számítógépek jelenléte ma már természetesnek számít. Ezeken keresztül történik a felderítési információk elosztása, a tűzvezetés, a manővertámogatás, illetve sok esetben a logisztikai ellátás tervezése, szervezése. Ez megfelelő szoftveres támogatást igényel, amely a hálózatokon keresztül elérhető kell hogy legyen.

A digitalizációnak köszönhetően az 1990-es évek közepe óta nagy erőkkel folyik a virtuális valóság (*virtual reality,* VR) beépítése is a katonai tevékenységekbe. Ma már a VR a vezetéstől egészen a kiképzésig, szimulációig számos helyen jelen van a hadseregek életében. A VR, illetve még inkább ennek továbbfejlesztett változata, a kiterjesztett valóság (*augmented reality,* AR) segítségével olyan programok születtek, amelyek a vezetési pontok rendszerét VR- vagy AR-alapon igyekeztek megoldani. Ezek a technológiák azonban a korai szakaszban – az 1990-es években – nem mindig jártak teljes sikerrel, és jelenleg sem találhatók meg széles körben a vezetésben. Ugyanakkor a kiképzésben és a szimulációban a virtuális valóság, illetve annak technikai, technológiai háttere rendkívül jól alkalmazható. Ez költséghatékony megoldást is jelent egyben, hiszen gondoljunk bele: egész alakulatok tevékenységei szimulálhatók számítógépek segítségével anélkül, hogy több tíz vagy akár több száz katonát kellene a terepen mozgatni, nem beszélve mindezen műveletek logisztikai, környezetvédelmi és egyéb fizikai térre is hatást gyakorló kérdéseiről. Ráadásul a virtuális valósággal a szemben álló fél, az időjárás vagy akár a terep minden egyes hatását realisztikusan lehet a katona számára bemutatni úgy, hogy ezt akár fizikai interakcióval is lehet támogatni az említett kiterjesztett valóság technikai megoldásai segítségével.

A virtuális és a kiterjesztett valóság technológiája további hatalmas fejlődés előtt áll a hadseregekben is, hiszen előbb vagy utóbb a vezetés és irányítás területére is meg fognak érkezni azok a ma még futurisztikusnak tűnő megoldások, amelyek az 1990-es években kezdeti szinten a kutatók tervezőasztalán megjelentek 3 dimenziós, a fizikai térrel is interakcióba hozható megvalósítások révén.

Visszatérve a katonai vezetés-irányításra, elmondhatjuk, hogy ennek egyik alapja és nem utolsósorban egyik legfontosabb funkciója a kommunikáció.

A kommunikáció azonban ma már nemcsak hangalapú jelátvitelt jelent a vezetésben, hanem természetszerűleg számítógépes adatátvitelt is. Ennek a kommunikációnak robusztusnak, a változó környezethez való alkalmazkodásra képesnek, azaz adaptívnak kell lennie. Az adaptív (adat)kommunikációs rendszereknek nemcsak a környezet – például a terep – változatosságához kell alkalmazkodnia, hanem az olyan tevékenységekhez is, mint például az elektronikai zavarás vagy akár a kibertámadások jelentette helyzet. Az elektromágneses spektrumban megjelenő elektronikai zavarás esetén a kommunikációs rendszernek fel kell ismernie, majd automatikusan (szoftveres beavatkozással) el kell kerülnie azt. Erre az elkerülésre a frekvenciaváltás, a kisugárzott teljesítmény növelése vagy a modulációs mód automatikus megváltoztatása – például a korábban már említett SDR-technológia révén – nyújthat megoldást. Az elektronikai zavarás mint az elektronikai hadviselés része szintén nem új keletű a hadszíntéren, hiszen „[a]mióta az első komolyabb elektronikai eszköz, nevezetesen a harctéri rádió megjelent a katonai műveletekben, azóta beszélhetünk annak felderítési, lehallgatási, később pedig zavarási igényéről”.[37]

A katonai tevékenységek során a fizikai pusztítás az egyik legmarkánsabb tevékenység, amely elsősorban háborúban jellemző. A fizikai pusztítás azonban, köszönhetően többek között a digitális eszközök nyújtotta valós idejű felderítési információknak, ma már néhány centiméteres vagy néhány méteres pontossággal történhet meg. Ezt a precíziós csapásmérési képességet mind a szárazföldi erők, mind a légierő tűzeszközei számára – legyen szó harckocsiról, helikopterről, merev szárnyú repülőgépről vagy akár pilóta nélküli repülő eszközről – automatizált tűzvezető rendszerek teszik lehetővé. Ezekben a számítógép-vezérlésű tűzvezető rendszerekben integrálva jelenik meg a taktikai, tehát az adott eszközön elhelyezett szenzorból származó, valamint a magasabb vezetési szintről érkező felderítési információ, annak feldolgozási képességével együtt.

Természetesen mind a vezetés-irányítási, mind a tűzvezetési rendszerek működésének nélkülözhetetlen feltétele az a geoinformációs rendszer (*geoinformation system,* GIS), amely digitális térképi és domborzati adatbázissal támogatja őket. A GIS-rendszerek egyik legnagyobb előnye az, hogy használatukkal már szoftveres úton számos olyan tervezési művelet is elvégezhető, mint például a terepen történő vizuális vagy elektromágneses tájékozódás, illetve

[37] Kovács László: Az elektronikai hadviselés jelene és lehetséges jövője. *Hadmérnök,* 12. (2017), 1. 216.

a terepi adatokra alapozva egyéb, például logisztikai számvetések automatikus elkészítése.

A szárazföldi erők harceszközei szintén számítógép-vezérlésűek, amely számítógépek hálózatokba kötve működnek. Ez nemcsak a harcvezetésben és a csapatok műveleteinek koordinációjában, hanem többek között a logisztikában, a javításban és az utánpótlások biztosításában is tetten érhető. Természetszerűleg ehhez integrált vezetési rendszerre van szükség, amelyben az adott harceszköz, például egy harckocsi nemcsak statikus végpont, hanem egy olyan szenzorkészlet, amely a lőszertől kezdve az adott harceszközt kezelő katona fiziológiai állapotán át a szükséges utánpótlásig sokféle adatot továbbít egy központi rendszerbe. Ez a központi rendszer az a vezetés-irányítási rendszer, amely ezeket az információkat összefűzi, korrelálja, majd eljuttatja a döntéshozóig, vagy bizonyos körülmények között akár automatikusan is döntéseket hoz.

Ma egy korszerű harckocsi magában hordozza azokat az előnyöket, amelyeket az I. vagy a II. világháborútól kezdve ezeknél a nehéz-haditechnikai eszközöknél látunk, ugyanakkor technikai felszereltsége ma természetes módon tartalmaz számítógép-vezérelt önvédelmi rendszert, amely természetszerűleg már egy integrált elektronikai rendszer. Ez kiegészül felderítőszenzorokkal, nappali és éjjellátó kamerákkal, műholdas és/vagy rádiónavigációval, sajáterő-követési rendszerrel, illetve tűzvezetési rendszerrel. Ezek a korszerű haditechnikai eszközök moduláris felépítésűek, így könnyen az adott feladatra vagy küldetésre alakíthatók. Az eszköz digitális berendezései a legtöbbször – küldetéstől függetlenül – azonosak. Mindezeket figyelembe véve voltaképpen kijelenthető, hogy ezek az eszközök olyan számítógépek, amelyek több tonna páncéllal vannak körbevéve.[38] Ugyanez igaz a tüzérségre és a tűzvezető rendszerekre is. Ezek a rendszerek integráns részét képezik az említett vezetési rendszereknek, összekapcsolják a tűzeszközöket a szenzorokkal, valamint a döntést meghozó parancsnokokkal.

Rendkívül érdekes megfigyelni – ahogy korábban erről több alkalommal is említést tettünk –, hogy a biztonságpolitikai környezet és a geopolitikai erőviszonyok átalakulásával ezeket korszakonként többé-kevésbé változó módon a hadviselés átalakulása is követi, amelynek során maguk a hadviselés eszközei, így a hadseregek felszerelése és fegyverzete, fegyverrendszerei is változnak. Ugyanakkor a nehézfegyverzet, azaz a nehézpáncélosok vagy akár a tüzérségi eszközök

[38] Rheinmetall: *MBT Revolution: Rheinmetall's Mission-Oriented, Modular Upgrade Package for Main Battle Tanks* (2010. június 14.).

állandó szereplői egy adott ország fegyverarzenáljának. Utóbbiakon belül nagyon pontosan nyomon követhető a változás, hiszen a kinetikus képességek mellett az eszközökben, eszközrendszerekben alkalmazott információtechnológia ma már meghatározó szerepet kap. Napjainkban egy modern harckocsi tucatnyi olyan elektronikai és informatikai berendezést alkalmaz, amelyek értelemszerűen hálózatba vannak kapcsolva, és fő feladatuk a harckocsi túlélőképességének biztosítása mellett a hatékonyság növelése. Ennek megfelelően ma egy harckocsi többek között olyan eszközöket tud felmutatni, mint például az automatizált tűzvezető rendszer, amely kiegészül távolságmérő rendszerrel; az elektronikus toronyfegyverzet-vezérlő rendszer; a harctéri vezetési rendszerkapcsolat a harctéri megjelenítőeszközzel, amelyben a navigációs és a helymeghatározási adatok is megjelennek; a lézerbesugárzásra figyelmeztető rendszer; a vezetőt segítő nappali és infraképet biztosító videórendszer; vagy akár a digitális periszkóp.[39] Ezek a rendszerek akár több számítógépes hálózatba kapcsolva működnek a harckocsi támogatása érdekében, ugyanakkor pont e hálózatok, informatikai és elektronikai rendszerek, illetve a bennük meglévő esetleges sérülékenységek, sebezhetőségek miatt kiemelt feladat a harckocsi kibervédelmének biztosítása. Természetesen az elektronikai eszközök, elsősorban az elektromágneses spektrumban működő aktív, azaz elektromágneses energiát kisugárzó készülékek – például rádiók, adatátvitelt biztosító elektronikai eszközök – vagy passzív eszközök miatt hárul kiemelt szerep az elektronikai védelemre. Ez utóbbi azonban már az elektronikai hadviselés – könyvünk lapjain csak röviden, annak a kibertérrel való kapcsolata mentén bemutatott – kérdéseihez tartozó feladat. Ugyanakkor, ahogy később utalni fogunk még rá, az elektronikai hadviselés és a kiberműveletek vagy a tágabb értelemben vett kiberhadviselés a jövőben egyre több és több azonosságot fog mutatni, köszönhetően annak, hogy az elektromágneses spektrum egyre inkább a kibertér részévé válik.

A légierő mindig is élen járt a technikai, technológiai fejlesztésekben, az új és innovatív megoldások alkalmazásában. Ez a digitalizáció tekintetében is igaz. A repülőeszközök, legyen szó akár merev, akár forgószárnyas repülőgépről, számos elektronikai, illetve informatikai eszközt tartalmaznak. Ezek egy része a repülést segíti, sőt egyes esetekben magát a repülést vezérli a pilóta helyett, másik részük viszont a feladat-végrehajtást – sok esetben a fegyverrendszerek kezelését – végzi, illetve segíti. A repülőgépek fedélzetén lévő – a legtöbb esetben 3-4 vagy még több – számítógép, illetve a repülőgép egyes részrend-

[39] Aselsan: *Next Generation Main Battle Tank Upgrade Solutions* (2022).

szerei, valamint a szenzorok és a fegyverek közötti összeköttetés ma már számítógép-hálózatokon keresztül, sok esetben a civil hálózatoknál is megszokott protokollok segítségével történik.

1. táblázat: A korszerű harckocsi digitális eszközei

Hatékonyságot növelő rendszerek	Túlélőképességet biztosító rendszerek	Szenzorok
– Tűzvezető rendszer, amely magában foglalja a következőket: • tűzvezető számítógép • automatikus célkövető rendszer • elektromos fegyver-/toronymozgató rendszer • fegyver-/toronystabilizálást biztosító rendszer – C4ISR-rendszerkapcsolat – Lézeres távolságmérő rendszer	– Parancsnok panorámás periszkópja – Infrakamera-rendszer – Nappali optikai egység (közvetlen optika és CCD) – Helyzetfelismerő rendszer – Inerciális navigációs rendszer	– Toronymagasság-érzékelő – Toronyazimut-érzékelő – Meteorológiai érzékelők – A fegyver/torony tehetetlenségi mérőegységei – Lőszerhőmérséklet-érzékelő

Forrás: Aselsan (2022): i. m. alapján a szerző szerkesztése

A harcmező egyik legnagyobb kihívása napjainkban a drónok megjelenése, illetve egyre több funkcióra történő alkalmazása. Ezek olyan autonóm eszközök, amelyek ma már nemcsak felderítésre, hanem többek között csapásmérésre is alkalmasak. Naponta jelennek meg újabb és újabb típusú, különböző méretű drónok, amelyek az egyik oldalról a hatékonyságot növelik, a másik oldalról azonban hatalmas biztonsági kihívásként jelentkeznek. A biztonsági kihívást elsősorban az ellenük való védekezés és a védelmi rendszerek, ezek autonóm rendszerekbe szervezése és a vezetési rendszerbe történő integrálása jelenti, hiszen ma már olyan drónrendszerekkel kell felvenni a harcot, amelyek a legtöbb esetben önmagukban is autonóm rendszerek. Esetükben is igaz az, amit korábban már említettünk, hogy az 1990-es évek sokszor kudarcokkal járó útkeresése után a 2000-es évek elejétől megvalósuló, elsősorban az elektronika még nagyobb ütemű miniatürizálódásának, a szenzortechnológia fejlődésének, illetve a számítógépek méretben csökkenő, viszont kapacitásban fejlődő evolúciójának köszönhetően robbanásszerűen terjedtek el az autonóm repülésre és önálló feladat-végrehajtásra képes eszközök.

Ez a fejlődési trend az egyes katona, az egyes harcos technikai felszerelésében is nagyon jól nyomon követhető. Ma a katonát éppen ezért digitális katonának nevezhetjük, hiszen a felszerelése jellemzően digitális eszközökből tevődik össze. Így a digitális katona alapvető felszereléséhez tartozik a nappali és éjjellátó kamera, a navigációs berendezés, a széles sávú adatátvitelre, akár műholdas jelátvitelére is képes rádió, az ellenség-barát felismerő rendszer, és még hosszan folytathatnánk a sort. Természetesen szükség van egy megjelenítőeszközre is – ez lehet tablet vagy kisméretű számítógép –, amely eleve biztosítja az adatátvitel lehetőségét, valamint a kommunikációs megoldásokat, hiszen ezzel az eszközzel kapcsolódik be a katona az említett hálózatba.

A digitális hadsereg a fentiekben bemutatott számos előnye ellenére azonban viszonylag nagy kitettséggel is rendelkezik. Ez a kitettség nem más, mint az a tény, hogy a digitális eszközök vagy rendszerek, legyen szó a katona sisakján elhelyezett kameráról, illetve annak adatátviteli rendszeréről vagy akár a stratégiai szintű döntéshozatalhoz vagy a harcászati vezetéshez szükséges C4ISR-rendszerekről, számos olyan sérülékenységet tartalmaznak, amelyek kibertámadással vagy kibertámadások sorozatával kihasználhatók, így érve el ezen rendszerek részleges vagy teljes, időleges vagy végleges működésképtelenségét.

Ebből következően, ahogy a továbbiakban bemutatjuk, ezek a rendszerek lesznek sok esetben a katonai kiberműveletek elsődleges célpontjai. A későbbiekben utalni fogunk rá, hogy a kiberhadviselésen belüli katonai kibertérműveletek elsődleges célja az információ megszerzése, majd annak felhasználásával olyan beavatkozás, amellyel részlegesen vagy teljesen megakadályozható vagy akár teljesen ellehetetleníthető a szemben álló fél vezetése. A vezetési ciklusba történő beavatkozás nem új keletű, hiszen korábban ezt vezetési hadviselésnek hívták. Maga a vezetési hadviselés mint fogalom kissé elavult, azonban ha végiggondoljuk, akár a kiberhadviselés egyes műveleteinek célpontjait vagy a műveletek vezetési ciklusra gyakorolt hatásait, akkor láthatjuk, hogy valójában ma is megállná a helyét.

1.2. A hadviselés változása az információs korban

Haig és szerzőtársai 2014-ben megjelent *Az infokommunikációs technológia hatása a hadtudományra* című könyvében az IKT-t mint a hadtudományokban megvalósuló innováció fő hajtóerejét jelölték meg. Két tézist fogalmaztak meg munkájukban, amelyek alapvetésként jelen tanulmányt is végigkísérik.

Az első tézis az, hogy az információ a társadalmi fejlődés egyik alappillére. Ennek kezelésében, azaz a megszerzésétől a felhasználásáig tartó folyamatban azonban hosszú és koronként nagyon változatos módszereket láthatunk. Az említett könyv így fogalmaz: „amióta emberi közösségről, fejlettebb szintjein társadalomról beszélhetünk, a mindennapi élet szerves része volt és maradt az információ, az ismeretek elemi vagy összetett szintjén álló tudás, amely a létfenntartástól az elvont és egzakt tudományos gondolkodás legmagasabb szintjéig terjed. Ennek a megszerzése, tárolása, közvetítése a társadalom más egyedei, csoportjai számára az adott korokra jellemzően más és más módszerekkel, technológiákkal történt, de ez a feladatcsoport mindig is létezett."[40] Mindezek arra utalnak, hogy az információ az emberi történelem során mindig is fontos szerepet játszott. Ugyanakkor az emberiség fejlődésében az információ előállítása, feldolgozása és nem utolsósorban tárolása meghatározó, sőt sok esetben korszakokat elválasztó szerepet játszott. A nyomtatás megjelenésével a tudás kialakításához szükséges információk mennyisége és az addiginál sokkal szélesebb társadalmi rétegekhez történő eljuttatása forradalmi változást hozott. Az információtechnológia 20. század közepe óta tartó minden képzeletet felülmúló fejlődése pedig még a nyomtatásnál is nagyobb hatással volt és jelenleg is van az információ áramlására, amely hatalmas mértékben alakította át az emberiség kollektív tudását is. Az információs vagy tudásalapú társadalom kifejezések ma már egyáltalán nem futurisztikusak, hiszen ezek az alapjai a társadalom és végső soron az emberiség fejlődésének a 21. században.

Persze paradox módon ez is hozzájárul ahhoz, hogy a Föld népessége közelít a 8 milliárd főhöz, hiszen a szabad információáramlásra alapozott extenzív tudományfejlődés – bár nem mindenhol és nem egyenlőképpen – nagymértékben növelte az emberek várható élettartamát is. Mindez pedig exponenciális módon járult hozzá a Föld népességének robbanásszerű növekedéséhez a 20. század közepe óta.

Az említett másik tézis a hadviseléssel kapcsolatos: „az emberiség történetét a kezdetek óta végigkíséri a hadakozás. A táplálék megszerzése, a vadászterületek elhódítása, egyes csoportok leigázása, mint cél, mai napig nem sokat változott, csupán a nyersanyagforrásokhoz való hozzájutásnak, az élettér kibő-

[40] Haig Zsolt et al.: *Az infokommunikációs technológia hatása a hadtudományokra.* Budapest, Nemzeti Közszolgálati Egyetem, 2013. 7.

vítésének vagy az agresszív hódítók ellen vívott harcnak nevezzük, de mint oly sok minden, ez is sokszor nézőpont kérdése csupán."[41]

E két gondolat mentén egy-egy főbb tényezőt felvillantva vizsgáljuk meg a hadviselés változását.

Az emberi történelem során a hadviselés változása nagyon sokszor az olyan technikai újdonságok hadszíntéren való megjelenéséhez köthető, mint például a tűzfegyverek, a belsőégésű motor vagy a repülőgép. A tűzfegyverek, azaz a puskák, majd később az ágyúk a szemben álló fél előereje elleni harcot tették hatékonyabbá, olyannyira, hogy a géppuska megjelenése nagyságrendekkel nagyobb pusztítást volt képes végezni, mint a néhány évszázaddal korábban megjelent elöltöltős, nehezen és körülményesen kezelhető puskáké. A belsőégésű motorok harctéren való megjelenése forradalmi változást hozott. Az így hajtott harckocsi megjelenésével maga a hadviselés is komoly változáson ment keresztül, mert a harc megvívásának taktikai elemei is változtak a mobilitás, a hatékonyság és nem utolsósorban a jóval nagyobb tűzerő okán. Emellett az olyan logisztikai feladatokban, mint például a szállítás, szintén forradalmi változást jelentett az új technológia, hiszen ne feledjük, a belsőégésű motorok megjelenéséig a szállítás és az utánpótlás biztosítása volt az egyik legnehezebb feladat a háborúk során.

Ugyanez igaz az információs korra is. A 20. század közepén kezdődött – akkor még információsnak, ma már egyre inkább digitálisnak nevezett – korban a technika és a technológia változása természetszerűleg a hadviselésre is hatással volt. Nem túl meglepő módon azonban ez nemcsak a technikai eszközök harctéren való megjelenését jelenti, hanem magának a hadviselésnek az átalakulását is.

A hadviselés átalakult, de gyökeresen nem változott meg. A cél továbbra is a győzelem megszerzése, a politikai akarat rákényszerítése a szemben álló félre. Ez pedig ma már sokféleképpen elérhető, amibe még sokáig bele fog tartozni természetesen a fizikai erő alkalmazása, azaz a kinetikus katonai műveletek végrehajtása is. Ugyanakkor az eszköztár rendkívüli mértékben bővült azzal, hogy a kibertér globalitása miatt nemcsak hogy nem kell minden esetben fizikai erőt alkalmazni, hanem a kiberműveleteket anélkül is végre lehet hajtani, hogy az adott szemben álló fél földrajzi területére fizikailag bel kellene lépni.

A digitális korszakban a hadviselés egyik legfontosabb változása a fentieknek megfelelően az, hogy míg a történelem során mindeddig jól definiált hadszíntereken vagy csatatereken – még ha azok lakott területeket is érintettek – zajlott a fegyveres küzdelem, addig ma a digitális technikának és a digitális rendszerek

[41] Haig et al. (2013): i. m. 7.

összekapcsoltságának köszönhetően nem lehet a hadszínteret elválasztani a mindennapok társadalmi, gazdasági, kulturális és egyéb tereitől. Pont ez teszi veszélyessé a kiberhadviselést, hiszen így a különböző katonai tevékenységek akár minden állampolgárt érinthetnek. Ráadásul míg a hagyományos hadviselésnek viszonylag jól meghatározott, nemzetközi jogban szabályozott keretei vannak, addig a kiberhadviselés esetén ez koránt sincs így.

A kibertérben folytatott műveletek – amelyeket rövid, összefoglaló néven csak kiberműveleteknek hívunk – és a hagyományos katonai műveletek között az egyik legfontosabb különbség, hogy a hagyományos katonai műveleteket csak háborúban lehet végrehajtani,[42] míg a kiberműveletek már békeidőben is zajlanak.

A digitális technológia hatalmas előnyökkel jár, ugyanakkor számos olyan veszélyforrást is magában hordoz, amelyek eddig soha nem tapasztalt módon jelentkeznek a társadalom egésze vonatkozásában. Ez a veszély a „háború a nappalinkba költözik" gondolattal, illetve kifejezéssel jellemezhető a legjobban, amelyre már fentebb is utaltunk. A globálisan összekapcsolt digitális infrastruktúráknak köszönhetően ma már nemcsak szervezetszerű, úgynevezett reguláris hadseregek, hanem akár egy egyszerű állampolgár is tud kibertámadást indítani valamely fontos infokommunikációs rendszer ellen.

A fentiekben foglaltaknak megfelelően a kiberműveletek jellegüket tekintve legalább kétirányúnak tekinthetők. Az egyik irány a már korábban említett, a hadseregekben megjelenő digitalizáció miatt lehetséges kiberműveletek, hiszen ebben az esetben ezeknek a műveleteknek a fő célpontjai a hadseregekben meglévő információs rendszerek lesznek. A másik irány a civil társadalom digitalizációja révén létrejövő, a civil információs rendszerek ellen irányuló kiberműveletek. Ez az a kettősség tehát, amely talán a legjobban jellemzi a kiberműveleteket.

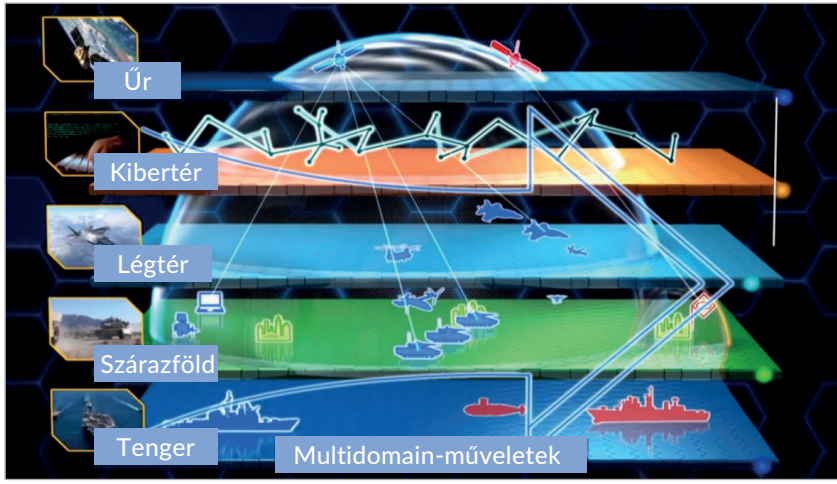
Ugyanakkor ez a kettősség jelenti a kiberműveletekben rejlő legnagyobb kihívást is egyben. Persze a másik oldalról mindezek lehetőséget is jelentenek. Lehetőséget, hiszen anélkül lehet egy másik országra rákényszeríteni akaratun-

[42] Természetesen ennek ellenére léteznek békeidőben végrehajtott – ma már hagyományosnak tekinthető – katonai műveletek, de ezek alapvetően nem a háborús, hanem a békefenntartó, békekikényszerítő műveletek kategóriájába tartoznak. A hagyományos, fegyveres kinetikus műveletektől eltérő békeidős katonai műveletek már sokkal inkább a hibrid műveletek körébe tartoznak. (A hibrid műveletekről, azok összetevőiről, céljairól és módszereiről külön is fogunk szót ejteni jelen könyvünk következő fejezeteiben.)

kat, hogy ott fizikailag meg kellene jelenni, ott fizikai pusztítást kellene okozni, veszélyeztetve ezzel saját katonáink fizikai épségét vagy életét.

A kiberműveletek sorozatát sok esetben kiberhadviselésnek nevezik. A kiberhadviselés mint kifejezés nem hivatalos doktrinális meghatározás, sokkal inkább a média által a különböző kiberműveletek általánosítására használatos. Bár nem hivatalos megnevezésről beszélünk, mégis célszerű lehet ennek alkalmazása, amennyiben a kiberműveletek sorozata eléri azt szintet vagy azok azt a hatást váltják ki, amelyek már a fegyveres küzdelem szintjével azonosíthatók. Mielőtt azonban megvizsgálnánk a kiberhadviselést, azaz a kiberműveletek összességét, nagyon röviden tekintsük át napjaink katonai műveleteinek legjellemzőbb vonásait.

A hadseregek digitalizációja lehetővé tette, hogy a katonai vezetés és irányítás alapjaiban változzon meg. A rendelkezésre álló nagy távolságú kommunikáció révén az addig lineáris, azaz nagyjából egyenes vonalban elhelyezkedő, egyszerre csak egy földrajzi helyen fegyveres küzdelmet megvívni képes egységek és alegységek lehetőségei varázsütésre megváltoztak, kinyíltak. Megvalósult az, ami korábban csak álom volt: egyszerre több helyen, ráadásul több tartományban (más néven domainben) van lehetőség a harcot megvívni. Ez persze nemcsak lehetőség, hanem sok esetben kényszerűség is, hiszen az olyan katonai műveleti területek, mint például Irak vagy Afganisztán, mindezeket kikényszerítették.



1. ábra: A multitérműveletek dimenziói

Forrás: Devon Suits: Futures and Concepts Center Evaluates New Force Structure. *Army.mil,* 2020. április 22. alapján a szerző szerkesztése

Létrejöttek az úgynevezett elosztott műveletek. Ezek a műveletek a több domain miatt úgynevezett multitérműveletekké is váltak egyben. Ezek a multitér- vagy más néven multidomain-műveletek olyannyira új hadviselési formák, hogy meghatározásukra hivatalosan elfogadott definíció még nem született. Ugyanakkor ezeknek a tevékenységeknek a megjelenése alapjaiban változtatta meg a hadviselés elveit. Természetesen nem szabad abba a hibába esnünk, hogy a hagyományos katonai elveket, főleg az erőre vonatkozó elveket félretesszük, és abban a hitben ringatjuk magunkat, hogy a hagyományos katonai erők – a szárazföldi nehéz, közepes és könnyű eszközök, fegyverek vagy akár a légierő eszközei, a harci repülőgépek vagy helikopterek – felett eljárt volna az idő. Ezekre az eszközökre a közeljövőben még ugyanúgy szükség lesz, mint korábban ahhoz, hogy a sikert a harcmezőn ki lehessen vívni és meg is lehessen tartani. Ugyanakkor az olyan új dimenziók, mint a kibertér vagy akár az űr, egyre inkább a hadviselés tereivé válnak, és fokozatosan átveszik a hagyományos dimenziók helyét.

A multitérműveletek kialakulását szintén a digitális technológia, a számítógép-hálózatok és a forradalmian új kommunikációs megoldások tették lehetővé. Ezek nélkül az egymással szinkronizált, összehangolt vagy egymásra ható műveletek egyszerre több helyen történő végrehajtása csak nagyon nagy

energiabefektetéssel és hatékonyságukat tekintve csak jóval alacsonyabb szinten lenne kivitelezhető.

A multitérműveletekben egy időben jelennek meg a szárazföldi erők, a légierő, a különleges rendeltetésű erők, az elektromágneses spektrumban végrehajtott – alapvetően elektronikai hadviselési –, valamint a kibertéri erők műveletei.

Mindezekből kiemelve a kiberműveleteket az világosan látszik, hogy ezek a műveletek a hadviselés minden szintjén, tehát a stratégiai, a hadműveleti és a harcászati szinten is jelentkeznek. Ennek megfelelően a kiberműveleteket integrálni kell a szárazföldi erők, a légierő, de még a különleges rendeltetésű erők művelettervezésébe is. Mindezekkel elérhető a komplex – több dimenzióban egyszerre zajló – művelet-végrehajtás, amelynek célja nem más, mint a szemben álló fél vezetési rendszereinek megbontása, azok működésének akadályozása. Ez műveleti fölényt eredményez a számunkra, ami a sikerhez, azaz a győzelemhez vezető út egyik záloga. Ehhez azonban sok esetben szükség van az információs fölény elérésére is. Az információs fölény nagyon leegyszerűsítve nem jelent mást, mint hogy megfelelő mennyiségű és minőségű információkkal rendelkezünk, amelyek alapján a saját oldali döntéshozatali mechanizmusunk, beleértve az információs rendszereinket is, megfelelő hatékonysággal működik, míg a szemben álló fél döntéshozatala a nem megfelelő vagy a nem megfelelő időben megjelenő és esetenként nem is valós információk miatt lassabb és hatékonyságát tekintve is alacsonyabb szinten működik. Az információs fölény eléréséhez nagymértékben járulhatnak hozzá a kiberműveletek, mivel ezek hatással vannak a szemben álló fél információs rendszereinek működésére (például működésükben akadályozzák azokat) vagy a szemben álló fél kognitív terére (például hamis információk bejuttatásával).

A multitérműveletek egyik legfontosabb eleme az, hogy egy időben több művelet is zajlik, amelyek ráadásul eltérő dimenziókban – ahogy korábban utaltunk rá, például a szárazföldön, a levegőben vagy az elektromágneses spektrumban, illetve a kibertérben –történnek, mégis képesek egymás hatásait támogatni.

Az Amerikai Egyesült Államok hadserege doktrinális központjának, a US Tradocnak 2018-ban megjelent tanulmánya már megfogalmazta a multitérműveletekre való felkészülés szükségességét. E szerint nemcsak az elmúlt évek háborúiból – ahogy korábban mi is utaltunk rá, Irak, Afganisztán, vagy a Balkán fegyveres összecsapásaiból és konfliktusaiból – leszűrhető tapasztalatok vezettek a multitérműveletek körvonalazásához, hanem az a felismerés is, hogy az Egyesült Államoknak olyan versenytársakkal kell szembenéznie, mint Kína vagy Oroszország. Ezek az országok pedig hatalmas ütemben fejlesztik techni-

kai és műveleti képességeiket, amelyek alkalmassá teszik őket egy időben több helyen és több dimenzióban történő katonai műveletek végrehajtására.[43]

Ahogy láthattuk, a multitérműveletek egyik eleme a kibertéri műveletek összessége. Hogy milyen szerepe van ma a hadviselésben a kiberműveleteknek, a későbbiekben a kiberhadviselés elemzésénél részletesen is vizsgálni fogjuk, így ezen a helyen ezt csak nagyon röviden, a hadviselés változásának bemutatása céljából villantjuk fel.

Ahogy korábban bemutattuk, a hadseregekben is megjelenik a digitális technológia, ami – hasonlóan a civil társadalomhoz – számos előnyt, többek között hatékonyságnövelést, gyorsaságot, egyszerűbb vezetést, pontosságot eredményez. Ugyanakkor ennek árnyoldala, illetve veszélyei is vannak, hiszen ezeken a rendszereken keresztül maguk a katonai egységek válnak támadhatóvá. Ez önmagában is komplex kihívást jelent, hiszen nemcsak a vezetés digitalizációjára és az ezáltal megjelenő előnyökre, hanem ezen rendszerek védelmére is fel kell készülni.

A támadás, illetve az ellenfél támadhatósága oldaláról vizsgálva a fentieket, mindez hatalmas lehetőséget teremt a digitalizált hadseregek életében. Új és hatékony támadási lehetőségek tárulnak fel, hiszen a digitalizáció és a digitális technika új és hatékony offenzív képességeket biztosít számukra. Mindez azonban azt is jelenti, hogy a hadseregekben új harcvezetési eljárásokat kell bevezetni, ezeket be kell gyakorolni, és nem utolsósorban hatékonyan alkalmazni is kell őket. Ebben az együttműködés kiemelt fontosságú, amelynek során ma már nemcsak a hadseregeken belüli különböző haderőnemek, illetve fegyvernemek együttműködését kell megteremteni, hanem a hadsereg egyes egységeinek vagy akár az egyes katonának civil szereplőkkel – legyenek azok egyes állampolgárok, vállalatok vagy akár a közigazgaztás valamely entitásai – kell gördülékenyen együttműködnie. Ez hatalmas kihívás elé állítja még a legkorszerűbb és legfelkészültebb hadseregeket is, hiszen számos korábban ismeretlen területen kell egy időben, ugyanakkor akár földrajzilag elkülönült helyen egymással koordinált műveleteket végrehajtani, katonának és civil szakembernek együtt dolgoznva, amely műveletek ráadásul nem csak a fizikai térben zajlanak, és amelyek eredményeit több dimenzióban kell folyamatosan figyelemmel kísérni, illetve értékelni.

A hadviselés változásának bemutatásakor külön kell szólnunk a korábban már említett információs műveletekről. Ezek megítélése és főleg alkalmazása

[43] Tradoc: *The U.S. Army in Multi-Domain Operations 2028*. TRADOC Pamphlet 525-3-1 (2018. december 6.). 9.

nagyon sokat változott az elmúlt 30 évben: az 1990-es évek közepének alapvetően technikai oldalú megközelítése az iraki és az afganisztáni háború hatására a befolyásolás irányába mozdult el. Ugyanakkor a 2010-es évek elejétől kezdődően, főleg a mindennapi média hatására, az „információs" jelző sok esetben olyan, békében is végzett műveletekre is használatos, amelyek célja alapvetően a politikai befolyásolás.

Eredetileg tehát az információs műveletek katonai tevékenységeket jelentettek és jelentenek ma is. Definíciószerűen megfogalmazva – a Magyar Honvédség ez irányú doktrínájának meghatározása alapján – az információs műveletek összessége nem más, mint „az a törzsfunkció, melynek célja, hogy az információs környezet elemzése alapján megtervezze és integrálja, majd értékelje az információs tevékenységeket úgy, hogy azok végrehajtása biztosítsa a kívánt hatás elérését a célközönség akaratában, megértésében és képességeiben a küldetés célkitűzéseinek elérése érdekében. A célközönséget a szemben álló felek, a lehetséges szemben álló felek és más, a politikai szint által jóváhagyott személyek és meghatározott csoportok alkotják."[44] Ebből a meghatározásból azonban jól látszik, hogy az információs műveletek – a mai, alapvetően a különböző médiumok hatására elterjedt vélekedéssel szemben – nemcsak a befolyásolást jelentik, hanem olyan katonai tevékenységek koordinált és szinkronizált alkalmazását, amelyek fő célja az információs fölény kivívása.

Az információs műveleteken belüli katonai tevékenységek nagyon jól kategorizálhatók, hiszen ezekben megtaláljuk az olyan információs műveleti alapelemeket, mint például a már említett kiberműveletek – amelyeket korábbi terminológiával számítógép-hálózati műveleteknek neveztünk –, az elektronikai hadviselés, a lélektani műveletek, a civil-katonai együttműködés, a katonai tájékoztatás, a műveleti biztonság, a katonai megtévesztés vagy az alapelemeket támogató olyan tevékenységek, mint a fizikai pusztítás.

Az elektronikai hadviselés egyre nagyobb konvergenciát mutat a kiberműveletekkel: „az elmúlt évtizedben a számítógépek és számítógép-hálózatok katonai műveletekben való elterjedése, valamint a polgári számítógép-hálózatok célpontként való megjelenése egyre többször és egyre nagyobb átfedést jelent az elektronikai hadviselés, valamint a kibertérben folyó műveletek között".[45] Az elektronikai hadviselés definíciószerűen megfogalmazva nem más, mint „olyan katonai tevékenységek összessége, amelyek az elektromágneses környe-

[44] *Információs műveletek doktrína* (2014). (Ált/57.)

[45] Kovács (2017): i. m. 214.

zetben, az elektromágneses energia tudatos használatával biztosítják az elektromágneses műveletek részeként végrehajtott támadó és védelmi jellegű hatások és célok elérését".[46] Ez közérthetőbb megfogalmazásban azt jelenti, hogy az elektromágneses spektrumot felhasználva beavatkozunk a szemben álló fél elektronikai eszközeibe és rendszereibe, miközben megvédjük saját elektronikai rendszereinket a szemben álló fél hasonló tevékenységétől. Funkcióját tekintve az elektronikai hadviselés három nagy területre osztható fel: elektronikai támogatásra, amely nagy hasonlóságot mutat az elektronikai felderítéssel, az elektronikai ellentevékenységre, amely nem más, mint elektronikai támadás, valamint az elektronikai védelemre.

Az elektronikai hadviselés tehát alapvetően olyan katonai tevékenység, amely a legintenzívebben a háborús műveletekben jelentkezik. Ugyanakkor az elektronikai hadviselés egyes elemei békeidőszakban is nagy hangsúlyt kapnak. Ilyen elektronikai hadviselési feladat például a repülőgépek fedélzeti integrált elektronikai hadviselési rendszerének működtetése, amely komplex módon a fent említett mindhárom funkciót egyszerre ellátja. Emellett békeidőben sok alkalommal van szükség például a mobilkommunikáció (GSM-telefonszolgáltatás) vagy akár a műholdas navigáció zavarására[47] is.

Az elektronikai hadviselés jellemzői tehát egyrészt nagy hasonlóságot mutatnak a kiberműveletekkel, másrészt a kiberműveletek kiegészítésére vagy akár támogatására nagy hatékonysággal alkalmazható az elektronikai hadviselés az olyan informatikai eszközök vagy infokommunikációs rendszerek esetében, amelyek az elektromágneses spektrumot használják például az összeköttetéseik biztosítása érdekében.

[46] Krajnc Zoltán (szerk.): *Hadtudományi lexikon. Új kötet.* Budapest, Dialóg Campus, 2019. 185.

[47] A műholdas rendszerek és így a műholdas navigáció zavarása esetén elsősorban természetesen a vevőegységek, azaz a földi navigációs vevőegység zavarására kell gondolni.

2. fejezet

Kiberműveletek és kiberhadviselés

2.1. Kibertér, szereplők, kihívások, hatások

2.1.1. A kibertérről és annak biztonságáról röviden

A kibertér mint nem is annyira új domain robbanásszerű hatást gyakorolt a hadviselésre, és részben át is alakította azt. Ez önmagában nem új dolog, hiszen a kibertér megjelenése előtt nagyjából 100 évvel a levegő, azaz a légtér hasonlóan új dimenziót jelentett a hadviselésben.

A levegővel mint domainnel történő összehasonlítás nem alaptalan témánk szempontjából, hiszen közel az említett 100 évvel ezelőttig ez a dimenzió nem vagy csak alig játszott szerepet a hadviselésben. De amikor a levegőben megjelentek a katonai célokra is használható eszközök – azaz a léggömbök – mellett már a valódi irányított repülésre is alkalmas gépek, akkor a levegő mint domain a hadviselésben is azonnal fontos szerephez jutott. Analóg módon ugyanez igaz a kibertérre is.

Ugyanakkor míg a levegő mint műveleti tér viszonylag jól meghatározható, határai jól körülírhatók, addig a kibertér esetében ez korántsincs így. Ráadásul a kibertér fogalmára ma még egységesen elfogadott meghatározással sem rendelkezünk. Számos többé-kevésbé jól használható definíció ugyan létezik, de ezek egy része a tartományt, más része viszont magát a környezetet tekinti a fogalom kiindulópontjának, míg megint mások a hálózatok összességeként adják meg a kiberteret.[48]

A levegőhöz hasonlatosan az űr mint új dimenzió szintén analógiák keresésére adhat okot a kibertér és a hadviselés vonatkozásában. Az űr, egészen pontosan a külső űr és a hozzá kapcsolódó nemzetközi jogi kérdéseket vizsgálta, valamint a kibertérrel történő összehasonlítására tett kísérletet egy tanulmányában Nyman-Metcalf, aki így vélekedett: „A kibertérrel való hasonlóság a mögöttes

[48] Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány,* (2018), 1. 115.

üzenet megfogalmazásának módjában van: hogy tudniillik az emberiség valami olyan, teljesen új korszakba lépett, elhagyva a föld korlátait, amely teljesen új jövőt jelent, melyben a nemzeti határok és a földi viták nem játszanak szerepet. A kibertérrel foglalkozók közül sokan valószínűleg most helyeslőleg bólogatnak, hiszen a korai kibertéri vitákban is hasonló nyelvezetet használtak."[49]

Mivel sok megfogalmazást láthatunk a kibertérre, és azok összehasonlítása bár tudományos szempontból rendkívül érdekes, amelyek összehasonlító elemzéséből számos következtetést le is tudunk vonni – például azt, hogy a megfogalmazás megalkotójának nézőpontja határozza meg a definíciót –, mégis érdemes egyet kiválasztanunk közülük annak érdekében, hogy jelen könyvünk témáját, azaz a kiberműveleteket pontosabban megérthessük.

A választott kibertér-meghatározás bár meglehetősen réginek tűnik, hiszen közel egy évtizede, 2013-ban született, egyre inkább bizonyítja időtállóságát. Ez a meghatározás nem más, mint az első hazai nemzeti kiberbiztonsági stratégiában foglaltdefiníció: „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti."[50]

Ez a meghatározás nagyon jól rávilágít arra a tényre, amely akkor sem, és sajnos még ma sem teljesen világos sok esetben, hogy a kibertér puszta technikai szempontú megközelítése nem elégséges, sőt sok kesetben félreviszi annak értelmezését. A fenti meghatározásból viszont jól látszik, hogy a technikai vonal mellett, amely kétségkívül jelen van a kibertérben, a társadalmi és gazdasági folyamatok együttese is kiemelt fontosságú. Ezek a társadalmi és gazdasági folyamatok, amelyeket korábban a digitális társadalom bemutatásánál igyekeztünk körbejárni és megvizsgálni jelen könyv lapjain is, oly mértékben támaszkodnak a kibertérre – ha tetszik, *függenek a kibertértől* –, hogy nem választhatók szét egyértelműen és világosan tőle.

Természetesen vannak olyan kibertér-meghatározások is, amelyek egy adott szervezet vonatkozásában hivatalosnak tekinthetőek. Ilyen a NATO által használt definíció, amely szerint a kibertér az a „globális tartomány, amely magában foglalja mindazon infokommunikációs és egyéb elektronikai rendszereket, hálózatokat és azok adatait – beleértve az elkülönült vagy független

[49] Katrin Nyman-Metcalf: A Legal View on Outer Space and Cyberspace: Similarities and Differences. *The Tallinn Papers,* (2018), 10. 2.

[50] 1139/2013. (III. 21.) Korm. határozat. I. 3.

rendszereket, hálózatokat –, amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak".[51]

A kibertér definíciója mellett a biztonsága is vizsgálódásunk előterébe kell hogy kerüljön, hiszen a kiberbiztonság lesz a támadó kiberműveletekkel szembeni egyik olyan eszközünk, amely megnehezíti vagy akár el is lehetetleníti ezeknek a műveleteknek a végrehajtását, vagy legalábbis csökkenteni tudja hatásukat. Ezért e tekintetben is kell egy jól használható meghatározást keresnünk. Bár a kiberbiztonság esetében is számtalan megfogalmazást találhatunk, a Nemzetközi Telekommunikációs Egyesület (International Telecommunication Unit, ITU) által adott definíció tűnik alkalmasnak számunkra. E szerint a kiberbiztonság „az eszközök, politikák, biztonsági koncepciók, biztonsági garanciák, biztonsági technológiák, irányelvek, kockázatkezelési módszerek, tevékenységek, képzések, valamint a legjobb gyakorlatok összessége, amelyek arra irányulnak, hogy megvédjék a számítógépes környezetet, az ezt használó szervezetek és felhasználók eszközeit, rendszereit".[52]

A hazai 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (röviden csak Ibtv.) korábban még információbiztonság, ma már kiberbiztonság elnevezéssel mutatja be ezt a fogalmat: „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez."[53]

Ha a két definíciót, azaz az ITU-féle és az Ibtv.-ben megjelenített meghatározást összehasonlítjuk, sok hasonlóságot állapíthatunk meg. Az egyik legfontosabb az lehet, hogy mindkét definíció komplex módon tekint az információbiztonság területére, illetve egyre inkább a kiberbiztonság kifejezést alkalmazza.

Mielőtt ezt a komplexitást – amely egyébként a már említett kiberműveletek, illetve a tágabb értelemben vett kiberhadviselés ellen megfelelő eszközöket tud felsorakoztatni – megvizsgálnánk, az információbiztonság alapvető tényezőit kell górcső alá vennünk.

[51] UK Ministry of Defence – NATO: *Allied Joint Doctrine for Cyberspace Operations.* AJP-3.20, „A" kiadás, 1. változat (2020. január). 4.

[52] ITU: *Definition of Cybersecurity* (2021a).

[53] 2013. évi L. törvény 1. § 26.

Ezek a jellemzők az információbiztonság területén már-már klasszikusnak számítanak, hiszen általuk lehet magát az információbiztonságot nemcsak jellemezni, hanem mérhetővé is tenni. Alapvetően három olyan tényezőt sorol fel a szakma ezen a területen, amelyek a legfontosabbak, nevezetesen: a bizalmasságot, a sértetlenséget és a rendelkezésre állást. E fogalmak angol megfelelőinek *(confidentiality, integrity, availability)* kezdőbetűi alapján CIA-elvnek hívjuk az információbiztonság e három alapjellemzőjét.

Ugyanakkor a kiberbiztonság önmagában nem egyenlő az információbiztonsággal, még akkor sem, ha komplex információbiztonságról beszélünk. Szintén alapvetés az információbiztonság területén, hogy maga a biztonság az a megkívánt állapot, amelyet el szeretnénk érni, a védelem pedig azoknak a tevékenységeknek a tudatos és tervszerű végrehajtása, amelyek eredményeként ez a megkívánt állapot, azaz a biztonság létrejön. Ennek megfelelően a kiberbiztonság szélesebb körű tevékenységek sorozatát jelenti, mint az információbiztonság, hiszen számos olyan kérdés is megválaszolást igényel, amely jóval túlmutat az információbiztonság fogalmán. Ilyen például a – más nemzeti szintű stratégiákhoz csatlakozó – nemzeti stratégia megalkotása, azoknak a kereteknek a meghatározása, amelyeken belül már nemcsak az adott szervezet, hanem akár az egész ország kibertéri biztonsága (az ahhoz szükséges feltételek, anyagi, humán és gazdasági erőforrások, képzési felkészítés, kutatás-fejlesztési kapacitások biztosításával) megvalósítható.

Visszatérve a komplex információbiztonságra, erre is számos definíció született az elmúlt években. Hasonlóan a kibertér egyes megfogalmazásaihoz a komplex információbiztonság meghatározása is erősen nézőpontfüggő, azaz az azt megalkotó nézőpontja határozza meg a meghatározás tartalmát. Haig a komplex információbiztonságot annak legfontosabb eleméből és céljából vezette le: „az információs társadalom információbiztonsága szempontjából tehát a fő cél a kritikus információk megóvása."[54]

A megfogalmazáson kívül természetesen maga a tartalom is nagyon fontos. A komplex információbiztonság tartalmi elemeit Haig a következő területeken végzett tevékenységek sorozataként mutatja be: személyi biztonság, fizikai biztonság, adminisztratív biztonság vagy korábbi terminológiával élve dokumentumbiztonság, valamint elektronikus információbiztonság.[55]

[54] Haig Zsolt: *Információ, társadalom, biztonság.* Budapest, NKE Szolgáltató Kft., 2015. 48.
[55] Haig (2015): i. m. 59.

A kibertér jelen van mindennapi életünk minden szegmensében. Az pedig ma már világosan látszik, ami néhány évvel ezelőtt még nem volt ennyire egyértelmű, hogy a kibertér már nem csak az internetet jelenti. Magában foglalja a belső hálózatokat és az infokommunikációs technológia számos elemét, de ahogy korábban bemutattuk, a kritikus infrastruktúrák infokommunikációs elemeit sem szabad figyelmen kívül hagyunk a kibertér értelmezése során. Ugyanez igaz a védelmi szféra, azon belül is például a már szintén említett hadseregek olyan rendszerei esetében is, mint például a fegyverirányítási rendszerek, a vezetés-irányítási rendszerek, vagy akár a nyílt rendszerek mellett a minősített adatkezelő és -továbbító rendszerek. Összességében ma már elmondhatjuk, hogy a kibertér minden olyan elektronikus eszközt és hálózatot is magában foglal, amely vezetékes vagy vezeték nélküli kapcsolattal kapcsolódik egymáshoz. Ebbe értelemszerűen beletartozik az elektromágneses spektrum is, hiszen a vezeték nélküli kapcsolatok révén a kibertér kiterjesztése erre az egyébként fizikai tartományra is szükséges.[56]

Nagyon fontos annak a ténynek a hangsúlyozása, amely ma már trivialitásnak tűnik, de a kiberhadviselés eljárásai szempontjából mégis kiemelt jelentőséggel bír, hogy a kibertér egyes szegmensei, illetve a kiberteret alkotó egyes hálózatok információ- és adatáramlás szempontjából globálisan összekapcsoltak. Ez a globalitás nagyon megnehezíti a kibertér földrajzi helyhez kötését. Természetesen a hálózati elemek, legyenek azok szoftverek vagy hardverek, valahol elhelyezkednek, azaz földrajzilag elméletileg behatárolhatók, de mégis maguk a szolgáltatások vagy a hálózatokon éppen aktuálisan „utazó" adatok esetében ez már nem mondható el. Ráadásul nagyon sok olyan technikai lehetőség létezik, amely akár hardveresen, akár szoftveresen lehetővé teszi az anonimitás biztosítását és így akár a földrajzi behatárolás megakadályozását is a hálózatokon. Mindezek különösen megnehezítik a hadseregek esetében a műveleti területek világos lehatárolását, de ez ugyanúgy igaz többek között a kiberbűnözés elleni fellépés esetében is.

Ugyanakkor mégis szükséges a kibertér szerkezetének, vagy ha tetszik, struktúrájának meghatározása. Ezért a szakirodalom a kiberteret alapvetően három rétegre osztja fel. Ezek a következők: fizikai réteg, logikai réteg, illetve a „kiberszemélyiség" réteg.[57]

E három réteg vizsgálata során az egyszerűsítés és az absztrakció módszerét használjuk annak érdekében, hogy tisztább képünk alakuljon ki magáról

[56] Haig Zsolt – Kovács László – Ványa László: Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata. *Felderítő Szemle,* 10. (2011), 1–2. 195.

[57] AJP-3.20: i. m. 1.9. pont

a kibertérről, hiszen ezzel a képpel felvértezve tudjuk majd meghatározni a kiberhadviselés műveleteinek célpontjait, azok hatásait és eredményeit, illetve a másik oldalról így tudjuk majd az eredményes és hatékony kibervédelmet felépíteni és azt folyamatosan magas szinten tartani.

A kibertér három rétege közül az első a fizikai réteg. Ez a réteg azokból a hardverekből, alapvető hálózati és infokommunikációs infrastruktúrából áll, amelyeket korábban már említettünk. A fizikai réteg tehát nem jelent mást, mint hálózati eszközöket, azaz *switch*eket, *router*eket, számítógépeket, szervereket és munkaállomásokat, adathordozókat, vezetékes és vezeték nélküli adatkapcsolatokat, valamint számos egyéb elemet. Ahogy korábban utaltunk rá, a fizikai rétegben meglévő összes elem földrajzilag valahol elhelyezkedik, így az adott ország jogszabályi környezete vonatkoztatható ezekre az eszközökre. Ez nagyon fontos kérdés lesz majd akkor, amikor egy-egy kibertámadás kiindulópontját, illetve elkövetőjét kell beazonosítani. Ezt a beazonosítást vagy más szóval megszemélyesítést attribúciónak hívják a kibertérben. A kibertér fizikai rétege számos kapcsolattal rendelkezik magával a fizikai térrel is, hiszen az említett hálózati infrastruktúra működési környezete értelemszerűen a fizikai térben van, de ugyanígy a fizikai réteg számos egyéb kapcsolatot tart fent például az elektromágneses spektrummal, akár a vezeték nélküli adatátvitel során, de akár a nem szándékos kisugárzás esetén is. Nem szándékos kisugárzással gyakorlatilag minden elektronikai eszköz, amelyet ez ellen nem védenek, rendelkezik. Így a számítógépek, a monitorok, de még a hálózati eszközök is sugároznak bizonyos szintű elektromágneses energiát a környezetükbe. Ez persze veszélyt is hordoz magában, hiszen így ezek az eszközök, illetve a rajtuk áthaladó vagy éppen feldolgozás alatt lévő adatok kinyerhetők bizonyos távolságból egy viszonylag egyszerű, az elektromágneses spektrumban működő vevőegységgel, és reprodukálhatóvá válnak. A nem szándékos kisugárzás ellen természetesen létezik védelem, többek között az elektromágneses árnyékolás, amely ebben a körben a *Tempest* megnevezést kapta. A problémát ennek műszaki megvalósíthatósága és nem utolsósorban a bekerülési költsége jelenti.

A kibertér következő rétege a logikai réteg, amely már sokkal kevésbé megfogható, mint a fizikai réteg. A logikai réteg az a digitális információs és parancsréteg, amely adatokból és kódokból áll. Idetartoznak a dokumentumok, fájlok, firmware-ek, azaz az adott eszköz működését vezérlő szoftverek, az operációs rendszerek és a programok, illetve az applikációk is.[58]

[58] AJP-3.20. 1.11. pont.

A logikai réteg a fizikai rétegre épül. Jelenleg a logikai réteg működése még nem képzelhető el a fizikai réteg, azaz a hardverek, hálózati eszközök, számítógépek nélkül, hiszen a fizikai réteg közvetíti, azaz szállítja az adatokat, az értelmezi és dolgozza fel azokat, és ott történik azok tárolása is. Ugyanakkor a logikai réteg egyes megvalósulási formái lehetnek mágneses állapotok (erre épült nagyon sokáig az adatrögzítési technológiánk), elektromágneses hullámok, vagy akár kvantumállapotok formái is.

A kibertér harmadik rétege a „kiberszemélyiség" réteg. Az angol terminológiában ezt *cyber phenomen*ának hívják, amely sokkal inkább visszaadja ennek a rétegnek a lényegét, mint a kissé nyakatekert magyar megfelelő. A kiberszemélyiségi réteg nem egy valós személy vagy személyiség, és nem is minden esetben az adott felhasználót jelenti, hiszen sokkal inkább egy digitális identitás formájában van jelen. Ebből következően egyetlen valós felhasználónak több kiberszemélyisége is lehet. A felhasználón kívül kiberszemélyiség lehet például egy e-mail-cím vagy akár egy közösségimédia-profil is, az ahhoz kapcsolható IP- (Internet Protocol) címmel együtt, vagy akár az adott kapcsolat során használt számítógép (tablet, okostelefon, laptop vagy asztali gép) fizikai címe (*Media Access Control,* MAC),[59] egy internet-előfizetés vagy akár egy mobiltelefon SIM-kártyája (*Subscriber Identity Module,* SIM) is. A fentiek azt is jelentik, hogy a kibertérben meglévő kiberszemélyiség nem feltétlenül és nem minden esetben feleltethető meg a fizikai térben meglévő adott személynek vagy személyeknek.

A kiberműveletek szempontjából mind a három kibertéri réteg nagyon fontos. Azonban míg a logikai réteg minden esetben, addig a másik két réteg nem feltétlenül kell hogy részt vegyen egy-egy kiberműveletben. Ugyanakkor a kiberművelet hatása mind a három rétegben jelentkezik. Emellett azt is meg kell jegyeznünk, hogy egy adott kiberművelet nem feltétlenül csak a kibertérben fejti ki hatását, hanem sok esetben azon kívül is. Így a kiberműveleteknek a fizikai térben is lehetnek, sőt az esetek többségében lesznek is hatásai. Itt vissza kell utalnunk a digitalizáció során már említett IoT-eszközökre, amelyek felhasználásával – vagy éppen az ellenük irányuló kibertámadások során – a fő cél, hogy segítségükkel a fizikai térben fejtsünk ki valamilyen hatást. Azaz kapcsoljunk be, le vagy ki valamit, állítsunk át valamit úgy, hogy azzal a fizikai térben gyakorolunk hatást valamire.

[59] Az IP-cím a hálózati eszközhöz hozzárendelt egyedi cím, míg a MAC-cím a hálózati kapcsolatot lehetővé tevő eszköz, azaz a hardver egyedi azonosítója.

2.1.2. Szereplők a kibertérben

A kibertér és biztonsága rövid vizsgálata után szükséges azt is áttekintünk, hogy az átlag, mindennapi felhasználókon kívül kik és milyen céllal használják – persze nem mindig ártatlan és békés szándékkal – a kiberteret. Ebben az áttekintésben ismét az egyszerűsítés és az általánosítás módszerét kell alkalmaznunk, hiszen célunk a kibertéri szereplők főbb kategóriáinak megnevezése, majd ezek legfontosabb jellemzőinek felvázolása.

Az említett általánosítás annak fényében történik, hogy a kibertér már elég jól ismert olyan szereplőit, mint például a hackereket vagy a kiberbűnözőket, nem külön említjük, hanem csoportosítva mutatjuk be őket. Ezek a csoportok a következők: ellenérdekelt szereplők; nem állami szereplők; ellenérdekelt állami szereplők; proxy szereplők; ellenérdekelt nem állami szereplők; ellenérdekelt belsős munkatársak; kiberbűnözők; semleges szereplők.

A kibertér szereplőinek bemutatását a kiberműveletek, illetve a kiberhadviselés szempontjából az egyik legfontosabb csoporttal, az ellenérdekelt szereplőkkel kezdjük. Az ebbe a csoportba tartozók értelemszerűen nem baráti és nem békés célú kiberműveleteket hajtanak végre. Az ellenérdekelt szereplők egyik legfontosabb célja, hogy mind a kiberműveleti, mind a fizikai térben meglévő katonai alakulataink, illetve csapataink mozgás- és cselekvési szabadságát akadályozzák. Egy gyors kitérő arról, hogy mit is jelent a mozgás- és cselekvési szabadság. A katonai terminológiában ez az egyik legfontosabb olyan tényező, amely biztosítja, hogy az adott parancsnok az alárendeltségében lévő katonai erőket, azok képességeit és lehetőségeit akadálytalanul, azok maximális hatékonyságával tudja alkalmazni, mind térben, mind időben. Ennek a mozgás- és cselekvési szabadságnak a fenntartása nemcsak a fizikai térben, hanem a kibertérben is kiemelten fontos, hiszen ez lesz az egyik alapja annak, hogy a képeségeinket a lehető leghatékonyabban tudjuk alkalmazni.

Az ellenérdekelt szereplők tekintetében az egyik legnagyobb veszélyforrás az, hogy mind a kibertérhez, mind az ott alkalmazható legújabb műszaki, technikai megoldásokhoz rendkívül könnyű ma hozzáférni. Ehhez még az is hozzájárul, hogy a számítógép-hálózatokhoz szintén könnyű a hozzáférés és a kapcsolódás, ami így – az említett új technikai és műszaki ismeretek birtokában – komoly lehetőséget biztosít rosszindulatú tevékenység végzésére azok számára is, akik egyébként nem lennének képesek rosszindulatú, illetve támadó kiberműveleteket végrehajtani. Mindezt tetézi az a tény, hogy ezeket a rosszindulatú kiberműveleteket akár globális méretekben is végre lehet hajtani, hiszen a számítógép-hálózatok

összekapcsoltsága, ahogy azt korábban szintén bemutattuk, ezt lehetővé teszi. A kiberhadviselés szempontjából ez a globalitás rendkívül nagy problémát jelent. Később még kitérünk rá, de itt is meg kell említeni, hogy a kibertérben anélkül lehet támadó műveleteket végrehajtani, hogy a támadások mögött álló valós személyek kilétére teljes bizonyossággal fény derülne.

Ugyanakkor főleg az állami csoportok, elsősorban – ahogy a későbbiekben szintén kitérünk rá – a hadseregekben meglévő kiberműveleti erők, illetve az úgynevezett állami támogatású csoportok képesek ezek végrehajtására. Ezzel kapcsolatban fontos megemlíteni a kiberműveletek mögött állók beazonosítását, azaz az attribúció kérdését. Az attribúció az adott kiberművelet mögött álló elkövető(k) nyilvános megnevezését jelenti. Nyilvánvalóan ennek állami, stratégiai szinten van szerepe, hiszen az attribúció elrettentő erővel is bírhat. Ezzel az eszközzel azonban különböző okok miatt nem minden ország él. Az okok változatosak, a technikai bizonyosság 100%-os megvalósulásának a hiányától egészen a politikai és gazdasági okokig.

Természetesen egy-egy támadás után a technikai elemzések nagy biztonsággal megadják a támadó vagy támadók kilétére vonatkozó választ, de ez az esetek bizonyos részében nem jelent 100%-os bizonyosságot. Főleg akkor nem, ha a támadó igyekszik elfedni, álcázni a kilétét, vagy a támadások mögött másokat kíván láttatni. Ma ezek a támadási technikák rendkívül kifinomultak, bár természetszerűleg nem mindenki, illetve nem minden csoport képes olyan támadást vagy támadássorozatot kivitelezni, amely során részben vagy egyáltalán nem deríthető fel a személyazonossága.

Ahogy korábban már utaltunk rá, az attribúció a kibertámadás elkövetőjének beazonosítását, megnevezését jelenti. Ez azonban a fentiek fényében nem mindig egyszerű. Ahogy egy, az Amerikai Egyesült Államok Kongresszusának szóló jelentés is tartalmazza: „A kibertámadások attribúciója nehéz, de nem lehetetlen. A kormányzati nyomozók arra törekszenek, hogy átfogó képet alkossanak a kiberincidensekről, nemcsak az áldozattól, hanem az információk megerősítésével is, annak érdekében, hogy az attribúcióra vonatkozó állításokat megfogalmazhassák."[60]

Vannak olyan országok, mint például az Egyesült Királyság vagy Hollandia, amelyek alkalmazzák az attribúció politikáját, azaz sok esetben megnevezik a kibertámadások mögött álló elkövetőt, legyen szó akár hackercsoportról,

[60] Chris Jaikaran: *Cybersecurity: Selected Cyberattacks, 2012-2021.* Washington (D.C.), Congressional Research Service, 2021.

akár országról. Ugyanakkor az olyan nagy politikai-katonai szervezetek, mint például a NATO, csak nagyon ritkán teszik meg ezt a tagállamokkal szemben elkövetett kiberműveletek esetében. E ritka alkalmak egyike 2021 nyarán volt, amikor a szervezet nagyon diplomatikusan, de azért mindenki számára világos formában nevezte meg az elkövetőt: „Szolidaritást vállalunk mindazokkal, akiket a közelmúltbeli rosszindulatú kibertevékenységek érintettek, beleértve a Microsoft Exchange Server kompromittációját. Az ilyen rosszindulatú kibertevékenységek aláássák a biztonságot, a bizalmat és a stabilitást a kibertérben. Elismerjük szövetségeseink, például Kanada, az Egyesült Királyság és az Egyesült Államok nemzeti nyilatkozatait, amelyek a Microsoft Exchange szerver kompromittálódásért a Kínai Népköztársaságot teszik felelőssé."[61]

Természetesen az olyan nagy kiberbiztonsági vállalatokat, mint például az amerikai Mandiant, nem kötik a NATO-nál érvényben lévő diplomáciai szabályok. Ennek ellenére ezek a vállalatok, bár egy-egy kibertámadás esetén megnevezik az elkövetőt, ezt mégis óvatosan teszik. Így történt ez 2021 végén a Mandiant részéről is, amikor egyes kormányokat és üzleti szervezeteket célba vevő feltételezett orosz tevékenységről számoltak be. A közlemény számos helyen utal a bizonyítékok nem teljes vagy elégtelen voltára, amelyek megnehezítik a beazonosítást. Erre a körülményre a közlemény címében is utalnak a „feltételezett" jelzővel.[62]

A kibertéri szereplők következő csoportja az úgynevezett nem állami szereplők. Ők azok, akik az állami vagy ilyen támogatású csoportok támadási technikáinál általában alacsonyabb szintű, de mégis nagy károkat okozó kiberműveleteket képesek végrehajtani. Ennek a csoportnak az egyik legnagyobb fegyvere az, hogy többnyire alacsony költséggel végzik támadásaikat, mégis feltárják és kihasználják a biztonsági technológia és technika hiányosságait, sérülékenységeit. Ennek a csoportnakrendszerint mind humán kapacitásban, mind anyagiakban korlátozott erőforrások állnak a rendelkezésére, így támadásaik időtartama és volumene elmarad az állami vagy ilyen támogatású csoportok hasonló tevékenységeitől.

[61] NATO: *Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise* (2021. július 19.) 3. pont. (Erről az esetről a könyv későbbi fejezetében még szólunk.)

[62] Luke Jenkins et al.: Suspected Russian Activity Targeting Government and Business Entities Around the Globe. *Mandiant Blog,* 2021.

Ellenérdekelt állami szereplők. Sok állam fejleszti azokat a képességeket, amelyek segítségével előnyre tehet szert a kibertérben. A képességépítés a kibertéri adatforgalom lehallgatásának, elemzésének vagy az abba való beavatkozás képességének a kiépítésével kezdődik, hiszen ezek által lehet megfelelő mennyiségű és minőségű információt összegyűjteni. Ezek a képességek lehetővé teszik az ellenérdekelt állami szereplők számára, hogy hozzáférjenek egy másik ország vagy gazdasági érdekcsoport infokommunikációs rendszereihez, számítógéphálózataihoz. Így az azokban tárolt, feldolgozott vagy továbbított információk révén politikai, gazdasági vagy akár katonai előnyökre tehetnek szert. Természetesen ehhez az is szükséges, hogy megfelelő kibertámadó képességeket is kiépítsenek.

Mindez azt is jelenti, hogy az államok közötti konfliktusok során ez a fajta tevékenység egyre inkább jellemző lesz. Ugyanakkor nyilvánvaló, hogy amennyiben a megtámadott ország felderíti az esetet, az a kibertéren kívüli válaszokat is generálhat. Az állami szereplők kapcsán különösen figyelemre méltó az a tény, hogy gyakorlatilag korlátlan humán és anyagi erőforrásokkal rendelkezhetnek. Emellett már békeidőben lehetőségük van stratégiai szintű tevékenységre, valamint arra, hogy befolyásolják a kibertéri tevékenységeket, az együttműködés vagy a jogi lehetőségek megteremtésével ellenőrizzék az internetszolgáltatókat, akár úgy, hogy az ellenérdekelt ország területén ilyen szolgáltatókban tulajdonjogot szereznek. De szintén lehetőségük van a közösségimédia-platformokat, felhőszolgáltatókat, szoftverfejlesztőket és hardvergyártókat saját érdeküknek megfelelően szabályozni, azokat befolyásolni. Az ellenérdekelt állami szereplők összességében fejlett és összetett, nem utolsósorban pedig nehezen felderíthető kibertérműveleteket vezethetnek.[63] Ezért a kiberműveletek során ezek a csoportok jelentik a legnagyobb kihívást, így a kiberhadviselés vizsgálata során természetszerűleg az állami kiberműveletek kell hogy a legnagyobb prioritást kapják. Ennek megfelelően fogjuk majd könyvünk következő fejezeteiben az ezeket a képességeket építő országokat, illetve képességeiket röviden bemutatni.

A kibertéri szereplők következő csoportja a *proxy*k. Ma már sok ország alkalmaz nem állami, hanem közvetett, megbízott szereplőket a kiberműveletek végrehajtására. Ez főleg abban az esetben előnyös, ha az adott ország nem kíván konfrontálódni sem azzal az ellenérdekelt országgal, amely ellen a kiberműveletet végrehajtja, sem a nemzetközi közösséggel, vagy ha az adott ország jogszabályai, illetve egyéb, például etikai normái hivatalosan nem tennék lehetővé az adott

[63] AJP-3.20. 1.18. pont.

kiberművelet végrehajtását. A proxyk alkalmazása sok közvetett előnnyel is jár, hiszen így nem derül fény az adott ország valós kiberműveleti képességeire, illetve magának a kiberműveletnek a valódi okára is csak közvetett módon lehet következtetni. Más szóval a proxyk alkalmazása megfelelő fedést biztosíthat a megbízónak. Természetszerűleg ha nem is 100%-os bizonyossággal, de megfelelő technikai elemzésekkel a proxyk kiléte többnyire felfedhető. Ilyenek jellemzően az úgynevezett trollhadseregek vagy trollgyárak, amelyek legfőbb célja, hogy az adott állam megbízásából félretájékoztatást vagy zavarkeltést folytassanak. Mindezt úgy teszik, hogy sem az eszközökből (a használt módszerekből[64]), sem az elkövetők személyéből nem lehet egyértelműen következtetni vagy egyértelmű bizonyítékot nyerni a proxy mögött álló országra. A trollgyárak jelenségére és azok dezinformációs kampányokban játszott szerepére a NATO így utal egyik kiadványában:

> „Az internetes kommunikációban troll alatt azt értjük, aki vitákat gerjeszt, például vitatott témák felvetésével vagy más résztvevők támadásával. A trollgyár azonban olyan entitás, amely dezinformációs propagandatevékenységet folytat az interneten. Ezt a tevékenységet gyakran egy nem különösebben feltűnő név alá rejtik, például PR-ügynökség, internetes kutatóközpont stb. A trollgyárak működése általában a politikai vagy a gazdasági szférára összpontosul. A műveletek célja lehet például politikai ellenfelek megtámadása, versengő cég tisztességtelen támadása vagy a megrendelő által kért egyéb tevékenység. A trollgyárak többek között álhírekkel és gyűlöletbeszéddel érik el céljaikat."[65]

Egy másik kibertéri csoport az ellenérdekelt nem állami szereplők csoportja. Ma már számos olyan nem állami kibertéri szereplő van, aki értelemszerűen nem egy adott állam, hanem saját céljai elérése érdekében végzi rosszindulatú kibertéri műveleteit. A nem állami szereplők közé sorolhatók a kiberbűnözői csoportok, a hacktivista (hacker- és aktivistajegyeket egyszerre felvonultató csoportok), valamint a terrorista szervezetek.

A kibertéri szereplők egy másik csoportja – és egyben a kibertér egyáltalán nem elhanyagolható szereplői – az ellenérdekelt belső munkatársak. Az ilyen személyek általában jogszerű hozzáféréssel rendelkeznek az adott információs

[64] A trollhadseregek módszerei nagyon változatosak. Alapvető terep és eszköz a közösségi médiumokon fake news-ok, azaz hamis hírek elhelyezése, zavarkeltés és félretájékoztatás. Ezeket nemcsak emberek, hanem szoftverrobotok vagy a kettő kombinációja, az úgynevezett *cybor*gok végzik akár napi 24 órás tevékenységben.

[65] NATO: *Media – (Dis)Information – Security* (é. n.).

rendszerhez, így olyan tevékenység végzésére is módjuk van, amely veszélyt jelent e rendszerek bizalmasságára, sértetlenségére, illetve rendelkezésre állására. Az általuk képviselt veszélyt nem túlzás komolynak mondani, hiszen egy ilyen belső munkatárs a kiberbiztonság egészére jelent veszélyt. A kiberbiztonsági rendszerek általában külső veszélyek és fenyegetések elhárítására vannak felkészítve. Ezzel szemben az ellenérdekelt belső munkatárs a hálózaton vagy a védelmi rendszeren belülről, sok esetben számos rendszerhez és alrendszerhez való hozzáférés birtokában tevékenykedik, és így tudja elkövetni ártó szándékú cselekményeit.

Külön kibertéri csoportot képeznek a kiberbűnözők. A kibertéri bűnözés nem sokban tér el a fizikai térben megvalósulótól, hiszen az esetek többségében itt is az anyagi haszonszerzés a cél. Ez azonban egy másik dimenzióban, a kibertérben történik, ahol az anonimitás sokkal könnyebben megoldható. Bár a kiberbűnözői tevékenységek alapvetően az említett anyagi haszonszerzés céljából zajlanak, főleg nemzetközi kiberbűnözői vagy állami támogatású csoportok alkalmazása révén elérhetik azt a szintet, amikor már a célország gazdasági rendszerének destabilizálását okozhatják. Ez a kiberhadviselés szempontjából szintén olyan fontos tényező, amelyet szem előtt kell tartani, hiszen látni fogjuk a későbbiekben, hogy a kiberhadviselés eszköztárába nemcsak a katonai tevékenységek, azaz a katonai célpontok elleni kiberműveletek, hanem békeidőben (azaz a mesterségesen a fegyveres konfliktus szintje alatt tartott időszakban) a civil célpontok, így a gazdasági rendszer vagy annak egyes elemei – például bankok, pénzügyi szolgáltatók – elleni kibertámadások is beletartoznak. A kiberbűnözői csoportok kibertéri tevékenységének az anyagi haszonszerzésen túl olyan közvetett céljai, illetve tevékenységüknek olyan közvetett következményei lehetnek, mint a hírnévrontás, a kompromittált adatok nyilvánosságra hozása, de akár közvetlen katonai kockázatot is jelenthetnek a beszerzési eljárásokba vagy az ellátási láncba történő beavatkozásuk során.[66]

Ugyanakkor nem mehetünk el szó nélkül a 2020-ban kezdődött Covid–19-es, biológiai vírushoz kapcsolódó pandémiás helyzet és a kiberbűnözés hirtelen emelkedést mutató trendje mellett. A világjárvány, azaz a pandémiás helyzet, illetve az ezzel együtt járó olyan élethelyzet, mint például az oktatás vagy akár a munkavégzés nagyon gyors áthelyezése az online térbe, már-már természetszerűleg magával hozta azt a negatív következményt, hogy mindezekkel párhuzamosan a kiberbűnözés is magasabb fokozatra kapcsolt. Az Interpol elemzése

[66] AJP-3.20. 1.20. pont.

szerint 2020-ban jelentősen emelkedett az online csalások, a phishing, a zsarolóvírusok, valamint az adatlopások száma. A hirtelen online térbe költöztetett munka és oktatás a legtöbb helyen nem volt felkészülve és felkészítve a biztonságos munkavégzés körülményeinek kialakítására. Az európai országok kétharmada jelentett olyan rosszindulatú tevékenységekre utaló jeleket, amelyek a felhasználókat a Covid vagy korona kifejezésekkel kapcsolatos online kereséseik eredményeként csaló vagy adathalász oldalakra irányította. Az Interpolhoz beérkezett adatok szerint a Coviddal összefüggő kiberbűncselekmények és kibertéri veszélyek 14%-a hamis hírekkel, 22%-a káros tartalmakat tartalmazó domainekkel, 36%-a rosszindulatú programokkal és zsarolóvírusokkal, 59%-a pedig adathalász-tevékenységekkel függött össze.[67]

A Covid előtti időszakban a Világgazdasági Fórum egyik összeállítása szerint hazánk kiberbűnözés szempontjából 2019-ben kifejezetten jó helyen szerepelt az európai országok összehasonlításában, hiszen csak a számítógépek 4,83%-a volt érintett kiberbűnözői tevékenységben. Összehasonlításként ez az arány Franciaországban 5,41%, míg Bulgáriában 17,55% volt.[68]

A kibertéri szereplők felsorolásából nem hiányozhatnak a semleges szereplők sem. Ők azok, akik nem vesznek részt az adott kiberműveletben, de azonosításuk és így elkülönítésük is a többi szereplőtől rendkívül nehéz és körülményes. A semleges szereplők elkülönítésére egyrészt azért van szükség, hogy a kiberműveletek során az olyan hatásokat, amelyek a semleges szereplőket érintenék, el lehessen kerülni, másrészt pedig az ellenérdekelt vagy szemben álló fél ne tudja őket felhasználni a kibertéri konfliktusban.

Az ENISA 2020-as és 2021-es évet érintő vizsgálata szerint a kibertéri szereplők között azok veszélyességét figyelembe véve a következő sorrend állítható fel: 1. államilag támogatott szereplők, 2. a kiberbűnözés szereplői, 3. hackerek és bérelt hackercsoportok, 4. hacktivisták.[69]

[67] Interpol: *Cybercrime: Covid-19 Impact.* Lyon, Interpol General Secretriat, 2020.

[68] Dmitry Samartsev: *Cybercrime Is Maturing. Here Are 6 Ways Organizations Can Keep Up.* (H. n.), World Economic Forum, 2020.

[69] European Union Agency for Cybersecurity: *ENISA Threat Landscape 2021. April 2020 to Mid-July 2021* (2021a. október). 4.

2. táblázat: A kibertéri szereplők és jellemzőik

Szereplők és jellemzőik	Jellemzők	Kiberműveleti jelentőségük
Ellenérdekelt szereplők	– jelentős erőforrások – információszerzés – kibertéri mozgás- és cselekvési szabadság akadályozása – károkozás – dezinformáció	nagy
Nem állami szereplők	– közepes erőforrások – károkozás	nagy/közepes
Ellenérdekelt állami szereplők	– jelentős erőforrások – nagy intenzitású, kiterjedt kiber-műveletek indítása és fenntartása – szervezettség – állami akarat és célok érvényesítése – információszerzés – kibertéri mozgás- és cselekvési szabadság akadályozása – károkozás – dezinformáció	nagy
Proxy szereplők	– felelősség elrejtése, hárítása – rejtett célok	nagy/közepes
Ellenérdekelt nem állami szereplők	– rosszindulatú, ártó szándékú tevékenység – korlátozott erőforrások	közepes
Ellenérdekelt belső munkatársak	– ártó szándék – rendszerekhez való hozzáférés és pontos kép – korlátozott erőforrások és lehetőégek	közepes
Kiberbűnözők	– ártó szándék – korlátozott erőforrások – anyagi haszonszerzési cél – nagy láthatóság	közepes/alacsony
Semleges szereplők	– nem vesznek részt a kiberkonfliktusokban – azonosításuk szükséges – befolyásolható réteg	alacsony

Forrás: a szerző szerkesztése

2.1.3. A kibertérben megjelenő kihívások és fenyegetések

A fentiekben bemutatott kibertéri szereplők után az ezek által kiberműveletekre alkalmazott eszközöket és eljárásokat is célszerű számba vennünk, hiszen a szereplők jelentette fenyegetések azok, amelyekre a védelmi célú kiberműveleteknek meg kell találniuk a hatékony válaszokat.

3. táblázat: A kibertéri fenyegetések lehetséges felosztása

Kibertéri fenyegetések	
Eredet szerint	ellenérdekelt fél vagy felek tevékenysége
	nem szándékos tevékenység (például gondatlanságból, hozzá nem értésből eredő veszélyek)
	természeti katasztrófák
Típus szerint	fizikai fenyegetések (például tűz, áramkimaradás miatt bekövetkező fizikai veszélyek)
	technikai meghibásodás
	szándékosság miatt bekövetkező működéskiesés
Technika/eljárás szerint	elosztott túlterheléses támadás (distributed denial of service, DDoS)
	rosszindulatú program (malware) telepítése
	felhasználó megtévesztése (social engineering)
	szabotázs (például zsarolóvírus-, azaz ransomware-támadás)
	tartalommódosító támadás (defacement)
	információszivárogtatás (information leakage)
	személyiséglopás (identity theft)

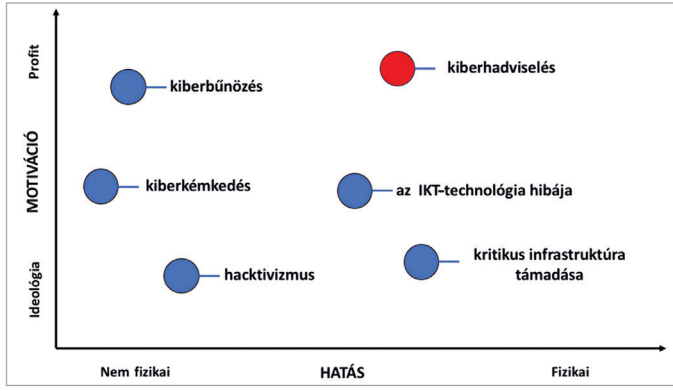
Forrás: az AJP-3.20 alapján a szerző szerkesztése

A kibertérben megjelenő konkrét kihívások és fenyegetések számos rendezőelv mentén kategorizálhatók. Az egyik ilyen osztályozás lehet, hogy ezeket a veszélyeket az eredetük, típusuk és technikájuk szerint csoportosítjuk.[70] Az így meghatározott, alapvetően fenyegetéseket tartalmazó felosztást a következő táblázatban összegezzük. Itt meg kell jegyezni, hogy a szándékos tevékenységek rendkívül gyorsan változnak mind technikájukat, mind eljárásukat tekintve. Ezeket a későbbiekben nagy vonalakban még elemezni fogjuk, hiszen számos technika vagy eljárás kiberfegyverként is alkalmazható. Ugyanakkor a bemutatott és felsorolt fenyegetések jelenleg a legjellemzőbbek. A különböző típusú fenyegetések között természetesen átfedések is felfedezhetők, hiszen például

[70] AJP-3.20. 1.22. pont.

az eredet szerinti besorolásnál megadott természeti katasztrófák értelemszerűen fizikai veszélyeket jelentek.

A kibertéri fenyegetések számbavétele kapcsán ki kell jelentenünk, hogy a kibertérben elkövetett rosszindulatú tevékenységek szándékossága és az általuk okozható hatások mértéke egyenes arányban van egymással, vagyis az ártó szándékkal elkövetett kiberműveletek hatásai nagyobbak, mint a nem szándékos tevékenységek következményei. Ezt szimbolizálja a következő ábra, amely a fentieket kiegészíti a kibertéri műveletek mögött álló motiváció vizsgálatával, illetve a hatások elemzését kiterjeszti a kibertéren kívülre, azaz a fizikai térre is. Az ábrán jól látszik, hogy a legnagyobb, akár a fizikai térben is bekövetkező fizikai hatásokat elérő kibertéri tevékenység a kiberhadviselés.



2. ábra: A kibertérben megjelenő kihívások és veszélyek motiváció és hatás szerinti bemutatása
Forrás: a Cyber Research Center – Industrial Control Systems 2015-ös kutatásai alapján a szerző szerkesztése

Természetesen minden ország és az olyan nemzetközi szervezetek is, mint például a NATO, folyamatosan elemzik és értékelik a kibertérben megjelenő veszélyeket és fenyegetéseket.

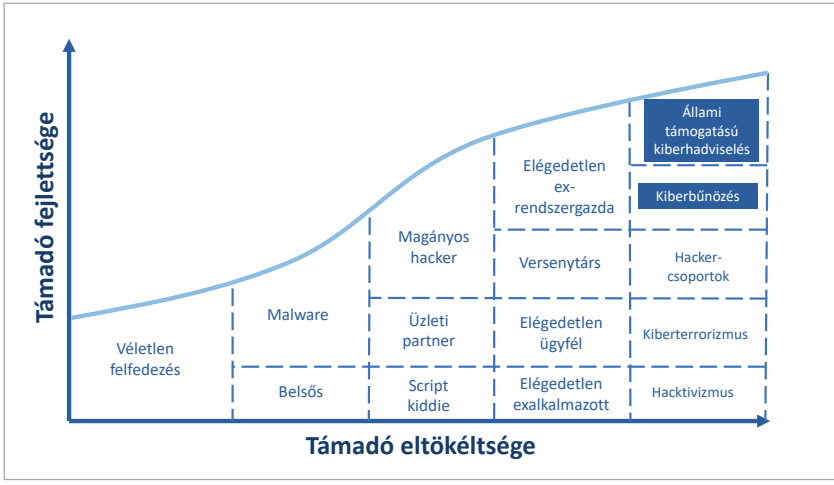
A NATO 2018-ban megjelent összefoglaló tanulmányban tette közzé mindazokat a stratégiai kihívásokat, amelyekkel a szervezetnek, illetve a szervezet tagállamainak 2030-ig várhatóan szembe kell néznie.[71] A tanulmány

[71] Amy Ertan et al. (szerk.): *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2020.

a „Kiberveszélyek és a NATO 2030: a várható új technológiák felmérése és elemzése" címet viseli, és öt fő területre fókuszálva elemzi ezeket a kihívásokat. Az öt fő terület a következő:

1. kibertéri ellenérdekelt felek (országok);
2. új technológiák;
3. a kibertérben megvívandó harc és a hadviselés;
4. az információmegosztás és a kibertéri veszélyek felderítése, valamint a kibergyakorlatok;
5. a kibertér szabályozása és a kiberbiztonsági kihívásokra adott válaszok.

A fenti felsorolásból is jól látszik a kibertéri kihívások és veszélyek komplexitása. Ebből az összetett képből ki kell emelni magát a hadviselést, hiszen az állami támogatással vagy általuk végrehajtott kibertéri műveletek lesznek mind hatásaikban, mind volumenükben a legnagyobb kihívások és veszélyek a jövőben.

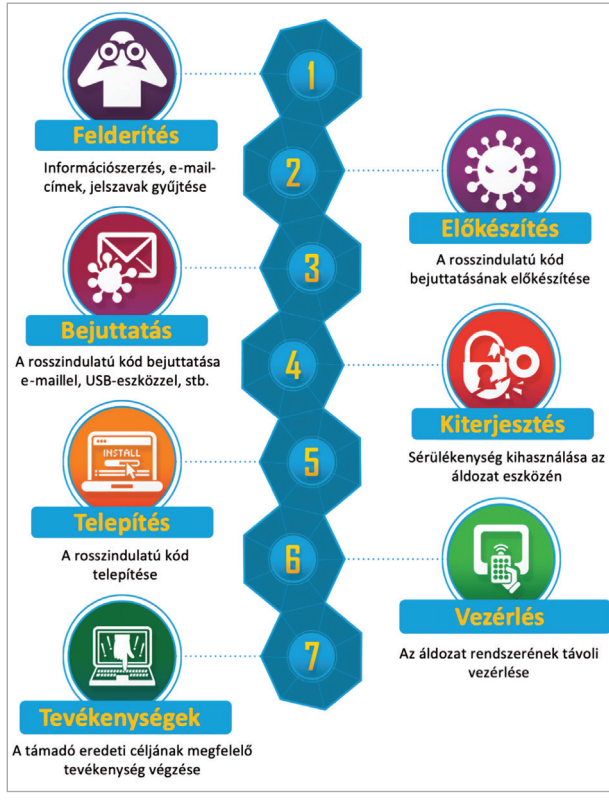


3. ábra: A kiberműveletek által okozható károk mértéke a támadók fejlettsége és a támadók eltökéltsége viszonyrendszerében

Forrás: Petra Cicvaric: Cyber Security – A Strategic Security Priority for NATO. *Atlantic Forum,* 2019 alapján a szerző szerkesztése

Annak vizsgálata sem elhanyagolható, hogy mekkora károk is okozhatók a kiberműveletekkel. Jól szemlélteti ezt az alábbi ábra, amely a kiberművelet mögött

álló személy vagy személyek, azaz a támadó vagy támadók tudása és tapasztalata, illetve céljai szerinti összefüggések alapján vizsgálja az okozható károkat. Az ábrán látható grafikon ezek mértékére vonatkozóan is eligazítást nyújt, hiszen ahogy növekszik a támadó tudása és tapasztalata, illetve ahogy a támadók csoportjai egyre szervezettebbek, annál tetemesebbé válnak az okozható károk, továbbá hogy az olyan nagy tudással rendelkező támadókból álló állami támogatású kiberműveleti csoportok okozhatják a legnagyobb kárt, amelyek már a kiberhadviselés szintjét is elérő kiberműveleteket, illetve kiberműveletek sorozatát képesek végrehajtani.

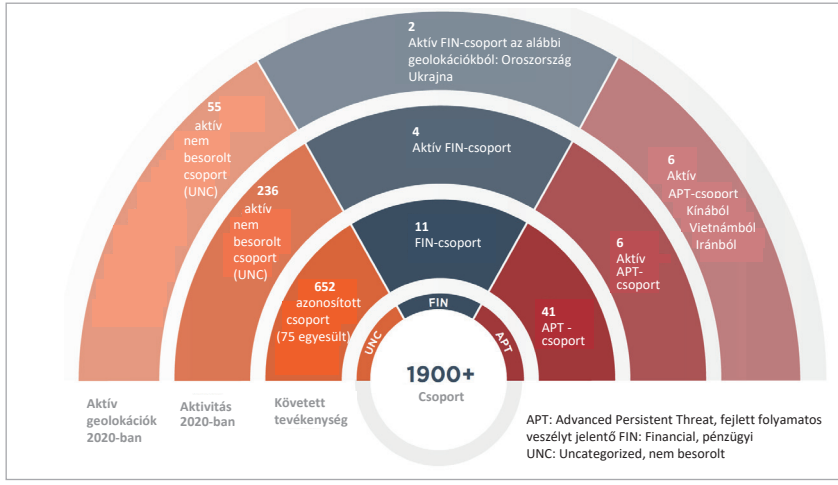


4. ábra: A tipizált kiberművelet egyes fázisai

Forrás: Lockheed Martin: *The Cyber Kill Chain* (2021) alapján a szerző szerkesztése

Amennyiben az egyes kiberműveleteket megvizsgáljuk, akkor azt megállapíthatjuk, hogy ezek nagyon jól tipizálhatók, és nagyon jól felosztható különböző fázisokra. A fázisok feltérképezése és általánosítása a Lockheed Martin amerikai hadiipari cég nevéhez köthető, amely mindezeket a fázisokat egy nagyon demonstratív ábrával is szemléltette. Ezen az ábrán – amelyet most mi is kölcsönzünk – a kiberműveletek életciklusának, illetve ahogy a cég angolul elnevezete, a *cyber kill chain*nek a korai információszerzéstől a beavatkozásig tartó folyamatát láthatjuk. A hét tipizált fázisra osztott kiberműveleti ciklusban megtalálható a felderítés, az előkészítés, a bejuttatás, a kiterjesztés, a telepítés, a vezérlés és a támadó eredeti céljának megfelelő tevékenység végrehajtása.[72]

Ha a kibertéri szereplőket és a kiberműveleteket egyszerre vizsgáljuk, felfedezhetünk olyan csoportokat, amelyek szintén tipizálhatók az általuk rendszerint alkalmazott kiberműveleti eljárások, valamint a támadások célpontjai alapján. A FireEye az egyik 2020-ról szóló jelentésében a következő ábrán látható felosztást alkalmazta mindezekre a csoportokra.



5. ábra: Kibertámadó csoportok 2020-ban

Forrás: FireEye–Mandiant: *M-Trends. 2021. FireEye Mandiant Services – Special Report.* 2021 alapján a szerző szerkesztése

[72] Lockheed Martin (2021): i. m.

Amennyiben számba vesszük, hogy a fent felsorolt és csoportosított fenyegetések közül jelen könyv írásakor melyek a legnagyobb veszéllyel járó kihívások, akkor az ENISA 2021 év végi jelentését segítségül híva a következő kibertéri veszélysorrendet lehet felállítanunk: *ransomware,* azaz zsarolóvírus típusú támadások; rosszindulatú programokkal elkövetett támadások; *cryptojacking,* azaz kriptovaluták bányászására tervezett rosszindulatú alkalmazásokkal elkövetett támadások; e-mailekkel kapcsolatos fenyegetések; adatok elleni fenyegetések; a rendelkezésre állás és az integritás elleni fenyegetés; dezinformáció – félretájékoztatás; nem rosszindulatú fenyegetések, azaz emberi hibára visszavezethető veszélyek; az ellátási láncok elleni támadások.[73]

2.2. A kiberhadviselés meghatározása

A kiberhadviselés meghatározására jelenleg nincs egyértelmű és általánosságban elfogadott definíció. Az azonban egyre nyilvánvalóbb, hogy nagyon sok ország e terület fontosságára tekintettel egyre nagyobb figyelmet fordít a kiberműveleti és a tágabb értelemben vett kiberhadviselésre alkalmas erőinek és képességeinek fejlesztésére.

Fentiek hátterében az az egyszerű ok áll, hogy az állami támogatású kiberműveletek egyre többször és egyre nagyobb volumenben következnek be. Ezt gyakorlatilag minden fejlett ország komoly fenyegetésként értékeli.[74] Az így megjelenő veszély értékelése néhány éve már alapvető témája a nemzeti biztonsági stratégiáknak, illetve ennek kihatásaként a nemzeti katonai stratégiák is egyre nagyobb figyelmet fordítanak erre a területre. Mindezeknek természetes következménye, hogy a fejlett országok megkezdték kiberműveleti erőik építését.

Magára a kiberhadviselés értelmezésére korábban már számos kísérlet született, de ezek egyike sem volt teljes és átfogó. 2011-ben a Haig–Kovács–Ványa szerzőhármas a következő meghatározást adta a kiberhadviselésre: „Cyberhadviselésnek nevezhetjük mindazon tevékenységeket, amelyekben a számítógép-hálózati hadviselés, a számítógép-hálózati műveletek, az elektronikai hadviselés, bizonyos esetekben a SIGINT, valamint a cyberterrorizmus, illetve az ellene

[73] ENISA (2021a): i. m. 4.
[74] Kovács (2018b): i. m. 45.

folyatott tevékenységek közösen jelennek meg."[75] A meghatározásból világosan látszik, hogy

> „[e]z […] még egy meglehetősen technikai alapú megközelítés volt, amelyből ráadásul hiányzott az egyik legfontosabb tényező is. Ez nem más, mint annak a felismerése, hogy kiberhadviselésről – a hagyományos hadviseléssel analóg módon – akkor beszélhetünk, amennyiben egy adott ország vagy országcsoport stratégiai fontosságú rendszerei (például kritikus infrastruktúrái) ellen indított kibertámadások mögött egy másik ország vagy ország csoport (esetleg ezekkel egyenértékű gazdasági vagy politikai hatalom) áll."[76]

A kiberhadviselés meghatározására egy másik kísérlet abból indult ki, hogy mivel ez a biztonság-, illetve védelempolitikának egy rendkívül új területe, célszerű a hagyományos eszközökhöz visszanyúlni. Ezért a kiberhadviselést a hagyományos hadviselés eszköztárába kell illeszteni, és erre is alkalmazni kell a hagyományos hadviselés elveit.

Ennek megfelelően a kibertámadások és a kiberhadviselés is sok esetben a hibrid, azaz a hagyományos hadviselési elemeket az újabb, nem konvencionális elemekkel ötvöző, politikai és katonai célokat egyaránt elérni kívánó tevékenységekként írhatók le, amelyek például a médiaműveletek és a politikai befolyásolás eszköztárát is alkalmazzák.

Ez az irány nem tűnik rossznak, hiszen a hibrid hadviselés, illetve a hibrid műveletek egyik eszközeként felfoghatók a kiberműveletek is, amelyek a tradicionális katonai műveletekkel, valamint az olyan hibrid műveleti elemekkel kiegészítve, mint például az említett médiaműveletek, valóban hatékony és befolyásoló tényezőként léphetnek fel.

Összefoglalva a kiberhadviselés meghatározására irányuló kísérleteket, a belőlük levonható következtetéseket, illetve a kibertér jelenlegi biztonságpolitikai megítélését, nevezetesen azt, hogy a kibertér a lehetőségek mellett komoly veszélyeket is rejt magában, kijelenthetjük, hogy a kiberhadviselés nem jelent mást, mint olyan állami vagy ilyen támogatású kiberműveletek összességét, amelyek célja az adott ország politikai, gazdasági vagy katonai akaratának egy másik országra történő rákényszerítése a kibertéren keresztül. Azonban a korábban jelzettek miatt ez nem feltétlenül jelenti azt, hogy minden kiberhadviselés jellegű kibertámadás mögött egy állam állna, még abban az esetben sem, ha annak politikai vagy katonai céljai vannak. „A kiberhadviselés veszélyességét

[75] Haig et al. (2011): i. m. 199.

[76] Kovács (2018a): i. m. 41–42.

pont az jelenti, hogy olyan kis létszámú csoportok is – állami támogatás mellett, de nyilvánvalóan akár annak hiányában is – el tudják követni ezeket a támadásokat, amelyek tagjai nem feltétlenül az adott országban, hanem akár több eltérő (esetleg pont a cél)országban vannak."[77] Ezzel kapcsolatban meg kell jegyeznünk: jelen írás nem kíván állást foglalni abban a nemzetközi jogot érintő vitában, hogy államnál kisebb szervezet folytathat-e háborút.

A kiberhadviselés korábban már említett két iránya – azaz a hadseregek vezetési és infokommunikációs rendszerei elleni kiberműveletek mint a hagyományos hadviselés fizikai dimenzióiban folyó műveleteinek támogatása, illetve a civil rendszerek elleni kiberműveletek – mellett azonban a már szintén említett hibrid műveletek részeként folytatott kiberműveletek komoly befolyásoló erővel is bírnak.

Ez a befolyásolás politikai téren is nagyon hatékonyan működik, hiszen egy adott ország lakosságát megfelelően tervezett és végrehajtott kiberműveletekkel nagyon jó hatékonysággal lehet befolyásolni. Ennek céljai természetesen változóak lehetnek. Az egyik ilyen cél például a különböző politikai választások kimenetelének befolyásolása. Erre ma már egy-egy klasszikusnak mondható példa a 2016-os amerikai elnökválasztásba történő – elemzések alapján feltételezhetően orosz – beavatkozás, vagy a közvetlenül ezt követő németországi és franciaországi parlamenti, illetve szintén elnökválasztásokba – sok esetben közvetett módon, tehát a választók befolyásolása útján – történő beavatkozások.[78] Összességében elmondható, hogy „[a] politikai befolyásolással kapcsolatban nagyon gyakran két ország – Kína és Oroszország – merül fel, pedig a másik oldalról például az Egyesült Államok is él hasonló módszerekkel".[79]

A kiberhadviselés meghatározása során fontos kijelentenünk, hogy azt el kell határolni a kiberbűnözéstől. A kiberbűnözés fő célja az anyagi haszonszerzés, míg a kiberhadviselés ennél lényegesebb komplexebb és hatásait tekintve is nagyobb veszélyeket jelent. Természetesen nem szabad elfelejtenünk a korábban a kiberbűnözés vonatkozásában már említett tényezőket, amelyek alapján szintén le kell szögeznünk, hogy a kiberbűnözés is lehet egyfajta eszköze a kiberhadviselésnek. Azaz a kiberhadviselés jellegű kiberműveletek sorába nagyon jól és hatékonyan beilleszthetők azok a kiberbűncselekmények, amelyek nagysága elérheti azt a küszöböt, amikor egy adott ország gazdasági rendszerének destabilizációja

[77] Kovács (2018a): i. m. 41.

[78] Kovács László – Krasznay Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Elemzések,* (2017), 9.

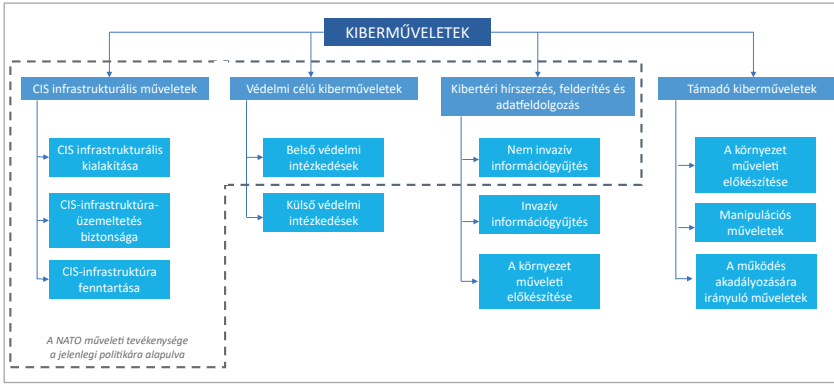
[79] Kovács (2018a): i. m. 42.

bekövetkezik. Elemzők számos úgynevezett FIN-, azaz pénzügyi csoportot azonosítottak, amelyeknek közvetlen célja természetesen az anyagi haszonszerzés valamely kibertéri – rosszindulatú — tevékenység révén, de közvetett céljaik ennél nagyságrendekkel nagyobbak: az adott ország pénzügyi vagy akár teljes gazdasági ellehetetlenítése. Észak-Korea egyes hírek szerint kiberbűnözői módszerekkel tetemes anyagi haszonra tett szert, amellyel az egyébként nagyon mély válságban lévő gazdaságát kívánja támogatni.[80]

Ugyanakkor általában a kiberbűnözés sem céljaiban, sem volumenében nem éri el azt a szintet, amely a hadviseléssel lenne azonosítható.

2.3. A kiberműveletek fajtái

Általánosságban elmondható, hogy a kiberhadviselés kiberműveletek sorozataként jellemezhető. Függően a kiberműveletek jellegétől, azaz függően attól, hogy azok katonai vagy civil célpontok ellen irányulnak-e, természetszerűleg számos más művelet is csatlakozhat a kiberműveletek sorozatához. Ilyenek például a médiaműveletek, a lélektani műveletek, vagy akár az elektronikai hadviselés egyes műveletei.



6. ábra: A kiberműveletek fajtái, NATO-felosztás

Forrás: NATO: *High Level Taxonomy of Cyberspace Operations* (2018) alapján a szerző szerkesztése

[80] The Lazarus Heist: How North Korea Almost Pulled off a Billion-Dollar Hack. *BBC News,* 2021. június 21.

A kiberműveletek fajtáinak meghatározása során a NATO felosztását használjuk kiindulópontként. A szövetség szerint négy alapvető fajtáról beszélhetünk: CIS infrastrukturális műveletek; kibertéri hírszerzés, felderítés és adatfeldolgozás; védelmi célú kiberműveletek; támadó kiberműveletek.[81] A 6. ábra ezeket foglalja össze.

A CIS infrastrukturális műveletek nem jelentenek mást, mint az alapvető vezetés és irányításhoz, fegyverirányításhoz, illetve a hírszerzéshez szükséges infokommunikációs infrastruktúra kialakítását, biztonságának megteremtését, valamint a kiépített infokommunikációs infrastruktúra fenntartását. Ebbe a műveleti körbe tartozik az elektronikus információbiztonság megteremtése, fenntartása és folyamatos fejlesztése is, azaz az információs rendszerekben megjelenő adatok és információk esetében a – korábban már tárgyalt – bizalmasság, sértetlenség és rendelkezésre állás biztosítása a legfontosabb cél. Bár az infokommunikációs rendszerek elektronikus információbiztonsági eseménykezelését nagyon sok ország, de egy adott országon belül is nagyon sok szervezet igyekszik különválasztani a CIS infrastrukturális műveletek alapvető tevékenységi körébe tartozó üzemeltetés feladataitól, mégis azt kell mondanunk, hogy az mind technikai, mind szabályozási kérdései révén nagyon sok szállal kötődik az üzemeltetéshez.

A CIS infrastrukturális műveletek egyik legnagyobb kihívása a különböző dimenziókban – tehát a fizikai dimenziókban, a kibertérben és az információs dimenzióban egyidejűleg – biztosítani az infokommunikációs rendszerek működését, amihez még az olyan hadviselési elvek is komplexitása is hozzáadódik, mint például a multitérműveleteké, hiszen itt az egy időben több helyen történő művelet-végrehajtás infokommunikációs igényei jelennek meg.

A CIS infrastrukturális műveletek jelentik tehát azon alapvető infokommunikációs rendszer együttesének a kialakítását és üzemeltetését, amelyet a korszerű, digitális hadseregek esetében már elemeztünk.

A kiberműveletek következő típusát a védelmi célú kiberműveletek jelentik. Ezek célja, hogy a kibertérben biztosítsák és fenntartsák mind a kiberműveleti, mind a hagyományos erők mozgás- és cselekvési szabadságát annak ellenére, hogy a szemben álló fél kiberműveletekkel ezt igyekszik ellehetetleníteni, illetve akadályozni. Definíciószerűn megfogalmazva a védelmi kiberműveletek olyan tevékenységek és intézkedések összességét jelentik, amelyek szavatolják

[81] NATO: *High Level Taxonomy of Cyberspace Operations.* A 3400 TSC FCX-0010/TT-180202/Ser:NU0171. számú dokumentum „A" melléklete (2018).

a kibertérben a mozgás- és cselekvésszabadságot, valamint a saját erők védelmét. Ezek lehetnek sérülékenységvizsgálatok, kockázatelemzések és egyéb, a műveletekhez kapcsolódó konkrét védelmi intézkedések.[82] A védelmi célú kiberműveletek tehát olyan intézkedéseket és technikai eljárásokat alkalmaznak, amelyek gyakran magukban foglalják az elektronikus információbiztonság kialakítását és fenntartását is. Az elektronikus információbiztonság szorosan kapcsolódik a védelmi kiberműveletekhez, sok esetben integráltan jelenik meg ezekben.

A védelmi célú kiberműveletek egyik alapvetése, hogy csak akkor lehet hatékonyan alkalmazni, illetve végrehajtani őket, ha tisztában vagyunk a saját infokommunikációs rendszereink felépítésével, az azokban meglévő esetleges sérülékenységekkel, valamint az ellenérdekelt felek kiberműveleti képességeivel.

Fontos megjegyezni, hogy a védelmi kiberműveletek néhány esetben támadó kiberműveletek végrehajtását igénylik a saját kiberműveleti erőinktől ahhoz, hogy egy a jövőben potenciálisan bekövetkező ellenérdekelt kibertámadást megelőzzünk. Ezen megelőző, alapvetően a védelem érdekében végrehajtott kibertámadások célja az, hogy az ellenérdekelt fél kiberműveleti lehetőségeit és eszközeit működésükben akadályozza, és így gyakoroljon hatást mozgás- és cselekvési szabadságára. Természetesen bár a védelmi célú támadó kiberműveleteket a kibertérben hajtják végre, hatásaikat sok esetben a kibertéren kívül a fizikai térben is kifejthetik. Mindezeken túl a szemben álló fél kiberműveleti képességei vagy infokommunikációs rendszerei ellen a fizikai térben végrehajtott kinetikus műveletek szintén hozzájárulnak a saját oldali védelmi célú kiberműveletekhez. Azonban már itt hangsúlyoznunk kell, amire a későbbiekben még részletesen is kitérünk, hogy a kibertérben megvalósított műveletek és a fizikai dimenziókban végrehajtott műveletek csak abban az esetben lesznek hatékonyak, és csak abban az esetben támogatják egymást hatásait, ha mindenre, azaz térre, időre, közvetlen és közvetett hatásaikra is kiterjedően szinkronizáltan és összehangoltan mennek végbe.

A következő kiberműveleti fajta a kibertéri hírszerzés, felderítés és adatfeldolgozás.[83] Ahhoz, hogy hatékony kiberműveleteket lehessen végrehajtani, elengedhetetlen, hogy reális kiberhelyzetkép birtokában legyünk. Ennek a kiberhelyzetképnek nemcsak naprakésznek kell lennie, hanem lehetőség szerint tartalmazni kell az ellenérdekelt fél jövőben várható tevékenységére vonatkozó minél

[82] AJP-3.20. 2.20. pont.
[83] AJP-3.20. 1.32. pont.

pontosabb előrejelzéseket is, valamint a saját rendszereink sérülékenységeitre, illetve az ellenérdekelt fél kiberműveleti képességeire, eszközeire és eljárásaira vonatkozó információkat is. A kiberhelyzetkép kialakítása az egyik legfontosabb feladata a kiberhírszerzésnek, amely minden elérhető és releváns katonai és civil információ- és adatforrást felhasznál műveletei során. A saját rendszerek vonatkozásában összegyűjti, elemzi és értékeli a saját eseménykezelő rendszer információit, valamint általában saját kibertéri korai figyelmeztető rendszert is kiépít.

A kiberhírszerzés az ellenérdekelt fél infokommunikációs rendszereiről és rendszereiből olyan információkat szerez, amelyek azok sérülékenységeire, támadható pontjaira utalnak, vagy amelyeken keresztül további információk nyerhetők ki. Ebbe az információgyűjtésbe beletartozik a rendszereket kezelő személyzetről gyűjtött információ is, a parancsnokoktól kezdve egészen az üzemeltető vagy fejlesztőmérnökökig. Természetesen a nyugati országokban ezt a kiberhírszerzési munkát szigorú előírások szabályozzák, és általában katonai és/vagy polgári nemzetbiztonsági szolgálatok végzik a megfelelő jogszabályi felhatalmazások alapján.

A kiberhírszerzési munka nagyban támaszkodik a nyílt forrású felderítésre, amelyet az angol terminológia alapján OSINT-nek *(open-source intelligence)* nevezünk. A közösségi média előretörésével természetes módon az ott folytatott információszerzés is a mindennapok részévé vált a kiberhírszerzésben, hiszen az ellenérdekelt fél rendszereit kezelő említett szakszemélyzet esetében is nagyon sok és releváns információ szerezhető a közösségi médiában végzett felderítéssel (*social media intelligence,* SOCMINT).

A megszerzett adatok és információk feldolgozása kiemelt fontosságú. Ez a munka ma már nem képzelhető el automatizált adatfeldolgozó rendszerek nélkül, amelyek nemcsak a különböző kibertéri és más forrásokból származó adatok gyűjtését és összehasonlítását végzik el, hanem a mesterséges intelligencia bizonyos fokú felhasználásával trendelemzéseket, összefüggések feltárását, hálózati kapcsolatok összefűzését is képesek elvégezni.

A negyedik kiberműveleti fajta a támadó célú kiberművelet. Ezt gyakran offenzív kiberműveleteknek is nevezik, bár rögtön le kell szögezni, hogy az offenzív kiberműveletek szélesebb tevékenységi kört jelentenek, mint a támadó kiberműveletek, mert az offenzív kiberműveletek magukban foglalják az információszerzést, magát a támadó műveletet, illetve a hatáselemzést is.

A támadó kiberművelet valamilyen erőt használ az ellenérdekelt fél kiberterében, hogy akadályozza, megnehezítse vagy ellehetetlenítse annak elérését,

illetve meggátolja az ott alkalmazott ellenérdekelt infokommunikációs rendszerek működését.

A támadó kiberműveletek végrehajtását különböző szakaszokra lehet osztani. Az első szakasz az információgyűjtés, amelyek során a támadó műveletek megtervezéséhez szükséges minden releváns információt összegyűjtenek. Ekkor vetik egybe az ellenérdekelt fél információs rendszereiben feltárt sérülékenységeket a saját kiberműveleti képességekkel, ami alapján kidolgozzák a támadás alternatív megoldásait. A következő szakasz a célpontok azonosítását, priorizálását és a műveletek részletes megtervezését foglalja magában. Ekkor határozzák meg a szükséges erőforrásokat és dolgozzák ki a támadás eljárásrendjét. Természetesen a kiberműveleteket – köztük a támadó célú kiberműveleteket – önállóan is végre lehet hajtani, de általában más műveletekkel együtt, azokkal koordinált módon alkalmazzák őket. Így biztosítható, hogy hatékonyan támogassák a más domainekben zajló műveleteket, illetve hogy azok hatásait növeljék. Ezt követi maga a támadás végrehajtása, ami a korábban már említett tipizált kiberművelet *(cyber kill chain)* fázisaival megegyező módon a behatolást, a telepítést, majd a hatás kiterjesztését jelenti. A támadó célú kiberműveletek egyik fontos eleme a támadás technikai végrehajtását követően annak hatáselemzése. Ennek során felmérik, hogy a támadás az eredeti tervek szerint elérte-e a kívánt hatást – ha nem, akkor szükség esetén új kiberművelet végrehajtása válik szükségessé, vagy a folyamatban lévő műveletben kell megfelelő változtatást eszközölni.

A kiberműveletekre történő felkészülés nemcsak sok energiát és technikai fejlesztést, hanem sok időt is igényel. Azok a tapasztalatok, amelyek a különböző kiberműveletek során keletkeznek, be kell hogy épüljenek gyakorlatilag minden katonai tevékenységbe, különösen a műveleti tervezésbe. Ennek egyik legfontosabb eleme a hatások felmérése. A különböző kiberműveleti tevékenységek hatásai, illetve azok felmérése komoly kihívás elé állítja napjaink hadseregeit. Ennek oka elsősorban az, hogy a kiberműveletek nemcsak a kibertérben, hanem többek között a fizikai térben és akár az információs térben is zajlanak. Ráadásul a digitális infrastruktúra összekapcsoltsága, komplexitása nem mindig teszi lehetővé, hogy az adott rendszer vagy rendszerelem ellen intézett támadás következményeit széles körben, mindenre kiterjedően előre megadjuk.

A hadseregek szemszögéből a kiberműveleteket nem csak a fenti négy, a NATO által is használt felosztásban lehetséges kategorizálni. Megkülönböztethetünk például védelmi és támadó kiberműveleteket – ez azonban a fentiek fényében kissé leegyszerűsítése lenne a valóságnak. Egy további felosztás lehet, ha nemzeti szintű, illetve közvetlen katonai célú kiberműveletek szerint csopor-

tosítjuk őket. A nemzeti szintűek esetében a hadsereg vezeti az ország kiberműveleteit, a civil kibertéri szereplők pedig támogatják mindezeket; illetve az is elképzelhető, hogy a hadsereg csak közreműködik, azaz támogatja a nemzeti kiberműveleteket, részt vesz a koordinációban, megerősítő kibererőket biztosít a civil kibertéri entitások számára, támogatja a nemzeti szintű kritikus infrastruktúra, valamint a kritikus információs infrastruktúra védelmét. A hadsereg által vezetett nemzeti kiberműveletek alapvetően különleges jogrendi helyzetben, azaz fegyveres konfliktus időszakában valósulnak meg. Ezzel szemben a közvetlen katonai célú kiberműveletek során a hadsereg a fizikai dimenziókban zajló, katonai célú műveleteket támogatja kiberműveletekkel, azaz együttműködik a szárazföldi, a légi-, valamint a különleges rendeltetésű erőkkel azok műveleteinek végrehajtásában.

2.4. Nagy visszhangot kiváltott kibertámadások

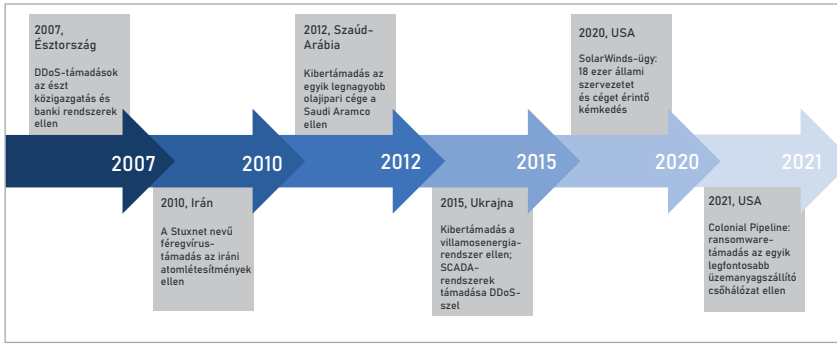
A legnagyobb visszhangot kiváltott kibertámadások, illetve kiberműveletek mentén fel lehet rajzolni a kiberhadviselés eddigi történetét, hiszen ha az első igazán jelentős olyan kibertámadási sorozatot keressük, amely egyrészt kielégíti a korábban általunk felvázolt kiberhadviselés-definíciót – azaz leginkább az jellemzi, hogy állam(ok) vagy állami támogatású csoportok kibertérben megvalósított rosszindulatú beavatkozása történik egy másik ország infokommunikációs rendszereibe, másrészt valódi károkat is okozott –, akkor 2007-ig, az Észtországot ért kibertámadás-sorozatig kell visszautaznunk az időben.

Meg kell jegyeznünk, hogy a kiberhadviselés történetének vázlatos áttekintése során nem térünk ki az olyan korábbi eseményekre, mint például az 1999 és 2003 között zajló, a későbbiekben *moonlight maze* (holdfénylabirintus) néven elhíresült kiberkémkedési sorozatra, vagy például a szintén a 2000-es évek elején történt, egészen pontosan 2000 és 2003 között zajlott *titan rain* (titáneső) elnevezésű kiberkémkedési akciókra. Ezek bár nagyon komoly károkat okoztak, alapvetően megmaradtak az információszerzés szintjén.[84]

Alább következő áttekintésünk nemcsak nagyon elnagyolt, hanem szubjektív is, hiszen a 2010-es évek óta már számos olyan kisebb-nagyobb kiberműveletet láthattunk, amelyek elérik a kiberhadviselés szintjét, de mégsem kerültek be összefoglalónkba. Olyan komolyabb, nagy nemzetközi visszhangot kiváltó téma-

[84] Kovács (2018b): i. m. 156.

dásokat, illetve támadássorozatokat igyekeztünk kiválasztani és bemutatni, amelyek jól példázzák és reprezentálják a kiberhadviselés legjellemzőbb vonásait.



7. ábra: A kiberhadviselés történetének néhány fontosabb művelete
Forrás: a szerző szerkesztése

2.4.1. 2007. április

2007 áprilisának végén a digitalizációban és az elektronikus közigazgatásban élen járó Észtországot, amelynek ekkor már az internetpenetrációja, azaz a lakosság arányához mért internetfelhasználók száma is igen magas volt, súlyos kibertámadások érték. Az alapvetően DDoS-támadásokra épülő kiberműveletek elsődleges célpontjai a közigazgatás, a média és a banki rendszerek.

A támadások nem voltak előzmény nélküliek, hiszen egy politikai döntés indukálta őket: egy II. világháborús, szovjet emlékmű eltávolítása Tallinnban. A döntést követően mind Észtországban, mind Oroszországban tüntetések kezdődtek, amelyekkel közel egy időben meg is indultak a kibertéri támadások.

Ez a támadássorozat olyannyira megdöbbentette az észt hatóságokat, hogy NATO-tagállamként azonnal a szövetség segítségét kérték. Ugyanakkor a NATO döntéshozói is meglehetősen értetlenül álltak az események előtt, hiszen a szervezet története során ez volt az első olyan eset, amikor egy tagállamot a kibertérből ért támadás, sőt az első időszakban még az is kérdéses volt, hogy ezek a kibertéri incidensek egyáltalán támadásnak minősíthetők-e. Az említett sorozatos akciók mellett a közösségi oldalakon és mobiltelefonos sms-üzeneteken keresztül tüntetésekre, ellenállásra és további erőszakra szólítottak fel a támadók mintegy

három héten át, amelynek végére Észtország internetes hálózata már szinte teljes egészében megbénult.

A támadások későbbi elemzése során kiderült, hogy több hullámban, alapvetően az országon kívülről érkeztek, és a szokásos adatforgalom többezerszerese is megjelent a különböző észt rendszereken. A célpontok kiválasztása nem véletlenszerűen, hanem nagyon is tudatosan történt: az ország internetes forgalmában kulcsszerepet játszó adat- és kapcsolóközpontok *(exchange)* naponta többször leálltak, a közigazgatás számítógép-hálózatait le kellett kapcsolni az internetről. A hálózati infrastruktúra kulcsfontosságú elemei mellett azonban a banki rendszerek is érintettek voltak, aminek következtében komoly pénzügyi válság volt kibontakozóban. Ezek a támadások közel két hétig folytatódtak, súlyos – elsősorban – erkölcsi és morális krízist okozva a közigazgatásban, a média területén és a banki, pénzügyi rendszerekben.

Ahogy korábban említettük, a NATO kezdetben tanácstalanul állt az események előtt, de ugyanez igaz volt az Európai Unióra is. Ugyanakkor a NATO döntéshozói kis késéssel felismerve a helyzetet – bár nem nyilvánították katonai támadásnak az eseményeket, és így a NATO-alapokmány 5. cikkelyének, azaz a kollektív védelemnek az életbe léptetése sem történt meg – számos hosszú távú intézkedésre tettek javaslatot az eset kapcsán.

Ilyen javaslat alapján a NATO 2008-ban felállította Kibervédelmi Kiválósági Központját (NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE) – nem meglepő módon éppen Tallinnban –, amely azóta a terület egyik vezető kutató- és koordináló szervezetévé vált. A CCDCOE többek között kutatja a kibertér jogi kérdéseit, a technikai védelem kialakítását, valamint számos – tudományos kutatásokra alapozott – ajánlást dolgoz ki, amelyek nem csak a NATO-tagországok számára hasznosak a kibervédelem szélesebb értelemben vett erősítése érdekében. Magyarország 2010-ben csatlakozott a központhoz, és azóta is aktív résztvevője az ott zajló munkának.[85]

2.4.2. 2010. október

2010 őszén kibertámadás érte Irán egyik atomerőművét, illetve urándúsító üzemének centrifugáit. A támadás egy olyan malware-rel történt, amely közvetett módon már nemcsak szoftveres, hanem hardveres, azaz a fizikai térben

[85] Kovács (2018b): i. m. 147.

megvalósuló károkat is okozott. A később Stuxnet névre keresztelt úgynevezett féregvírus – azaz a rosszindulatú programok családjába tartozó féreg, illetve a szintén rosszindulatú programként azonosítható vírusok közös jegyeit felmutató program – rendkívül gyorsan terjedt a megcélzott ipari környezetben. Ez volt az első egyértelműen ipari vezérlőszoftverek működésének manipulálására készített malware.

A Stuxnet az Irán által is használt Siemens PLC-ket *(programmable logic controller),* azaz ipari vezérlő számítógépeket támadta.[86] A Stuxnet azért is volt újdonság, mert ennek a féregvírusnak a megírása óriási mennyiségű pénzbe és időbe került, valamint az alkalmazása előtt a célpontokhoz hasonló környezetben tesztelni is kellett. A Stuxnet négy *zero-day exploit*ot, azaz olyan sérülékenységet használt ki, amelyre még nem volt védelmi mechanizmus kialakítva.[87] Egyértelmű bizonyíték nem került napvilágra a Stuxnet eredetét illetően, de 2011 januárjában a *New York Times* utalt rá, hogy a Stuxnet mögött Izrael és az Egyesült Államok állhatott. Ezt a megállapítást nem technikai elemzésekre, hanem közvetett bizonyítékokra alapozták. Egyrészt Izraelnek érdekében állhatott, hogy Irán ne jusson rövid időn belül olyan dúsított uránhoz, amellyel nukleáris fegyvert állíthat elő, illetve Izrael rendelkezett olyan infrastruktúrával, amellyel tesztelni lehetett a Stuxnetet és annak hatásait. A lap szerint további bizonyíték lehet, hogy az akkori amerikai külügyminiszter, Hillary Clinton, valamint a Moszad, azaz az izraeli titkosszolgálat egyik volt vezetője, Meir Dagan úgy nyilatkoztak, hogy reményeik szerint a Stuxnet által okozott károk az iráni atomprogramot akár több évvel is késleltetik.[88]

> „A Stuxnet rávilágít arra a tényre, hogy ma egy-egy malware […] esetében már jóval többről beszélhetünk, mint »egyszerű« kibertámadás[ról], amelynek esetlegesen semmilyen más célja nincs, csak az anyagi haszonszerzés. A Stuxnet-esetből is levonhatjuk azt a következtetést, hogy az államilag támogatott kibertámadásokkal egy új, sokkal veszélyesebb és sokkal beláthatatlanabb korszak köszöntött be a kibertérben, mint azt korábban feltételeztük."[89]

[86] Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. *Hadmérnök,* 5. (2010), 4. 163–172.

[87] Bruce Schneier: Stuxnet. *Schneier on Security,* 2010. október 7.

[88] William J. Broad – John Markoff – David E. Sanger: Israeli Test on Worm Called Crucial in Iran Nuclear Delay. *New York Times,* 2011. január 16.

[89] Kovács (2018b): i. m. 165.

2.4.3. 2012. augusztus

2012 augusztusában a Saudi Aramco, a világ egyik legnagyobb olajvállalata ellen történt kibertámadás. Az úgynevezett *spear-phishing,* azaz célzott adathalász-támadás végrehajtása után a cég számítógépeinek közel háromnegyede, azaz 30 ezer számítógép fertőződött meg. Maga a rosszindulatú program egy időzített logikai bombát is tartalmazott, amely akkor lépett működésbe, amikor a cég alkalmazottainak jelentős része egy vallási ünnep miatt nem dolgozott, így csökkentve annak a veszélyét, hogy a malware-t idő előtt felfedezzék. A malware minimum három komponensből állt, amelyek egyike a megfertőzött számítógépek merevlemezeinek törlését végezte. A rosszindulatú program néhány órán belül hatalmas károkat okozott a vállalat belső hálózatában, és bár nem érintette közvetlenül az olaj- és gázkitermelést, közvetve mégis komoly hatással volt a cég működésére. Amerikai elemzők később Iránt nevezték meg a támadás kivitelezőjének.[90]

2.4.4. 2015. december

2015 decemberében, majd pedig 2016 decemberében súlyos kibertámadások érték Ukrajna villamosenergia-hálózatát. Mindkét esetben egy ukrán regionális villamosenergia-elosztó és villamosenergia-átviteli cég számítógépeit és SCADA- *(Supervisory Control and Data Acquisition),* azaz ipari rendszerirányító rendszereit vették célba. A 2015-ös támadás során az úgynevezett BlackEnergy malware-t használták, amely többek között DDoS-támadásokra, információszerzésre, illetve adatok és információk megsemmisítésére alkalmas. A 2008-as grúz–orosz háborúban már használták ezt a trójai programot, amikor szintén DDoS-támadásokat hajtottak végre vele.[91] Az ukrán villamosenergia-cég számítógépeinek leállása számos kapcsolóközpont és terhelosztó kiesését jelentette, aminek következtében több mint 200 ezer fogyasztó nem jutott áramhoz.[92]

[90] Nicole Perlroth: In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. *The New York Times,* 2012. október 23.

[91] Global Research & Analysis Team: BlackEnergy APT Attacks in Ukraine Employ Spearphishing with Word Documents. *SecureList,* 2016. január 28.

[92] SANS: *Analysis of the Cyber Attack on the Ukrainian Power Grid* (2016. március 18.).

Ezek a támadások természetesen nem véletlenszerűen következtek be. Egyrészt a háttérben politikai, diplomáciai okok húzódhattak meg, másrészt magukat az akciókat komoly felderítés előzte meg. Ebben a felderítésben nagy szerepe volt annak, hogy a villamosenergia-rendszereket érintően korábban a gyártók számos sérülékenységet publikáltak, amelyek nyíltan elérhetők voltak az interneten.[93]

Természetesen nem az ukrajnai eset volt az első, és nem is a korábban említett Stuxnet-ügy, amelyek során a SCADA-rendszereket kompromittálták. 2000-ben Ausztráliában a Maroochy Shire-i szennyvíztisztító SCADA-rendszereibe hatolt be az elkövető: egy korábbi belső munkatárs volt, akit elbocsátottak.[94] Ez a volt munkatárs közel három hónapon át hatalmas mennyiségű tisztítatlan szennyvizet engedett ki a rendszerből az élő vizekbe úgy, hogy több mint száz szennyvízátemelő szivattyú vezérléséhez fért hozzá egy laptoppal.[95] Itt érdemes megjegyezni, mint ahogy a kibertér szereplőinél már említettük, hogy a belső munkatársak szerepe a támadások elkövetésében évről évre változik, de összességében véve növekvő tendenciát mutat. A FireEye amerikai kiberbiztonsági óriásvállalat egyik 2021-ben publikált jelentése szerint arányuk 2020-ra már elérte az 59%-ot az összes elkövető közül, míg 2019-ben ez az arány még 47% volt.[96]

Szintén SCADA-rendszereket ért támadás 2020-ban, amikor Izraelt érte nagyon érzékeny kibertámadás. A támadások egy része mezőgazdasági vízszivattyúkat célzott Izrael galileai részén, amelyek közül sikerült is néhányat leállítani. Egy másik támadássorozatban ivóvízellátási rendszerek kerültek célkeresztbe Izrael középső, vízben igencsak szűkös részén. A támadások nem jártak nagy sikerrel, de potenciális fenyegetésük hatalmas volt, hiszen a támadók nagy valószínűséggel nemcsak a vízellátást akarták leállítani, hanem az ivóvízbe a normál érték többszörösét meghaladó klórt is be akartak juttatni. Mindezeket a SCADA-rendszerek támadásával kívánták végrehajtani.[97]

[93] SANS (2016): i. m.

[94] Nabil Sayfayn – Stuart Madnick: *Cybersafety Analysis of the Maroochy Shire Sewage Spill (Preliminary Draft).* Cambridge, Massachusetts Institute of Technology, 2017.

[95] Jill Slay – Michael Miller: Lessons Learned from the Maroochy Water Breach. In Eric Goetz – Sujeet Shenoi (szerk.): *Critical Infrastructure Protection.* Az International Conference on Critical Infrastructure Protection (ICCIP) című konferencia anyaga. (H. n.), Springer, 2007.

[96] FireEye: *M-Trends* (2021). 10.

[97] Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps. *Times of Israel,* 2020. július 17.

2.4.5. 2020. december

2020 decemberében a FireEye közzétett egy blogbejegyzést, amely szerint a cég rendszereit komoly kibertámadás érte. Ez már önmagában is nagyon rémisztő hír, hiszen a világ egyik vezető kiberbiztonsági cégéről van szó, de emellett arról is beszámoltak, hogy a támadók kormányzati szervezetek kiberbiztonsági tesztelésére használt szoftverekhez is hozzáfértek az akció során.

A cég vizsgálatai rámutattak, hogy bár ők fedezték fel a támadást a saját rendszereikben, az az egyik szoftverbeszállítójukon, a SolarWindsen keresztül jutott be hozzájuk. A további elemzések szerint a SolarWinds rendszereiben a támadók hónapokkal korábban kémprogramokat és egyéb rosszindulatú szoftvereket helyeztek el. A probléma nagyságrendjére jellemző, hogy a SolarWinds közel 18 ezer vállalatnak szállított szoftvereket.

Ezt követően nagyarányú technikai vizsgálat kezdődött világszerte, amelynek eredményei azt mutatták, hogy a támadók a SolarWinds gyári frissítésein keresztül hatolhattak be a cég rendszereibe valószínűleg még 2020 áprilisában. Az ügyben olyan vállalatok voltak érintettek, mint például a Cisco, az Intel, az NVIDIA, a Deloitte, az SAP vagy a szintén kiberbiztonsággal foglalkozó Check Point. Ugyanakkor a vállalatok mellett az amerikai szövetségi kormányzat olyan szervezeteire is kiterjedt a támadás, mint például a Védelmi Minisztérium, a Belbiztonsági Minisztérium, az Államkincstár, illetve a NASA, továbbá világszerte sok ország kormányzati rendszere szintén az érintettek között volt. E szervezetek mindegyike adatlopási céllal történő támadás áldozatává vált az igen szofisztikált akcióban.[98]

Nagyon fontos kiemelni, hogy bár a támadás mögött szakértők Oroszországot sejtik,[99] az ügy nagyon jól rávilágít a beszállítói lánc (angol kifejezéssel a *supply chain*) biztonságának fontosságára, hiszen a támadók már a SolarWinds rendszereibe sem közvetlenül, hanem nagy valószínűséggel a harmadik vállalatokhoz kiszervezett szoftverfejlesztések során helyezték el a kémprogramokat.

[98] Christina Zhao: SolarWinds, Probably Hacked by Russia, Serves White House, Pentagon, NASA. *Newsweek,* 2020. december 14.

[99] E. David Sanger: After Russian Cyberattack, Looking for Answers and Debating Retaliation. *The New York Times,* 2021. február 23.

2.4.6. 2021. április

2021 áprilisában az Egyesült Államok egyik legnagyobb üzemanyag-szállító csőhálózatát üzemeltető vállalatot, a Colonial Pipeline-t érték kibertámadások. Érdekes módon a zsarolóvírus-támadás elkövetői azonnal vállalták kilétüket, és meg is nevezték az akció mögötti motivációjukat: az orosz, de nem állami kötődésű kiberbűnözői csoport, a DarkSide saját bevallása szerint nem politikai vagy egyéb okokból, hanem alapvetően pénzszerzési céllal követte el tettét.

A Colonial Pipeline csővezeték az Egyesült Államok keleti partvidékén majdnem 9000 kilométer hosszúságban fut végig, és a régió napi üzemanyag-mennyiségének 45%-a ezen a hálózaton jut el az elosztókig és a benzinkutakig.

A ransomware a csőhálózat teljes egészét elérte, így a cég kénytelen volt teljesen leállítani annak működését. Ez azonban azzal a következménnyel járt, hogy az elosztók, illetve a benzinkutak nem jutottak üzemanyaghoz, a lakosság kezdett kifogyni a benzinből és a gázolajból. Nagyon rövid időn belül súlyos ellátási problémák jelentkeztek több államban.

A cég kénytelen volt kifizetni a ransomware váltságdíját, amelyet az elkövetők bitcoinban kértek. A támadók ezután megadták a titkosított adatok feloldásához szükséges kódokat, de a hálózat újraindítása még napokat vett igénybe.[100]

A Colonial Pipeline esete ismét rávilágít arra a korábban már többször említett tényre, hogy a kibertérből érkező támadások nemcsak a kibertérben fejthetik ki hatásukat, hanem a fizikai térben is. Ez az olyan kritikus infrastruktúrák esetében, mint például az üzemanyag-ellátás, további erre épülő vagy ezzel interdependenciában, azaz kölcsönös függőségben lévő alágazatok működésében jelentkezhet negatív hatással, ami a lakosság alapvető ellátását – ahogy a Colonial Pipeline esetében láthattuk, akár az energiaellátását is – veszélyezteti.

2.4.7. 2021. január

2021 januárjában a világ egyik legelterjedtebb e-mail-kiszolgáló motorját érte támadás. A *Microsoft Exchange Server* elleni támadásokat először az Egyesült Államokban, majd a világ több pontján is detektálták: a szolgáltatás egyik sérülékenységét kihasználó akciók több tízezer e-mail-szerver kompromittálódását okozták. Elemzők a támadások mögött Kínát feltételezték, amit megerősít

[100] Colonial Pipeline Boss Confirms $4.4m Ransom Payment. *BBC News,* 2021. május 19.

a NATO hivatalos közleménye is. Ebben a szervezet kifejezte szolidaritását a támadást elszenvedő országokkal, és elítélte Kínát mint a támadások elkövetőjét. Ez nagyon fontos mérföldkő, hiszen a NATO korábban még sohasem élt hivatalosan az attribúció, azaz a támadó megnevezése eszközével kibertámadások esetében. A nyilatkozat úgy fogalmazott:

> „Szolidárisak vagyunk mindazokkal, akiket érintettek a legutóbbi rosszindulatú számítógépes tevékenységek, beleértve a Microsoft Exchange Server kompromittálódását. Az ilyen rosszindulatú számítógépes tevékenységek aláássák a biztonságot, a bizalmat és a stabilitást a kibertérben. Elismerjük a szövetségesek, például Kanada, az Egyesült Királyság és az Egyesült Államok nemzeti nyilatkozatait, amelyek a Microsoft Exchange Server kompromittálódásáért való felelősséget a Kínai Népköztársaságra hárítják."[101]

2.4.8. 2021. december

2021 decemberében nem konkrét kibertámadás, hanem egy komoly sérülékenység, a Log4j, illetve Log4Shell rengette meg ismét a kiberbiztonság világát. Az alapproblémát egy évekkel korábban naplózási segédeszközként, azaz az informatikusok munkájához mintegy kényelmi szolgáltatásként az Apache könyvtárstruktúrájába épített Log4j elnevezésű megoldás okozta (amelyről aztán a sérülékenység a nevét kapta). Ez a gyakorlatban egy könyvtárat jelent, amelyet számtalan Java-alapú alkalmazás használ, alapvetően hibaüzenetek naplózására. Ugyanakkor a napvilágra került sérülékenység révén ezt a szolgáltatást hitelesítés nélkül, távoli eléréssel és kódfuttatással ki lehet használni. Amennyiben ezt egy esetleges támadó valóban ki is tudja használni, akkor rendszerszintű hozzáférést is el tud érni az adott rendszerben. Bár mindez feltételezhetően korábban is ismert volt, mintegy „nulladik napi" sérülékenységként robbant be 2021. december elején a nemzetközi informatikai, majd a világsajtó segítségével az általános köztudatba. Számos incidenskezelő és egyéb szakmai szervezet, így a hazai Nemzeti Kibervédelmi Intézet is azonnal riasztást, ezzel párhuzamosan pedig az Apache-közösség, valamint az olyan nagy hardver- és szoftvergyártók, amelyek eszközei, illetve rendszerei használják a Log4j-t, nagyon gyorsan

[101] NATO (2021): i. m. 3. pont.

javítócsomagokat adtak ki a sérülékenységre. Természetesen ezek telepítése időt és nem kevés energiát igényelt a rendszereket üzemeltetők részéről.[102]

2.5. A kiberműveletek célpontjai

A kibertéri műveletek rendkívül komplexek: nemcsak céljaikban és célpontjaikban, hanem többek között ezek eltérő védelmi mechanizmusainak köszönhetően eszközrendszerükben is rendkívül nagy változatosságot mutatnak. A kiberhadviselés elemzése során az sem mellékes tehát, hogy – nagyon leegyszerűsítve – mit is nevezünk kiberfegyvereknek, illetve ezek a gyakorlatban mit jelentenek. Bár a fentiekben bemutatott kibertámadások alapján nem nehéz arra a kérdésre választ kapnunk, hogy mik lehetnek a kiberhadviselés, illetve az ebben foglalt kiberműveletek célpontjai (nagy bizonyossággal a kritikus infrastruktúrák és a közigazgatás), a válasz nem mindig ennyire egyértelmű és világos. A célpontok az elkövető szándékától, motivációjától és nem utolsósorban képességeitől is függenek.

Természetesen a fentiek alapján a kiberhadviselés, illetve a kiberműveletek célpontjai meglehetősen széles skálán mozognak. Ahogy korábban már megfogalmaztuk, a két legfontosabb irány: *a)* a hadseregek vezetése és irányítása, valamint a fegyverirányítási rendszerek; *b)* a civil rendszerek az említett kritikus infrastruktúrákkal, illetve kritikus információs infrastruktúrákkal, valamint a közigazgatással.

Ez persze nem jelenti azt, hogy az egyéni felhasználók ne lennének célpontok. Ennek több okát is meg lehet nevezni. Az első az erőforrások használata. A védtelen vagy nem megfelelően védett számítógépek, legyenek azok egyszerű otthoni munkaállomások vagy akár IoT-eszközök az okosotthonainkban, hatalmas erőforrásokat jelentenek abban az esetben, ha megfelelő számban állnak támadók rendelkezésére. Minél nagyobb számban áll ugyanis rendelkezésre olyan megfertőzött, kompromittált számítógép – természetesen a felhasználó tudomása nélkül – a támadó irányítása alatt, annál nagyobb műveletet és annál kiterjedtebben tud végrehajtani. Az otthoni munkaállomások kapacitása ezek számossága miatt összeadódik, így összesítve nagy erőforrást jelentenek a támadó számára. Ez már nem elsősorban az elosztott túlterheléses támadásokhoz szükséges, hiszen azok ma már viszonylag kis számú végponttal is hatékonyan elkövethetők,

[102] Nemzeti Kibervédelmi Intézet: *Riasztás Apache Log4j könyvtárt érintő kritikus sérülékenységgel kapcsolatban* (2021. december 12.).

köszönhetően a nagy sávszélességű hálózati eléréseknek, hanem például az olyan nagy számítási kapacitást igénylő műveletekhez, mint egy titkosítás feltörése vagy jelszó megfejtése. Utóbbi esetben például az úgynevezett *brute-force* (magyarul: nyers erő) technológia alkalmazásához szükséges mindez, amikor is a támadó nem a titkosítás dekódolását végzi el, hanem számtalan jelszóvariációt próbál ki és hasonlít össze a beállított jelszó „kitalálása" érdekében.

Egy másik ok, amiért az egyéni felhasználó célpont lehet, az, amikor a támadó már nem véletlenszerűen választ ki puszta erőforrásokat, hanem nagyon is tudatosan olyan felhasználót vesz célba, aki fontos adatok birtokában van, vagy kulcsfontosságú szereplő egy adott szervezeten belül, így rajta keresztül annak – egyébként esetleg jól védett – rendszerébe jóval kisebb erőfeszítéssel tud behatolni, mint ha közvetlenül támadná meg. A célpont tudatos kiválasztása a róla szóló információgyűjtéssel kezdődik, amely műveletben hatalmas segítség az, hogy a felhasználók jelentős része nagyon sok olyan információt is megoszt saját magáról vagy akár az adott szervezetről – főként a közösségi médiában, de sokszor a szervezet welapján is –, amely nagyon jó kiindulópontot jelent a támadás módszereinek és eljárásainak összeállításához. A már említett *spear-phishing* támadások jelentős részében az ezek elindításához szükséges olyan információk, mint például a célszemély napi tevékenysége, munkatársi kapcsolatai, szokásai stb., hatalmas segítséget jelentenek a támadónak.

Visszatérve a kritikus infrastruktúrákra, illetve a kritikus információs infrastruktúrákra mint célpontokra, gyakran felmerül a kérdés, hogy kell-e számolni például atomerőművek elleni kiberakciókkal, vagy esetleg vannak más hatékony módszerek egy ország energiaellátásának megtámadására. A válasz ismét csak összetett, hiszen a Stuxnet esetében láthattuk, nem lehetetlen a nukleáris létesítmények elleni kibertámadásokat kivitelezni, de ezek olyan nagy erőforrásokat igényelnek a felkészülés, a célpontkiválasztás, a tesztelés és a végrehajtás során, hogy gyakorlatilag nem éri meg ebben gondolkodni egy államnál kisebb szervezetnek. Másként fogalmazva, ezek a létesítmények – a pénzügyi és banki rendszerek mellett – a legjobban védett infrastruktúrák, mind fizikai, mind kibervonatkozásbant. (A pénzügyi rendszerek esetén persze él az a hamis vagy téves kép, hogy a kiberbűnözői csoportok a bankokat, illetve a pénzügyi szolgáltatókat támadják, de az esetek túlnyomó többségében ez nem így van. A kiberbűnözés első számú célpontja az ügyfél, hiszen ő sokkal kisebb erőforrással és sokkal sikeresebben támadható, mint a nagy anyagi és technikai erőforrásokkal rendelkező bank vagy pénzügyi szervezet, amely nagyon erős védelmet képes kiépíteni és fenntartani ezek birtokában.)

A fenti kérdésre adandó válasz azért sem egyértelmű, mert vannak olyan kritikus infrastruktúrák elleni támadások, amelyek a rendszerekben, illetve rendszerelemekben meglévő, már említett intra- vagy interdependencia révén közvetett módon fejtik ki hatásukat. Erre az egyik igen jó példa az Irán atomlétesítményei ellen elkövetett 2021-es támadás. A Stuxnettel elkövetett 2010-es kibertámadással ellentétben ez már nem a kibertérben, hanem a fizikai térben valósult meg: a natanzi atomdúsító komplexumot elektromos árammal ellátó erőműben történt robbantásos szabotázs. Sajtóhírek szerint két robbanás tette tönkre az egymástól független, nagyon jól védett natanzi belső energiaellátó rendszert, amely a föld alatti urándúsító centrifugákat is kiszolgálta. A támadás sikeres volt, és komoly termelési (működési) kiesést eredményezett Irán urándúsító kapacitásában.[103] Ez az eset tehát nagyon jól rávilágít arra a tényre, hogy akár kibertámadásokkal, akár a fizikai térben elkövetett támadásokkal az egymásra épülő infrastruktúrákban, illetve az általuk megvalósuló szolgáltatásokban komoly károk okozhatók.

A következő táblázat a kibertámadások célpontjainak az elmúlt 3 évben bekövetkezett változásait mutatja be.

4. táblázat: Kibertámadások célpontjai ágazatonként 2018 és 2020 között

Helyezés	2018	2019	2020
1.	Pénzügy	Média, szórakoztatás	Üzleti, szakmai szolgáltatások
2.	Üzleti, szakmai szolgáltatások	Pénzügy	Kiskereskedelem, vendéglátás
3.	High-tech ipar	Kormányzat	Egészségügy
4.	Kiskereskedelem, vendéglátás	Üzleti, szakmai szolgáltatások	Pénzügy
5.	Média, szórakoztatás	High-tech ipar	High-tech ipar
6.	Oktatás/kormányzat	Műszaki gyártás	Műszaki gyártás
7.	Egészségügy	Média, szórakoztatás	Média, szórakoztatás
8.	Műszaki gyártás	Egészségügy	Telekommunikáció
9.	Energia	Energia	Oktatás
10.	Szállítás, logisztika	Szállítás, logisztika	Kormányzat

Forrás: FireEye–Mandiant (2021): i. m. alapján a szerző szerkesztése

[103] Ronen Bergman – Rick Gladstone – Farnaz Fassihi: Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage. *The New York Times,* 2021. április 11.

A kiberműveletek célpontjainak következő nagy csoportja a közigazgatás. Közigazgatás nélkül szintén nagyon nehéz elképzelni a fejlett nyugati társadalmakat. Az ellene indított támadások jelenlegi trendjeként az információszerzésre irányuló műveleteket lehet felfedezni. Ezek a műveletek jól körülírható APT-csoportokhoz[104] köthetők, az így megszerzett információk pedig elsősorban politikai és gazdasági jellegűek, ami előrevetíti kiberhadviselés céljára történő későbbi esetleges felhasználásukat.

2.6. Kiberműveletek stratégiai szinten

2.6.1. Megváltozott hadviselés

A kiberműveleteket, illetve az ezek által kialakuló, tágabb értelmű kiberhadviselést mint fogalmat szükséges elhelyezünk a hadviselés rendszerének egészében. Ehhez korábban megvizsgáltuk a hadseregek – többek között a digitalizáció miatt bekövetkezett – változásait, valamint a hadviselés azon részének fejlődését, amely a kiberhadviseléssel valamilyen összefüggésben áll. Ezeken kívül szükséges még, hogy nagyon röviden kitérjünk azokra a hadviselési módokban bekövetkezett változásokra, amelyeknek az elmúlt időszakban tanúi lehetünk.

A már bemutatott multitér-, illetve az elosztott műveletek mellett számos egyéb olyan jellemzővel rendelkezik napjaink hadviselése, amelyeket érdemes górcső alá vennünk. Az első ilyen jellemző alapvetően a biztonság- és védelempolitika egyik legmarkánsabb 21. századi vonására vezethető vissza, amely nem más, mint az országok közötti konfliktusok fegyveres összecsapások szintje alatt tartása. Ez a nyílt fegyveres konfliktus elkerülését jelenti úgy, hogy közben úgynevezett szürke zónás műveletek zajlanak. Ezek a „már nem béke, de még nem is háború" elvű összecsapások a háttérben, sok esetben az átlagember számára láthatatlanul zajló különféle műveletek rejtenek. Így ír róluk az Egyesült Államok kiberparancsnokságánaka vezetője: „Az ellenség folyamatosan

[104] Az APT *(advanced persistent threat),* azaz folyamatosan fennálló, nagyon fejlett támadások kivitelezésére ma már elsősorban állami vagy államilag támogatott csoportok jöttek létre. Az APT-támadások jellegét jelen könyv későbbi részében elemezzük.

a fegyveres konfliktus szintje alatt tevékenykedik abból a célból, hogy meggyengítse intézményeinket, és stratégiai előnyökre tegyen szert."[105]

A szürke zónás műveletekhez nagyon hasonlóak a hibrid műveletek. Ezekre is igaz, hogy a támadók igyekeznek őket (köztük a kibertámadásokat is) a háborús küszöb alatt tartani, vagyis kerülik a nyílt, fegyveres összecsapásokat, s inkább olyan műveleteket és olyan intenzitással hajtanak végre, amelyek sem önállóan, sem hatásukat összegezve nem csapnak át még nyílt, fegyveres konfrontációba.

A hibrid műveletek, mint ahogy az elnevezés is mutatja, a hagyományos katonai és nem katonai műveletek jól megtervezett együttes sorozatát jelentik.[106] Ezek során a különböző tevékenységek végrehajtásához az egyik legfontosabb és talán leghatékonyabb eszköz a kibertér, amelyet közvetítő közegként használnak fel a célok eléréséhez. Ezek a műveletek jól felépített forgatókönyv alapján, egymás hatásait erősítve, azokat szisztematikusan felhasználva zajlanak. Közéjük pedig nagyon gyakran beépülnek a közösségi médiumokon keresztüli befolyásolás műveletei, a propagandatevékenységek, és sok esetben maguk a célzott kibermműveletek is.

Egy következő hadviselési mód – vagy ha tetszik, fogalom –, amely nem is teljesen új, mégis napjainkban a hibrid műveletekkel együtt kapott újabb értelmezést, a már szintén említett információs műveletek. Ilyen műveletek alapvetően az 1990-es évek közepe, illetve második fele óta jelen vannak a hadviselésben. A hadtudomány is komoly irodalommal rendelkezik erről a fogalomról, illetve tevékenységről, mind nemzetközi, mind hazai vonatkozásban.

A jelenlegi hivatalos hazai katonai megfogalmazás szerint az információs műveletek meghatározása a következő:

> „[a]z a törzsfunkció, melynek célja, hogy az információs környezet elemzése alapján megtervezze és integrálja, majd értékelje az információs tevékenységeket úgy, hogy azok végrehajtása biztosítsa a kívánt hatás elérését a célközönség akaratában, megértésében és képességeiben a küldetés célkitűzéseinek elérése érdekében. A célközönséget a szemben álló felek, a lehetséges szemben álló felek és más, a politikai szint által jóváhagyott személyek és meghatározott csoportok alkotják."[107]

[105] United States Cybercommand: *Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command* (2018. április).

[106] Kiss Álmos Péter: A hibrid hadviselés természetrajza. *Honvédelmi Szemle,* (2019), 4. 17.

[107] *Információs műveletek doktrína* (2014). 8.

Leegyszerűsítve: minden olyan képesség, amely a kinetikus energián alapuló hagyományos fegyvereken kívüli eszközök összehangolt és koordinált alkalmazását foglalja magában.

Haig megfogalmazásában az információs műveletek jelentése a következő:

> „Az információs környezetben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében kognitív képességekkel közvetlenül, illetve technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire."[108]

A fenti definíciókban megfogalmazottakat összefoglalva kijelenthetjük, hogy az információs műveletek katonai értelemben hozzájárulnak és támogatják a szárazföldi erők, a légierő és a különleges rendeltetésű erők, sőt még a logisztikai erők kinetikus tevékenységeit azokkal a nem kinetikus műveletekkel, amelyeknek egyik központi eleme az információ. Az információs műveletek azokra a folyamatokra hatnak, amelyek az információ összegyűjtését, feldolgozását, továbbítását és felhasználását foglalják magukban. Ebben az értelmezésben az információs műveletek magára a vezetésre is hatással vannak, hiszen a vezetés során pont az említett információs folyamatok zajlanak.

5. táblázat: Az információs műveletek elemei

Kiberműveletek (számítógép-hálózati műveletek): – védelmi célú kiberműveletek – támadó célú kiberműveletek	Cyberspace operations (computer network operations, CNO): – defensive cyber space operations – offensive cyber space operations
Elektronikai hadviselés	Electronic warfare (EW)
Lélektani műveletek	Psychological operation (PSYOPS)
Civil-katonai együttműködés	Civilian-military cooperation (CIMIC)
Tömegtájékoztatás/-kommunikáció	Military public affairs (MilPA)
Műveleti biztonság	Operations security (OPSEC)
Katonai megtévesztés	Military deception (MILDEC)
Megjelenés, viselkedés, arculat	Presence, posture, profile (PPP)
Kapcsolattartás kulcsvezetőkkel	Korábbi megnevezéssel: key leader engagement (KLE)

Forrás: az AJP-3.20 alapján a szerző szerkesztése

[108] Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018. 15.

A mai, egyre gyakrabban a média hatására jelentkező értelemben az információs műveletek a befolyásolási céllal végrehajtott, alapvetően stratégiai, tehát ország és ország vagy ország és nemzetközi szervezet között végrehajtott műveleteket jelentik. Ugyanakkor a fogalom lényege nem változik, sőt elemei is ugyanazok mindkét értelmezésben. Az információs műveletek elemei között kitüntetett helyen megtaláljuk a kiberműveleteket, korábbi megnevezéssel élve számítógép-hálózati műveleteket is. Az információs műveletek elemeit mutatja be a fenti táblázat azok angol megnevezésével együtt.

2.6.2. Kiberstratégia

A kiberműveletek és a kiberhadviselés eddig bemutatott fontossága miatt ma már az országok jelentős része stratégiai szinten igyekszik meghatározni mindazokat a tevékenységeket, amelyek az adott ország vonatkozásában a terület biztonságának megteremtése érdekében szükségesek.

A fejlett országok a nemzeti biztonsági stratégiáikban rögzítik azokat a célokat, amelyek a biztonság vonatkozásában kiemelten fontosak. A klasszikus biztonságidokumentum-hierarchia az adott ország nemzeti biztonsági stratégiájából kiindulva ágazati stratégiákat alkot meg. Ilyen stratégia többek között az adott ország katonai vagy éppen a kiberbiztonsági stratégiája.

Ugyanakkor vannak olyan elképzelések, amelyek ezen túlmenően a kibertér globalitása miatt nem látják elégségesnek a nemzeti stratégiákat, az azokban – egymáshoz nagyon hasonló, de mégiscsak nemzeti szinten és hatáskörrel – megfogalmazott stratégiai célokat. „[A]z egyes országok saját útkeresése mellett meg kell hogy jelenjen egy […] globális elképzelés is, amely mentén az előbb említett kihívások és veszélyek egységesen és hatékonyan kezelhetők."[109]

A különböző országok nemzeti kiberbiztonsági stratégiáinak felépítése változatos képet mutat. Ugyanakkor ezekben a stratégiai dokumentumokban számos azonos vagy hasonló elem felfedezhető, és elkészítésükhöz szerencsére ma már rendelkezésre állnak nemzetközi jó gyakorlatokon alapuló ajánlások.[110] A stratégiák általában az adott országra jellemző helyzetkép felvázolásával kezdődnek, számba véve mindazokat a kihívásokat és veszélyeket, amelyek a kibertérben

[109] Kovács László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus Kiadó, 2018c. 25.
[110] European Union Agency for Cybersecurity: *National Cybersecurity Strategies: With a Vision on Raising Citizens' Awareness* (2021c. november 29.).

vagy a kibertéren keresztül az adott ország társadalmi és gazdasági folyamatait fenyegetik. Ezekhez az értékelésekhez ma már szintén rendelkezésre állnak nemzetközi ajánlások,[111] és a kibertér sajátosságai miatt a nemzeti szintű értékelések természetszerűleg a nemzetközi környezet értékelését is tartalmazzák.

A feltárt kibertéri veszélyek után a stratégiák általános eleme azon stratégiai célok meghatározása, amelyek a kibertéren túl a nemzet egészének biztonságához járulnak hozzá. A legújabb nemzeti kiberbiztonsági stratégiák pedig a stratégiai célok eléréséhez szükséges erőforrásokat – humán és anyagi erőforrásokat egyaránt –, valamint a szükséges szervezeti struktúrát és annak működését is meghatározzák.

Egy-egy nemzeti kiberbiztonsági stratégia önmagában is nagyon előremutató, azonban ha ehhez még egy olyan cselekvési vagy akcióterv is hozzákapcsolódik, amely alapján a stratégia végrehajtásának sikeressége vagy esetleges sikertelen pontjai, intézkedései mérhetővé válnak, akkor az adott országban már nagy valószínűséggel kialakítható a kiberbiztonságnak egy magasabb szintje.

Hazánk 2020-ban megjelent – jelenleg legújabb – nemzeti biztonsági stratégiája már jóval markánsabban tartalmazza a kibertér kihívásait, az ezekre adandó válaszokat, a felkészülést és a katonai kiberműveletek szükségességét is, mint a korábbi, 2012-es nemzeti biztonsági stratégia. Mindezt jól mutatja, hogy

> „a 2012-es Nemzeti Biztonsági Stratégia a hazánkat érintő biztonsági fenyegetések, kihívások és azok kezelésének számbavétele, illetve meghatározása során a kiberbiztonságot már mint önálló területet határozza meg. Ugyanakkor a kiber kifejezés összesen csak hat alkalommal szerepelt a dokumentumban. Ezzel szemben az új, 2020-as Nemzeti Biztonsági Stratégiában már 33 alkalommal találkozunk vele különböző kontextusokban. Talán ez a statisztikai szám is igazolja a kiberbiztonság és a kiberműveletek elmúlt időszakban megnövekedett szerepét és jelentőségét."[112]

Stratégiai szempontból hazánk fent említett új nemzeti biztonsági stratégiájában a kiberbiztonság és a kiberműveletek vonatkozásában talán az egyik legfontosabb kitétel a következő: „Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek,

[111] European Union Agency for Cybersecurity: *Methodology for Sectoral Cybersecurity Assessments EU Cybersecurity Certification Framework* (2021b. szeptember).

[112] Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új nemzeti biztonsági stratégiájában. *Honvédségi Szemle,* 148. (2020), 5. 4.

alkalmazásukat fegyveres agressziónak tekinti, amelyre a fizikai térben megvalósuló válaszadás is lehetséges."[113]

A hazai, szintén új, 2021-ben megjelent nemzeti katonai stratégia – természetesen építve a nemzeti biztonsági stratégiában megfogalmazott elvekre és stratégiai célokra – a kibertér katonai vonatkozásait szintén kiemelten kezeli. Megfogalmazásában a kibertér, hasonlóan a hagyományos fizikai terekhez, azaz szárazföldhöz, a levegőhöz, illetve a tengerekhez, műveleti térként értelmezhető: „Egy potenciális európai hadszíntéren vívott háború során szerepet kaphatnak, illetve célponttá is válhatnak Magyarország kommunikációs és közlekedési infrastruktúrái, valamint más létfontosságú rendszerelemei, emiatt az ország teljes területe, légtere és kibertere katonai műveletek színtere lehet."[114] Erre azonban fel kell készülni. Ennek megfelelően a stratégia a Magyar Honvédség számára többek között a következőket határozza meg:

> „A katonai kibertérműveleti erők a kibertérben végrehajtott műveleteikkel, beleértve az offenzív műveleteket is, hozzájárulnak a szárazföldi erők és a légierő kinetikus műveleteinek hatékonyságához. Békében aktívan közreműködnek a nemzeti kibervédelmi feladatokban, valamint felkészülnek a különleges jogrendi helyzetben történő feladatvégrehajtásra."[115]

Hasonlóan a nemzeti biztonsági stratégiához a katonai stratégia is bizonyos esetekben fegyverként értékeli a hazánk ellen irányuló kiberműveleteket, illetve az azokban alkalmazott információtechnológiai eszközöket. Erről így ír a stratégia:

> „Ellenérdekelt állami szereplők az információs technológia eszközeivel a Magyar Honvédség vezetés-irányítási rendszerének megbénítására vagy működésének akadályozására is törekedhetnek. Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat pedig akár fegyveres támadásnak tekinti, amelyre adott esetben katonai válaszadás is lehetséges."[116]

Ez a fenti megfogalmazás el is vezet minket a következő stratégiai megfontolásig, amely nem más, mint az elrettentés. A NATO a 2010-es évek óta egyre inkább az elrettentés (fizikai elrettentés) politikájával él, sőt a szövetség stratégiai

[113] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. 101. pont.
[114] 1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról, 1.
[115] 1393/2021. (VI. 24.) Korm. határozat, 5.1.
[116] 1393/2021. (VI. 24.) Korm. határozat, 2.

koncepciója a védelem mellett az elrettentést is kiemelt helyen kezeli.[117] Korábban, a hidegháborúban az elrettentés alapvetően a nukleáris elrettentő erőre épült, de a hidegháború végével, illetve az új típusú fenyegetések megjelenésével az ezekre adandó egyfajta válaszként a 21. század kezdetén az elrettentés intézménye ismét előtérbe került. Az elrettentés tehát ma a NATO stratégiájában is nagyon hangsúlyos szerepet kap,[118] azonban már nem a nukleáris, hanem a hagyományos fegyverekre és katonai erőkre alapozva jelenik meg.[119]

Ezek után logikus kérdésként merülhet fel, hogy működik-e a kibertérben az elrettentés. Hiszen a kibertéri elrettentés mint fogalom sokáig nem is volt használatos a nemzetközi szakmai közösségben, illetve a szakirodalom sem számolt ezzel reális tényként. Ma már azonban számos ország – ahogy a fentiekben bemutattuk, hasonlóan hazánkhoz – stratégiai dokumentumaiban foglalkozik ezzel a kérdéssel,[120] így a kiberelrettentés sok országban bizony markánsan megjelenik.[121] Az Egyesült Államok korábbi, 2015-ben a Védelmi Minisztérium által jegyzett kiberstratégiájában például így fogalmazták meg a kibertéri elrettentést: „A fokozódó fenyegetés, amellyel szembe kell néznünk, szükségessé teszi, hogy a Védelmi Minisztérium átfogó kiberelrettentési stratégiát dolgozzon ki és ültessen át a gyakorlatba, s ezáltal megakadályozza a nagy állami és nem állami szereplőket az amerikai érdekek elleni kibertámadások elkövetésében."[122]

A kibertéri elrettentés egyik megvalósulási formája az, amikor egy ország nemcsak az említett stratégiáiban mutatja be, hanem építi, sőt nyilvánosságra is hozza kibertámadó képességét. Így tett például Németország, amikor a NATO számára felajánlotta kibervédelmi és kibertámadó képességeit is.[123] A NATO kibertámadó képességeivel kapcsolatban azonban le kell szögezni, hogy erre a szervezet mint a tagállamok által önkéntesen felajánlott képességekre tekint, hiszen önállóan nincsenek ilyen képességei, hanem csak a tagországok révén állnak rendelkezésére. A NATO ezt a szuverén kiberképességek önkéntes

[117] NATO: *Active Engagement, Modern Defence Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation Adopted by Heads of State and Government in Lisbon* (2010. november 19./2022. július 1.).

[118] NATO: *Deterrence and Defence* (2022b. július 6.).

[119] Kovács (2018a): i. m. 52.

[120] Kovács (2018a): i. m. 52.

[121] Kovács (2020): i. m. 23.

[122] The Department of Defence: *The DoD Cyber Strategy* (2015. április). 10.

[123] Pierluigi Paganini: Germany Makes its Cyber Capabilities Available for NATO Alliance. *Security Affairs,* 2019. február 15.

szövetségesi átadása (*Sovereign Cyber Effects Provided Voluntarily by Allies,* SCEPVA) mechanizmusának nevezi.[124]

A kibertéri elrettentés több elemből kell hogy álljon, illetve réteges szerkezetűnek kell lennie,[125] amelyben az egyik fontos összetevő az ellenálló, erős és megbízható kibervédelem. Ez hozzájárul ahhoz, hogy a szemben álló félnek olyan aránytalanul nagy energiabefektetést kelljen kifejtenie a védelmi mechanizmusaink áttörésére, amely már nem éri meg számára. Így a kibervédelem szintén elrettentésként funkcionál. Az elrettentési eszköztár további összetevője lehet (a fent említett offenzív képességek kialakításán és folyamatos fenntartásán túl) – ahogy az a magyar nemzeti biztonsági stratégiában is megjelenik – a kibertámadásokra akár a fizikai térben megvalósuló válasz kilátásba helyezése, valamint az attribúció is. Ahogy korábban láthattuk, az attribúció az adott kibertámadás elkövetőjének nyilvános megnevezését jelenti. Ezt akkor lehet megtenni, ha 100%-os bizonyossággal megállapított bizonyítékokkal lehet alátámasztani az elkövető kilétét. Azonban ez sok esetben már technikailag is rendkívül nehéz. A magyar nemzeti biztonsági stratégia így hivatkozik erre a tényre: „A kiberműveletek sokszor nehezen bizonyítható attribúciójára, az elkövető azonosítására, megnevezésére való tekintettel a válaszlépések különösen körültekintő, eseti elbírálást igényelnek az érintett kormányzati szervezetek bevonásával."[126]

Működhet-e tehát az elrettentés a kibertérben? A válasz nem egyértelmű, azonban a fenti elemek az attribúcióval párhuzamosan alkalmazva valódi és hatékony eszközt jelenthetnek a szemben álló fél rosszindulatú kibertevékenységeivel szemben.

A kiberképességek, köztük az offenzív kiberképességek fentiekben is említett nyilvánosságra hozatala alapján, azt kiegészítve számos egyéb mutatóval – például annak vizsgálatával, hogy van-e az adott országnak kiberbiztonsági stratégiája, milyen szintű a kiber-ellenállóképesége, van-e kiber-felderítőképessége, illetve milyen a kiberképességekhez szükséges humán erőforrás az adott országban – összehasonlíthatóvá válnak az egyes országok. Ez alapján néhány ország kiberfejlettségi rangsorolását mutatja be a következő táblázat.

[124] AJP-3.20. 16.

[125] National Security Archive: *Cyber Brief: Cyberspace Solarium Commission Recommendations in the FY21 National Defense Authorization Act* (2020. december 21.).

[126] 1163/2020. (IV. 21.) Korm. határozat. VI.101.

6. táblázat: Országok kategorizálása kiberképességeik alapján

Szint	Ország
Első szint (világvezető minden kategóriában)	Amerikai Egyesült Államok
Második szint (világvezető néhány kategóriában)	Ausztrália, Kanada, Kína, Franciaország, Izrael, Oroszország, Egyesült Királyság
Harmadik szint (erősség vagy potenciális erősség néhány kategóriában, de jelentős gyengeség több kategóriában)	India, Indonézia, Irán, Japán, Malajzia, Észak-Korea, Vietnám

Megjegyzés: a szinteket a következő szempontok határozták meg: 1. stratégia és doktrína; 2. vezetés és irányítás; 3. kiberhírszerzési képességek; 4. kibertéri lehetőségek és függőség; 5. kiberbiztonság és ellenálló képesség; 6. globális vezető szerep a kibertéri ügyekben; 7. támadó kiberképességek.
Forrás: International Institute for Strategic Studies: *Cyber Capabilities and National Power: A Net Assessment* (2021. június 28.) alapján a szerző szerkesztése

2.6.3. Kiberdiplomácia – a jog és az államok szerepe

Jelenleg a kiberműveletek, illetve a kiberhadviselés területének az egyik legnagyobb kihívása a jog, a jogi szabályozás, pontosabban annak hiánya. Abban ma már az országok és a nemzetközi szervezetek jelentős része egyetért, hogy a nemzetközi jog alkalmazása elkerülhetetlen a kibertéri tevékenységek, így a kiberműveletek során is. Ennek mikéntje azonban a kibertér jellegéből adódóan nem teljesen egyértelmű. Jelen könyvünk nem tűzte ki célul a kiberbűnözés és jogi szabályozottsága vizsgálatát, de mindenképpen szükséges egy mondatban kitérni erre a területre is, mielőtt a kiberműveletek jogi hátterét megvizsgálnánk.

A kiberbűnözés ellen már 2001-ben nemzetközi megállapodás született, amelyet Budapesten írtak alá. Az azóta eltelt időben azonban számos olyan változás történt a kibertérben és az ott elérhető szolgáltatásokban, amelyek azt igényelnék, hogy ezt a budapesti egyezményt újratárgyalja a nemzetközi közösség. Ugyanis

> „sajnálatos módon a kiberbűncselekmények vonatkozásában a jogalkotás és ennek megfelelően sokszor maga a jogalkalmazás jelenleg a legjobb esetben is csak követi az eseményeket. Ennek okait értelemszerűen több helyen és több tényezőben kell keresnünk. Az egyik ilyen összetett ok a nemzetállamok eltérő jogalkotási és jogalkalmazási gyakorlatában keresendő. Ez még az olyan – elvileg egységes jogi háttérrel rendelkező – nemzetközi szervezeten belül is igaz, mint az Európai Unió."[127]

[127] Kovács (2018b): i. m. 195.

A kiberműveletek és a kiberhadviselés területének jogi szabályozását már több alkalommal is megpróbálta a nemzetközi közösség felmérni. Az egyik ilyen, azóta is gyakran hivatkozott tanulmány az úgynevezett *Tallinni kézikönyv (Tallinn Manual),* amelyet a NATO már említett tallinni Kibervédelmi Kiválósági Központja szervezésében egy nemzetközi kutatókból álló csapat készített 2013-ban,[128] majd 2016-ban *Tallinn Manual II* címen ezt aktualizálták.[129]

A nemzetközi jog hatalmas kihívásokkal küzd a kiberműveletek és a kiberhadviselés területén, mert „amíg a hagyományos fegyveres konfliktusokra már nagyon régóta szigorú és az egész világra kiterjedő nemzetközi hadijogi (vagy másnéven humanitárius jogi) szabályozás létezik […], a kiberhadviselésre jelenleg nem találunk egy az egyben alkalmazható nemzetközi jogi szabályokat".[130]

Mindezen problémákra az említett *Tallinni kézikönyv*ek is felhívták a figyelmet. Ilyen probléma például annak a megfogalmazása, hogy egyáltalán mit értünk hadviselésen a kibertérben, illetve az állami támogatású csoportok azonosak-e az adott országgal. Egy másik problémacsoport olyan kérdéseket tartalmaz, mint például hogy bevonhatók-e semleges felek a katonai műveletekbe, vagy megtámadhatók-e az olyan kritikus infrastruktúrák, mint a kórházak vagy az egészségügyi létesítmények.

A nemzetközi jog a hadviselés területére vonatkozóan olyan elveket fektetett le korábban, mint például az arányosság elve, illetve a katonai és civil célpontok szétválasztásának elve. Óriási kérdés, hogy ezek a korábban már jól bevált elvek alkalmazhatók-e a kibertérben, hiszen ezek mellett stratégiai szinten olyan kérdések is megjelennek, mint hogy „[t]ekinthető-e egy kibertérben kivitelezett támadás az ENSZ Alapokmány 51. cikke szerinti fegyveres támadásnak, ha igen, akkor az állam önvédelmi jogosultsága meddig terjed, használhat-e hagyományos fegyvereket az önvédelem során".[131]

Az államok felelős szerepére hívja fel a figyelmet az Amerikai Egyesült Államok Német Marshall Alapjának támogatásával elkészült tanulmány. Ebben a szerzők megvizsgálva többek között az olyan nemzetközi szervezetek, mint az ENSZ vagy az EBESZ állami támogatású kibertámadásokkal kapcsolatos

[128] Michael N. Schmitt (szerk.): *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York, Cambridge University Press, 2013.

[129] Michael N. Schmitt (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* New York, Cambridge University Press, 2016.

[130] Kovács (2018b): i. m. 273.

[131] Kelemen Roland – Pataki Márta: A kibertámadások nemzetközi jogi értékelése. *Katonai Jogi és Hadijogi Szemle,* (2015), 1. 54.

gyakorlatát – és nyugodtan hozzátehetjük: egyelőre nem túl sikeres problémakezelését – a következőket írják: „A továbblépés egy új, semleges nem kormányzati szervezet létrehozása lehet, amely kivizsgálná a kibertámadásokat, és összegyűjtené a szükséges technikai bizonyítékokat, amelyek alapján nyilvánosan megnevezhető lenne a támadó."[132] Ez egyrészt utal arra, hogy egy államok felett álló, azok érdekeitől független szervezetet szükséges létrehozni, másrészt már önmagában ez a tény, hogy az államok kibertéri támadótevékenységeit egy független szervezet felügyelné, egyfajta elrettentő erő lehet. Másképpen megfogalmazva, mindezek hozzájárulhatnak az államok egyre inkább felelős magatartásához és tevékenységéhez a kibertérben.

2019 szeptemberében közel egy tucat állam, köztük Magyarország is, közös nyilatkozatot adott ki az államok felelős kibertéri szerepvállalásáról, amelyben kifejezték abbéli elkötelezettségüket, hogy minden olyan előny és előremutató tényező, amelyet a kibertér a 21. században biztosít a társadalmak számára, megvédendő. Úgy fogalmaztak:

> „Felelős államokként, amelyek fenntartják a nemzetközi szabályokon alapuló rendet, elismerjük szerepünket a szabad, nyitott és biztonságos kibertér előnyeinek megőrzésében a jövő generációi számára. Ha szükséges, önkéntes alapon együtt fogunk működni annak érdekében, hogy az államokat felelősségre vonjuk, ha ezzel a kerettel ellentétes módon cselekszenek, többek között átlátható és a nemzetközi joggal összhangban álló intézkedések meghozatalával. A kibertérben tanúsított rosszindulatú és ártó szándékú viselkedésnek következményekkel kell járnia."[133]

Ezt megelőzően már 2019-ben született egy francia kezdeményezés, amelyhez azóta közel 80 ország csatlakozott. Ez az úgynevezett *párizsi felhívás,* amely a kibertéri bizalom és biztonság erősítését tűzte ki célul a lehető legszélesebb nemzetközi összefogást előirányozva. A kezdeményezéshez 2021-ben az Európai Unió és az Amerikai Egyesült Államok is csatlakozott.[134]

Összefoglalva a kibertérben zajló tevékenységek jogi hátterét, valamint az államok szerepvállalását az kijelenthető, hogy egyelőre csak elviekben és nyilatkozatokban formálódó megoldásokat láthatunk.

[132] Bruno Lété – Peter Chase: *Shaping Responsible State Behavior in Cyberspace.* Washington, The German Marshall Fund of the United States, 2018.

[133] US Department of State: *Joint Statement on Advancing Responsible State Behavior in Cyberspace* (2019. szeptember 23.).

[134] Paris Call for Trust and Security in Cyberspace. *Pariscall.international,* 2018. november 12.

A fenti kérdések nagyon nehezek, és a válaszok még nehezebbek lehetnek, azonban a nemzetközi közösségnek mihamarabb meg kell találnia őket, különben a kiberműveletek alkalmazása és így a kiberhadviselés is kontrollálhatatlanná válik.

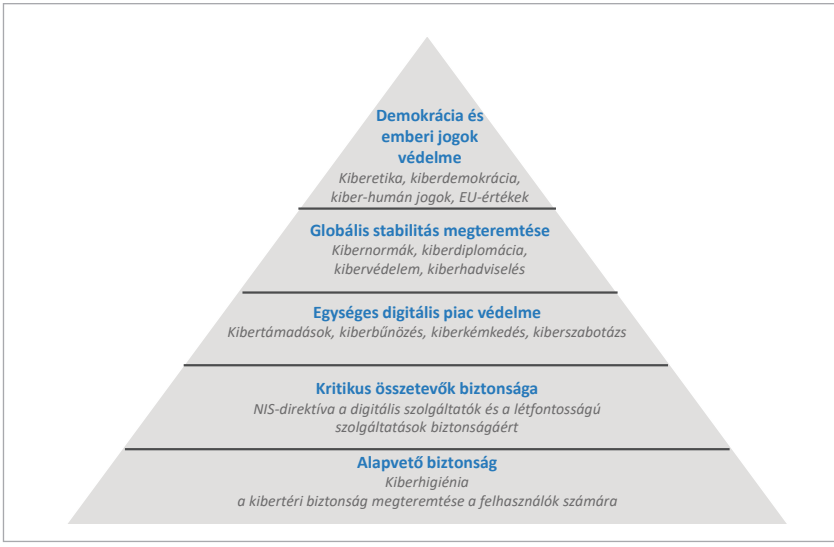
2.7. Ellenálló kiberbiztonság, avagy a kiberreziliencia

A kiberműveletek és a kiberhadviselés realitása számos országot ráébresztett arra, hogy a 21. század kibertéri kihívásai olyan rendszerszintű megközelítést igényelnek, amely komplex módon képes kezelni a felvázolt fenyegetéseket. A cél az, hogy a kibertéri kihívásokhoz, köztük a kiberhadviselés jelentette veszélyekhez alkalmazkodni képes nemzeti kibervédelmi rendszer épüljön ki. Mindezeket ma már az angol megnevezéssel élve adaptív kiber-ellenállóképességnek, kissé magyartalanul kiberrezilienciának nevezzük.

Az ellenállóképes kibervédelem megteremtése össznemzeti feladat. Ebben olyan főbb szereplőket kell együttműködésre bírni, mint a felhasználók, a közigazgatás, a szoftver- és hardvergyártók, a kis-, közepes és nagyvállalatok, az ipari szereplők, a védelmi szféra, a kritikus infrastruktúrák üzemeltetői, valamint az akadémiai szféra. E szereplők együttműködése komoly és nem utolsósorban központi, azaz kormányzati koordinációt igényel, amit általában a nemzeti kiberkoordinátor végez. Sok ország, így Magyarország esetében ez a koordináció mint stratégiai cél bekerült a nemzeti kiberbiztonsági stratégiába is.[135]

A kiberbiztonság megteremtése során figyelembe kell venni a teljes digitális ökoszisztémát, beleértve nemcsak a hazai, hanem a nemzetközi biztonsági összefüggéseket is. Erre a feladatra egy jól áttekinthető, egymásra épülő rendszer elvét dolgozta ki az Európai Unió kiberbiztonsági ügynöksége, az ENISA (European Union Agency for Cybersecurity), amelyet a következő ábrán mutatunk be.

[135] 1139/2013. (III. 21.) Korm. határozat. III. 10. *a)* pont.

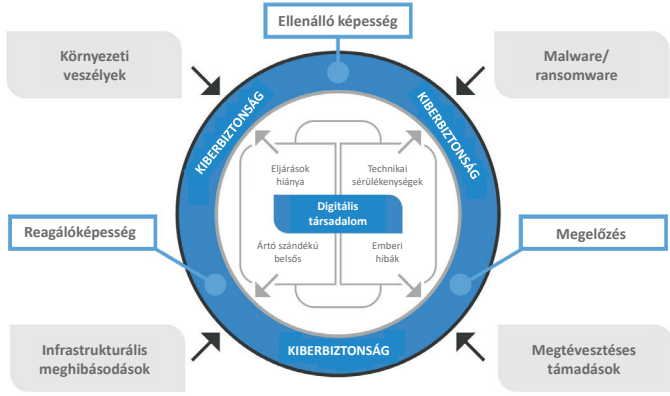


8. ábra: A kiberbiztonság rétegei az ENISA kidolgozásában

Forrás: European Union Agency For Network and Information Security: *ENISA Overview of Cybersecurity and Related Terminology.* 1. változat (2017. szeptember) alapján a szerző szerkesztése

A fentieknek megfelelően a kiberbiztonságnak számos olyan területét tudjuk – többé-kevésbé jól – elkülöníteni, amelyek együtt, az említett komplex módon képesek a kibertéri kihívások teljes vertikumát kezelni. Ezek a területek a teljesség igénye nélkül a következők: kiberdiplomácia és annak eszköztára, nemzeti kockázatmenedzsment, komplex információbiztonság, benne a jól működő elektronikus információbiztonsággal és a nemzeti incidenskezelés rendszerével, valamint a kiberbiztonsági képzés és tudatosságépítés.

Az ellenálló kiberbiztonság – vagy annak gyakran használt angol megfelelőjével élve a *cyber resilience* – az egyik legfontosabb biztonsági kérdéssé vált a digitális társadalomban. Ennek eléréséhez olyan védelmi rendszerek együttműködését kell kialakítani, amelyek a digitális technikai és technológiai kérdésektől kezdve a humán veszélyekig minden kihívásra adaptív módon képesek reagálni. Ennek összetevőit, valamint az összetevők közötti összefüggéseket mutatja be a következő ábra.



9. ábra: Az ellenálló kiberbiztonság főbb összetevői és ezek összefüggései
Forrás: Epp Maaten – Toomas Vaks: *National Cyber Security in Practice*. Tallinn, E-Governance Academy, 2020 alapján a szerző szerkesztése

3. fejezet

Kiberharcosok és kiberparancsnokságok

Az előzőekben bemutatottak arra késztetnek minket, hogy megvizsgáljuk, hol és milyen szervezettel készülnek a kiberműveletekre, illetve milyen humán erőforrásokat és nem utolsósorban milyen eszközöket magukban foglaló kibererőket építenek az egyes országok.

Azt rögtön le kell szögeznünk, hogy – amint azt korábban bemutattuk, a terület egyre inkább stratégiai fontosságúvá válása miatt – nagyon sok ország már az adott állam hadseregének részeként építi a kibererőit. Ugyanakkor számos országban léteznek az úgynevezett állami támogatású csoportok, amelyek hivatalosan nem az adott ország nevében hajtanak végre különböző kibertéri műveleteket (legyen szó információszerzésről, azaz kémkedésről, vagy akár kibertámadásról), de mégis annak politikai, gazdasági és/vagy katonai céljai elérése érdekében teszik mindezt, nem utolsósorban természetszerűleg erős, bár nem mindig hivatalos politikai felhatalmazással.

Léteznek azonban olyan nem állami szereplők, amelyek nem az adott ország politikai vezetésének felhatalmazásával, hanem saját céljaik elérése – elsősorban anyagi haszonszerzés – érdekében hajtják végre akcióikat. Sok esetben ezek a csoportok összemosódnak azokkal a gazdasági csoportokkal, amelyek célja elsősorban szintén az anyagi haszonszerzés, de emellett a konkurenciáról szóló információk – nem mindig legális – megszerzését, valamint az azokkal történő visszaélést célozzák. Itt már eljutunk a kiberbűnözői csoportokhoz is. Ezeknek a csoportoknak a fő célja természetszerűleg az anyagi haszonszerzés, azonban tevékenységeik – hasonlóan az állami támogatású csoportok műveleteihez – elérhetik azt a szintet, amikor már kiberhadviselésről beszélhetünk, hiszen „[a] kiberbűnözés során összegyűlt adatok, illetve az azok elemzéséből levonható következtetések alkalmasak lehetnek egy másik ország politikai és/vagy gazdasági befolyásolására, valamint felhasználhatók a kiberhadviselés során annak tervezési fázisától kezdve a kibertámadások kivitelezéséig számos helyen”.[136]

A következőkben – a teljesség igénye nélkül – bemutatjuk a kibererők építésének folyamatát, valamint ennek legfontosabb szereplőit az egyéni hackerektől

[136] Kovács (2018a): i. m. 39.

az APT-csoportokon át azokig a hivatalos kiberparancsnokságokig, amelyek a kiberműveleteket ma már stratégiai szinten is képesek nagyon hatékonyan végrehajtani.

3.1. Hackerek és hackercsoportok, avagy az APT ébredése

Az 1990-es évek egyik legendás hackere volt Kevin Mitnick, aki saját bevallása szerint inkább a *social engineering,* azaz a megtévesztésre épülő informatikai támadások területén volt kiemelkedően sikeres – ma viszont már nagyon jól jövedelmező kiberbiztonsági vállalkozást vezet.[137] Az ő karrierje (ha lehet így nevezni), illetve szakmai életútja akár tipikusnak is mondható, hiszen nagyon sok korábbi, szakmailag magas szinten álló hackerből lett később a „jó oldalon" vagy etikus hacker, vagy kiberbiztonsági szakértő. Az 1990-es évek fekete kalapos *(black hat),* rosszindulatú, azaz a károkozást vagy az anyagi haszonszerzést előtérbe helyező, illetve fehér kalapos *(white hat),* azaz jóindulatú, a világot jobbá tenni akaró hackereiről már sok írás, könyv és tanulmány, sőt számos film is készült.

Azonban a hackerek korai, az 1990-es évekből származó misztikuma egyre inkább eltűnik. Ma a hackerek több évtizedes szakmai tapasztalattal rendelkező szakemberek, akik eltérő, s ez alapján kategorizálható motivációkkal rendelkeznek. Az etikus hackerek ma már szerves és elengedhetetlen részei egy kiberbiztonsági vizsgálatnak. Napjainkban tevékenységük jól szabályozott üzleti alapon működik. Az informatikai rendszerek vizsgálata sok esetben az ő közreműködésükkel, *etikus hacking*gel kezdődik. Ehhez a vizsgálatot kérő szerződést köt az etikus hackerrel, így szabályozott módon történik az eljárás. Maga az etikus hackelés egy potenciális támadó szemszögéből vizsgálja meg – az említett szerződésben előre rögzített módon és mélységig – az informatikai rendszert, illetve annak folyamatait.

Az etikus hackerek és a rosszindulatú hackerek csoportjai között egyfajta átmenetet képeznek azok a hackerek, illetve az ő csoportjaik, akik valamilyen vélt vagy valós jó ügy mellé állnak, és ennek érdekében hajtanak végre kiberműveleteket. Ezek a „jó ügyek" természetesen sokszor csak a csoport vagy annak tagjai szempontjából tűnnek jó ügynek. Ilyen csoport például az Anonymous hacktivistacsoport, amely „[a]z elmúlt 10 évben […] több nagy támadást

[137] Kevin Mitnick: *Ghost in the Wires.* New York, Back Bay Books, 2012.

is végrehajtott különböző szervezetek ellen, amelyekben mindig valamilyen ügy mellett fejezték ki szimpátiájukat".[138]

Természetesen ma is léteznek rosszindulatú hackerek. Ezek a személyek szintén nagy szakmai tapasztalattal és tudással rendelkeznek, de az ő motivációjuk merőben más irányú, mint az etikus hackereké. A rosszindulatú hackerek motivációja elsősorban az anyagi haszonszerzés, ami még akkor is igaz, ha tudásukat és tapasztalatukat olyan tevékenységek elvégzése érdekében alkalmazzák, amelyek célja például a befolyásolás vagy akár a kritikus infrastruktúrák támadása. Ezekben az esetekben van egy olyan entitás, amely pénzügyi ellenszolgáltatás fejében gyakorlatilag béreli ezt a tudást, azaz fizet a szaktudásért, illetve ezekért a műveletekért.

Ebben az esetben már gyakran összemosódik az állami támogatású csoportok és a hackercsoportok tevékenysége. Az APT-csoportok pontosan ebbe a kategóriába sorolhatók, és sok esetben – bár nem teljesen bizonyítottan – állami támogatással és/vagy állami megrendelésre követik el akcióikat.

Az APT *(advanced persistent threat)* olyan kibertámadási eljárás, amely során sokáig fennálló, nagyon kifinomult kibertámadások egyszerre valósulnak meg. Az APT tehát egy összetett és számos támadási formát magában foglaló kiberműveleti eljárást takar, amelyet magyarul sok esetben kicsit leegyszerűsítve célzott támadásoknak is neveznek.[139]

Az APT-támadások meghatározott célú, előre gondosan megtervezett, több fázisból álló műveletek. Nem véletlenszerűen kiválasztott célpontok ellen irányulnak, hanem előre pontosan meghatározott, a támadó számára értékes politikai, üzleti, katonai vagy közigazgatási információkat kezelő rendszereket támadnak. Időtartamuk 1-2 héttől akár évekig is terjedhet.[140]

Az APT-támadások legjellemzőbb célja az információszerzés. A támadássorozat a célpont rendszereinek gyenge vagy sérülékeny pontjait nagyon magas szintű technikai eljárásokkal tárja fel, majd ezeken keresztül a rendszerbe behatol egy – jellemzően – másik ATP-komponens. Ezt követően egy újabb komponens a már kompromittált rendszerből adatokat juttat ki. A folyamat során a legtöbb esetben fontos cél a minél későbbi felfedezés, és a minél tovább tartó észrevétlen adatkijuttatás. Az APT-támadások során alkalmazott módszerek miatt kijelenthető, hogy „amennyiben az APT-támadások mögött álló – alapvetően

[138] Kovács (2018b): i. m. 176.
[139] Kovács (2018b): i. m. 150.
[140] Kovács (2018b): i. m. 160.

államilag támogatott – elkövetőkkel kombináljuk a kémkedést, és ezt tekintjük a támadások fő motivációjának, akkor eljuthatunk addig a megközelítésig, hogy államilag támogatott kiberkémkedéssel állunk szemben nagyon sok APT-támadás esetében is".[141]

Ma már számos APT-csoport, sőt a korábban említett pénzügyi szektort hasonló módszerekkel támadó FIN-csoport létezik. Ezeket a csoportokat a nagy kiberbiztonsági cégek a csoportok által használt eljárások és azok jellemzői alapján ma már nagy biztonsággal azonosítani tudják. A következő táblázat néhány nagy APT-csoportot sorol fel azok jellemző paraméterei alapján megkülönböztetve.

7. táblázat: Néhány APT-csoport és fontosabb jellemzőik

APT-csoport	Ország	Célpont	Tevékenység
APT-39	Irán	Telekommunikációs szektor, IT-vállalatok, high-tech cégek, utazási cégek	Adatlopás, személyes adatok gyűjtése
APT-35	Irán	Katonai, kormányzati, diplomáciai szervezetek/személyek	Adatlopás, kiberkémkedés
APT-41	Kína	Egészségügyi szervezetek, telekommunikációs szektor, high-tech cégek	Kiberkémkedés, szellemi tulajdon lopása
APT-40	Kína	Globális szervezetek (műszaki és védelmi szféra)	Kiberkémkedés
APT-27	Kína	Ipar, üzleti szolgáltatások, védelmi ipar, védelmi szektor, energia, kormányzat	Szellemi tulajdon lopása
APT-1	Kína	IT-szektor, közigazgatás, védelmi szektor, kormányzat, energia, logisztika	Kiberkémkedés
APT-38	Észak-Korea	Pénzügyi szektor	Pénzszerzés
APT-29	Oroszország	Nyugat-európai kormányzatok	Kiberkémkedés
APT-28	Oroszország	Kelet-európai országok, NATO, európai biztonsági szervezetek, kaukázusi országok	Kiberkémkedés

Forrás: FireEye: Advanced Persistent Threat Groups. *Mandiant,* 2021 alapján a szerző szerkesztése

[141] Kovács (2018b): i. m. 157–158.

3.2. A kiberképességek szervezeti háttere

Ma már a legtöbb ország építi katonai kiberműveleti képességeit. A NATO-országok esetében ezt a kiberképesség-fejlesztést – természetesen a kiberbiztonság és a kibervédelem erősítése érdekében – a NATO 2016-os varsói csúcstalálkozóján, ahol a szervezet műveleti térnek nyilvánította a kiberteret,[142] egy úgynevezett *Cyber Pledge*-ben, azaz a tagországok kibervédelmi képességeinek építésére és fejlesztésére tett vállaláscsomagban is rögzítették.[143]

Nyilvánvalóan ezek a kibervédelmi képességek nemcsak katonai, hanem civil kiberképességeket is jelentenek. Ezeknek a képességeknek az összessége adja az adott ország korábban már említett kibertéri ellenálló képességét.

Míg azonban a civil kiberképességek elsősorban a védelemre összpontosítanak, a katonai képességek sok ország esetében a támadó vagy offenzív kiberképességek fejlesztését is magukban foglalják.

A következőkben azt vizsgáljuk meg, hogy ezek az – elsősorban katonai – kiberműveleti erők milyen általános elveknek kell hogy megfeleljenek, illetve bemutatjuk, hogy néhány országban a katonai kiberműveleti erők építése jelenleg hol tart.

3.2.1. Hogyan fejlesszünk kiberműveleti erőket?

A katonai kibertérműveleti erők felépítése, illetve fejlesztése természetszerűleg országonként eltér, hiszen minden ország más és más jogszabályi háttérrel, kibertéri fejlettséggel és nem utolsósorban a katonai területen eltérő feladatokkal rendelkezik. Ugyanakkor általánosságban fel tudunk vázolni néhány olyan elvet, amelyek mentén ezek a katonai kiberműveleti erők felépülnek.

Az első ilyen elv rögtön egy csoportot is jelent egyben, amely nem más, mint a katonai kiberműveleti erők funkcióinak csoportja. Ezek a funkciók viszonylag jól szétválaszthatók egymástól. Az első a kiberműveleti információgyűjtés. A kiberműveletek végrehajtásához szükséges információk összegyűjtése és elemzése kiemelt feladat. Ebbe a funkcióba beletartozik a fenyegetéselemzés, a kiberműveleti helyzetkép felvázolása, valamint az információk eljuttatása a kiberműveleteket végrehajtókhoz. A következő kiberműveleti funkció

[142] NATO: *Warsaw Summit Communiqué* (2016b. július 9.).
[143] NATO: *Cyber Defence Pledge* (2016a. július 8.).

a tervezés. A kiberműveletek megtervezése és összehangolása a kinetikus műveletekkel szintén nagyon fontos, hiszen csak így biztosítható a maximális hatáskiváltás. Ez a művelettervezés a kiberműveleti információgyűjtés során megszerzett, elemzett és értékelt adatokra és információkra épít. A harmadik funkció maga a kiberművelet végrehajtása, amely lehet védelmi vagy támadó jellegű. Természetesen a hatékony műveletek feltételezik a művelettámogatási, benne többek között a kutatás-fejlesztési, valamint a képzési és kiképzési funkciókat is, amelyek szintén meg kell hogy jelenjenek a katonai kiberműveleti erőknél.

Ezek a funkciók képességként jelennek meg a katonai kiberműveleti erőknél, amelyek szervezetüket tekintve általában egy vagy több központi helyen működnek, s ott kiépített, stacioner infrastruktúrával rendelkeznek. Ugyanakkor sok esetben szükséges ezek mellett olyan mobilizálható szervezeti elemek kialakítása is, amelyek a kinetikus erők megerősítéseként, azok feladatellátási helyén tudnak számukra támogatást nyújtani. Természetesen ezen mobil csoportoknak egyik nagy előnye, hogy mind képzésük, mind felkészítésük, mind a közös elvi alapon felépített mobilizálható eszközparkjuk kialakítása az említett központi kiberműveleti erőkkel együtt történik. Így nemcsak egy „nyelvet" beszélnek, ami elengedhetetlen a gyors és hatékony problémamegoldáshoz, hanem mobilizálható kommunikációs megoldásaik révén a központi helyen meglévő adatbázisokhoz, illetve ezen a központi helyen meglévő, speciális ismereteket igénylő tudáshoz is hozzáférnek. Természetesen ezek a mobil kiberműveleti erők szükségszerűen együtt kell hogy mozogjanak a támogatandó erőkkel, így a kiberműveleti erők logisztikája – például gépjárművei –, fizikai felkészítése hasonló a támogatandó erőkéhez, vagy akár meg is egyezik azzal.

3.2.2. Kiberparancsnokságok

Ahogy utaltunk rá, a katonai kiberműveleti erők országonként eltérő módon alakulnak és fejlődnek. A felépítést nagyban meghatározza az adott ország nemzeti kibervédelmi politikája, stratégiája, valamint politikai és gazdasági döntései. Ugyanakkor érdemes górcső alá venni néhány ország kiberműveleti erőinek jelenlegi szervezetét, hiszen ezek azok a szervezetek, amelyek valamilyen módon a kiberműveleteket végrehajtják.

Bár, ahogy említettük, minden ország a saját útját járja a kibererők építése során, a szervezetek általában a fentebb bemutatott funkciók és elvek mentén jönnek létre. Gyakorlatilag minden kiberműveleti szervezet rendelkezik kibertéri

információszerző és -elemző képességgel, amely sok esetben magában foglalja a célkiválasztás, a célazonosítás és a célkövetés képességét is. Ezen szervezetek esetében ma már egyre gyakrabban láthatjuk, hogy a kibererők nemcsak a kibervédelem, hanem bizony a kibertámadás képességeit is magukban hordozzák. Nagyon érdekes megfigyelni, ahogy majd Németország vonatkozásában látni is fogjuk, hogy a kibertér mellett néhány ország az információs dimenziót is olyan műveleti területnek tekinti, ahol ezeknek az erőknek feladatokat kell ellátniuk.

Az minden országban világosan látszik, hogy a katonai kiberműveleti erőknek már jóval több feladatot kell ellátniuk a puszta katonai művelet-végrehajtásnál, illetve a kinetikus katonai erők támogatásánál. Egyrészt sok ország a fontos szerepet szán a katonai kibererőknek a kiberelrettentésben, másrészt a nemzeti kiber-ellenállóképesség egyik legfontosabb pilléreként határozza meg ezen erőket. Szintén országonként eltérő módon, de általában a katonai kiberműveleti erőknek egyik fontos feladata lehet az ország kritikus infrastruktúrájának, illetve kritikus információs infrastruktúrájának védelme, az ebben való közreműködés, illetve az ilyen feladatokra szakosodott szervezetek támogatása. Vannak olyan országok, mint például az Egyesült Államok, amelyekben a katonai kiberműveleti erők nagy politikai felhatalmazással vesznek részt – a katonai feladatok ellátása mellett – az adott ország politikai és gazdasági rendszereinek védelmében is. Az Egyesült Államok esetében ilyen feladat például a választásokba való illetéktelen kibertéri beavatkozás megakadályozása.

Megvizsgálva a katonai kiberműveleti erők kialakításának és fejlesztésének időszükségletét az is világosan látszik, hogy ez még a nagy anyagi és humán erőforrásokkal rendelkező országok esetében is több, akár 8-10 évet is igénybe vesz. Ahogy az egyes országok képességeinek bemutatása során látni fogjuk, minden ország nagy hangsúlyt helyez a humán erőforrás biztosítására. Ez nemcsak anyagi, azaz fizetésben megjelenő kérdés, hanem olyan tudatos és szisztematikus építkezés, amely már a középiskolai, majd az egyetemi képzések összehangolásában jelentkezik. Sok ország már a középiskolásokat megcélozza a katonai kiberműveleti utánpótlás biztosítása érdekében, akiket ezt követően egészen az egyetemi oktatáson át az ezt követő speciális szakmai képzésekig bezárólag folyamatosan motivál, nyomon követ, és például különböző ösztöndíjakkal, támogatásokkal el is kötelez a későbbi munkavállalás érdekében.

Nem elsősorban csak a katonai kiberműveleti képességek építése mentén, de szintén minden országban kiemelt szerepet kap a kiberbiztonsággal és a kiberműveletekkel összefüggő kutatás és fejlesztés kérdésköre. A K+F területe magához a kibervédelemhez hasonlóan össznemzeti kérdés, hiszen ezen a területen is

csak akkor lehet sikeres egy ország, ha az akadémiai szféra, a területen működő kis- és közepes vállalkozások, valamint az állami szféra, benne az adott ország hadserege is közösen egy tudatosan kialakított, fenntartható kutatás-fejlesztési ökoszisztémát alakít ki.

Szintén nagyon jól látszik a különböző országok esetében elvégzett vizsgálatokból, hogy bár minden ország önálló utat jár, mégis sok esetben különösen nagy hangsúlyt fektetnek a nemzetközi kapcsolatok kialakítására, és a nemzetközi együttműködésre. Gyakorlatilag minden ország felismerte, hogy a kibertérben a nemzetközi együttműködés elengedhetetlen. Ez az együttműködés számos területre ki kell hogy terjedjen, amely együttműködés magában foglalja a technikai eljárások kutatás-fejlesztési kérdéseit, a kiberbiztonság és a kiberműveletek jogi szabályozásának kérdéseit, vagy éppen a kölcsönös segítségnyújtást is.

Nézzük tehát, hogy mindezek mit is jelentenek pontosan egyes országok vonatkozásában. A vizsgált országok: Amerikai Egyesült Államok, Egyesült Királyság, Lengyelország, Magyarország és Németország. Ezen önkényesen kiválasztott országok katonai kiberképességeinek bemutatása mellett sort kerítünk nagyon röviden az Európai Unió új kezdeményezésének bemutatására is, amely egy közös uniós kiberegység felállítását célozza meg. Bár ez nem katonai kiberműveleti erő lesz, mégis nagyon jól szemlélteti azokat az elveket és jellemzőket, amelyeket a fentiekben bemutattunk, hiszen ezek a civil szervezetek esetében is hasonlóak.

3.2.2.1. Amerikai Egyesült Államok

Az Egyesült Államok 2009-ben állította fel a hadsereg Stratégiai Parancsnokságának (US Strategic Command) égisze alatt a katonai kibererőket integráló szervezetét, amely a US Cyber Command (röviden: USCYBERCOM), azaz az Egyesült Államok Kiberparancsnoksága nevet kapta. A USCYBERCOM közel 10 évig tartó fejlesztés és fejlődés után 2018-ban önálló komponensparancsnoksági státuszt nyert, ami nemcsak elismerése a szakmai munkának, hanem a szervezet számára világméretű feladatvégrehajtást is lehetővé tesz. Az USCYBERCOM-on belül 2013-ban megalakult az úgynevezett Kiberműveleti Erő (Cyber Mission Force, CMF), amely a kiberműveletek fő végrehajtó szervezeti eleme lett.

A USCYBERCOM parancsnoka egyben az Egyesült Államok Nemzetbiztonsági Ügynökségének (National Security Agency, NSA) az igazgatója, valamint az ő szakmai alárendeltségébe tartoznak a hadsereg elektronikai hadviselési

erői is. A USCYBERCOM vezetője hagyományosan – hivatalba lépésekor – kiad egy stratégiai jövőképet bemutató anyagot. 2018-ban a USCYBERCOM új parancsnoka[144] a következőket írta ebben a kiadványban: „A USCYBERCOM részt vállal a nemzeti stratégiai elrettentés biztosításában. Felkészítjük, működtetjük és együttműködésünkkel támogatjuk a harcoló parancsnokságokat, fegyvernemeket, szövetségeseket és az ipart az ellenséges kibertéri szereplők elleni folyamatos fellépésben és a tevékenységük akadályozásában, bárhol bukkanjanak is fel."[145] Önmagában már a kiadvány címe is erőt sugároz: *Achieve and Maintain Cyberspace Superiority – Command Vision for US Cyber Command,*[146] amely magyarul, kissé szabad fordításban így hangzik: „A kibertéri fölény elérése és fenntartása – Parancsnoki jövőkép az Egyesült Államok Kiberparancsnoksága számára."

A USCYBERCOM szervezetén belül 133 önálló kiberműveleti csoport, azaz CMF alakult meg. Ezek a kiberműveleti csoportok szakmailag a USCYBERCOM-hoz, de szervezetileg az adott csoport haderőneméhez tartoznak. Ennek a felosztásnak van egy óriási előnye, amelyet a kibererőket bemutató általános elveknél már említettünk, tudniillik a közös bázison, azonos elvek mentén történő felkészítés és kiképzés. A CMF-ek egységes felkészítése, felépítése és kiképzése nyomán tehát ugyanazt a szakmai terminológiát használják a szakemberek, valamint ugyanazokra a képességekre tesznek szert.

A USCYBERCOM számos katonai és nem katonai feladatot is ellát. Ezek egyike 2020-ban az amerikai elnökválasztás kibertéri védelme volt – ugyanakkor a már szintén említett kritikus nemzeti infrastruktúra védelmében is fontos feladatokat lát el az Egyesült Államok Belbiztonsági Minisztériumával (Department of Homeland Security, DHS) közösen.

A katonai feladatokat tekintve a USCYBERCOM egyik legismertebb akciója – *Glowing Symphony* fedőnév alatt – 2016-ban került sor. Ennek során a Joint Task Force Ares, a USCYBERCOM által offenzív kiberműveletek végrehajtására felhatalmazott egyik csoport az ISIS nemzetközi terrorszervezet ellen hajtott végre célzott kibertámadásokat.[147] Az offenzív kiberművelet az „ISIS

[144] A USCYBERCOM 2018-ban beiktatott parancsnoka és egyben az NSA igazgatója Paul Nakasone tábornok.

[145] U.S. Cyber Command (2018): i. m. 7.

[146] U.S. Cyber Command (2018): i. m.

[147] National Security Archive: *USCYBERCOM 30-Day Assessment of Operation Glowing Symphony: Executive Summary* (2016. december 13.).

média- és online műveleteit célozta meg, megfosztva a szervezetet infrastruktúrájától, és megakadályozva az ISIS tagjait a propagandájuk terjesztésében és közzétételében".[148]

Ahhoz azonban, hogy ilyen műveleteket végre lehessen hajtani, megfelelő szakembergárda szükséges. Ahogy korábban említettük, a megfelelő szakértelemmel rendelkező humán erőforrás bevonzása és nem utolsósorban megtartása kiemelten fontos minden országban. Ez így van az Egyesült Államok esetében is, ezért a parancsnokság kezdeményezésére létrejött az úgynevezett Cyber Patriot STEM program. Ennek égisze alatt a USCYBERCOM középiskolákkal, valamint közel félszáz műszaki orientáltságú egyetemmel működik együtt. Ez nemcsak toborzómunkát jelent, hanem olyan közös kutatás-fejlesztési programokat is, amelyek a technikai fejlesztések kidolgozása mellett a potenciális munkatársak megtalálásához is hozzájárulnak a fiatal kutatók és hallgatók körében.[149]

A humán erőforrás biztosításán túl szintén kiemelt fontosságú az említett kutatás-fejlesztési programokban való minél szélesebb körű részvétel. A USCYBERCOM ennek érdekében nemcsak hogy közreműködik K+F-programokban, de az egyik létrehozója is a Dreamport elnevezésű kutatás-fejlesztési programnak, amelynek keretében egy fizikailag is kialakított K+F-bázison többek között a USCYBERCOM megrendelésére számos kibertéri relációjú kutatás-fejlesztési, valamint innovációs projekt zajlik.[150]

3.2.2.2. Egyesült Királyság

Az Egyesült Királyság kibervédelmi és kiberműveleti erőit a Nemzeti Kiberbiztonsági Központ (National Cyber Security Centre, NCSC) vezeti. Az NCSC a titkosszolgálatként működő Kormányzati Kommunikációs Főparancsnokág (Governmental Communication Headquarters, GCHQ) része.[151]

Ugyanakkor a GCHQ és a védelmi tárca együttműködésében 2020-ban megalakult a Nemzeti Kibererő (National Cyber Force, NCF), amely az NCSC-től

[148] Mark Pomerleau: What Cyber Command's ISIS Operation Means for the Future of Information Warfare. *C4ISRNet,* 2020. június 18.

[149] U.S. Cyber Command: *Cybercom Media Roundtable* (2019. május 7.).

[150] Maryland Innovation & Security Institute: *Dreamport,* 2021.

[151] GCHQ: *Cyber Security. Making the UK the Safest Place to Live and Do Business Online* (2021).

eltérően nemcsak a kibervédelemre, hanem proaktív kiberműveletek,[152] valamint offenzív műveletek[153] végrehajtására is felhatalmazást kapott. Ennek megfelelően épült is fel maga a szervezet.

Az NCF egy olyan egységes parancsnokság, amely integrálja a GCHQ hírszerző és kiberbiztonsági képességeit, a Védelmi Minisztérium kiberképességeit, az MI6 titkosszolgálat kiberképességeit, valamint a Védelmi Tudományos és Technológiai Laboratórium (Defence Scientific and Technology Laboratory, DSTL) kibertérben hasznosítható erőforrásait.[154]

Az NCF ezekkel az erőforrásokkal olyan kiberműveletek elvégzésére képes, mint például a mobiltelefon-lehallgatás vagy a mobiltelefonok terrorcélú alkalmazásának gyanúja esetén működésük akadályozás; súlyos, a kibertérben megvalósuló bűncselekmények felderítése és megakadályozása, beleértve a gyermekek szexuális bántalmazását és kihasználását; valamint az Egyesült Királyság katonai repülőgépei elleni fegyverrendszerek alkalmazásával szembeni műveletek.[155] Ez utóbbi feltételezhetően azt is jelenti, hogy az NCF jogosultságot kap ellenséges katonai fegyverrendszerekbe, ebben az esetben radarrendszerekbe behatolni, és azokat működésükben akadályozni.[156]

Az NCF létrejöttének katonai szempontból az egyik legnagyobb előnye, hogy olyan kiberműveleti képességek állnak már nemcsak a civil szolgálatok és kormányzati intézmények, hanem a hadsereg rendelkezésére is, amelyek nemzeti szinten teszik lehetővé a szükséges (kiber)képességek integrálását és koordinálását.

3.2.2.3. Európai Unió

Bár az Európai Uniónak nincsenek katonai kiberműveleti erői, az EU 2020 végén kiadott kiberbiztonsági stratégiája egy közös kiberbiztonsági egység létrehozására tett javaslatot.

[152] Matt Burgess: The UK Created a Secretive, Elite Hacking Force. Here's What It Does. *Wired,* 2020. november 20.

[153] Gordon Corera: UK's National Cyber Force Comes Out of the Shadows. *BBC News,* 2020. november 20.

[154] Gov.uk: National Cyber Force Transforms Country's Cyber Capabilities to Protect UK (2021).

[155] Gov.uk (2021): i. m.

[156] Corera (2020): i. m.

Ez a közös uniós kiberbiztonsági egység a tagországok kiberbiztonsági szervezeteinek együttműködését szolgálná, alapvetően technikai, beavatkozó egységekkel. Az elképzelés szerint ez nem egy új, önálló szervezetet jelentene, hanem „inkább olyan védőhálóként működne, amelyben a résztvevők számíthatnának a többi résztvevő támogatására és szakértelmére, különösen akkor, ha különböző kiberbiztonsági közösségeknek kell szorosan együttműködniük".[157]

A tervezett közös kiberbiztonsági egységnek három fő célja lenne. Az első az, hogy ez a félig virtuális, félig a tagországok felajánlásával létrejövő, fizikai valóságában rendelkezésre álló szervezet hozzájáruljon a kiberbiztonsági szervezetek felkészüléséhez. Második célként a javaslat azt jelölte meg, hogy a tagországok információmegosztására építve folyamatosan figyelemmel kísérje a kibertéri helyzetet, s az ezzel kapcsolatos információkat ossza meg a tagországokkal. A harmadik cél nem más, mint egy esetlegesen bekövetkezett, valamely tagország vagy tagországok ellen irányuló támadás után működjön közre a károk minimalizásálásában, azok felszámolásában, illetve a helyreállításban. Mindezekhez a célokhoz alapvetően szükséges kialakítani a gyors és megbízható információáramlás platformjait, meg kell nyerni a gazdasági szereplők, benne a kiberbiztonsági ipar kiemelt szereplőinek támogatását, valamint ki kell alakítani a megfelelő koordináció képességét.

3.2.2.4. Lengyelország

Lengyelországban 2019-ben jött létre a Nemzeti Kiberbiztonsági Központ (Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni, NCBC). A Védelmi Minisztérium irányítása alatt működő központ feladata a védelmi szféra és a lengyel hadsereg infokommunikációs üzemeltetési és fejlesztési feladatainak biztosítása, kiszolgálása, valamint a kiberbiztonság nemzeti szintű koordinálása. Ezeken kívül gondoskodik a minősített rendszerek működéséhez szükséges kriptográfiai eszközökről, valamint üzemelteti a Katonai Elektronikus Információbiztonsági Eseménykezelő Központot (angol elnevezéssel MilCERT,Military Computer Emergency Response Team).

Az NCBC kiberműveleti egysége a Kiberműveleti Központ. Ez a központ egyrészt együttműködésével támogatja a hagyományos katonai erők fizikai

[157] Európai Bizottság (2020): i. m. 2.1. 16.

dimenziókban végzett tevékenységeit, másrészt önálló kiberműveleteket is vezet.[158]

Az NCBC vezetésével jött létre 2019-ben a Cyber.Mil.Pl elnevezésű program, amelynek célja támogatni a kibervédelmi erőket, továbbá integrálni a védelmi minisztérium kiberbiztonsági feladatait, beleértve a fejlesztést, a humán erőforrás toborzását, valamint a kiberműveleti szakértők felkészítését és képzését is.[159] A programban számos szervezet vesz részt, többek között a varsói Katonai Műszaki Egyetem, a lengyel Haditengerészeti Akadémia, illetve kutatóintézetként a Katonai Kommunikációs Intézet, de a lengyel területvédelmi erők is.[160]

Szintén a Cyber.Mil.Pl program keretében indult el egy, a köziskolai korosztályt megcélzó program. Ebben az NCBC a varsói Katonai Műszaki Egyetemmel közösen olyan középiskolai képzést indított, amely fő szakmai vonalként a kiberbiztonságot oktatja. Mindezek mellett, többek között a jövőben itt végző középiskolásokra hallgatóként számítva, az egyetem 2019-ben elindította kiberbiztonsági mesterképzését is.[161]

Az NCBC a képzés és felkészítés területén is hatalmas lépéseket tesz: 2020-ban felállította a Cyber Security Training Centre of Excellence kiberbiztonsági képzési központot, amelynek fő célja a lengyel kibervédelmi és kiberműveleti erők szakmai utánpótlásának biztosítása.[162]

3.2.2.5. Magyarország

Magyarországon a katonai kiberműveleti erők építése 4-5 éves múltra tekint vissza. A hazai kibervédelem természetesen ennél lényegesen nagyobb múlttal rendelkezik, azonban alapvetően civil intézményekre épül. Ezek egyik zászlóshajója a 2015-ben létrejött Nemzeti Kibervédelmi Intézet, amely a Belügyminisztérium irányítása alá tartozó Nemzetbiztonsági Szakszolgálat berkein belül működik.

A katonai területen 2017-ben a Katonai Nemzetbiztonsági Szolgálat alárendeltségében jött létre a Kibervédelmi Központ, amely honvédelmi ágazati feladatokat is ellát, illetve üzemelteti az ágazati incidenskezelő központot. 2019-ben

[158] Cyber.Mil.Pl. 2021.
[159] Cyber.Mil.Pl (2021): i. m.
[160] Cyber.Mil.Pl (2021): i. m.
[161] Cyber.Mil.Pl (2021): i. m.
[162] Cyber Security Training Centre of Excellence: *What We Do* (2021).

kezdődött meg a Magyar Honvédség kiberműveleti erőinek szervezetszerű kialakítása. Ennek keretében a Magyar Honvédség Parancsnoksága alárendeltségében 2019-ben megalakult a Kibervédelmi Haderőnemi Szemlélőség, illetve ennek szakmai vezetésével állították fel a Magyar Honvédség Katonai Kiber- és Információs Műveleti Központját. Amíg a haderőnemi szemlélőség fő feladata a stratégiai szintű szakmai irányítás, addig a Katonai Kiber- és Információs Műveleti Központ a szemlélőség szakmai irányításával várhatóan a következő években folyamatosan tesz szert a kiberműveleti képességekre, köztük a hazai nemzeti biztonsági stratégia vonatkozásában már említett offenzív képességekre.

Ez a képességépítés hazánkban sem nélkülözi a humán erőforrás, azaz a szükséges szakembergárda képzését és felkészítését. Ezt kapta feladatul a Magyar Honvédségen belül 2019-ben felállított kiberképzési központ, más néven a Kiberakadémia is. Természetesen a szervezet létrehozásán kívül számos más lépés is történt a képzés és a felkészítés területén. Több felsőoktatási intézményben indult el az informatikai szakokon kiberbiztonsági témájú tárgyak oktatása az ezeket megalapozó tudományos kutatásokkal egyetemben. Ezeken kívül a Nemzeti Közszolgálati Egyetem[163] és az Óbudai Egyetem is indított kiberbiztonsági szakokat.

A hazai katonai kiberműveleti képességek kialakításában szintén fontos mérföldkő, hogy a már többször említett nemzeti biztonsági stratégiában rögzített katonai kiberműveleti képességek[164] alkalmazásához megszületett a jogi felhatalmazás. 2020. január 1-jével a honvédelmi törvénybe ugyanis bekerültek a katonai kibertérműveleti erőkre vonatkozó szabályok. Ezek többek között olyan felhatalmazást – és egyben persze feladatokat is – jelentenek a hadsereg számára, mint például a Magyarország ellen irányuló kibertámadások megszakításának lehetősége, illetve az ezekre adandó, velük arányos kibertéri válaszok, azaz kiberműveletek indításának lehetősége.[165]

3.2.2.6. Németország

Németországban 2017-ben hozták létre azt a katonai kiberműveleti feladatokat is ellátó alakulatot, amely a Kiber- és Információsdomain-parancsnokság (német megnevezéssel Kommando Cyber- und Informationsraum, angolul Cyber and

[163] Nemzeti Közszolgálati Egyetem: *Kiberbiztonsági mesterképzési szak* (2021).
[164] 1163/2020. (IV. 21.) Korm. határozat 135. pont.
[165] 1163/2020. (IV. 21.) Korm. határozat 62/A. § (1) *c)* pont.

Information Domain Headquarters) nevet viseli. A Bundeswehr, azaz a német hadsereg új alakulata közel 14 ezer főt magába foglalva[166] fő feladatul a hadsereg infokommunikációs rendszereinek üzemeltetését, azok informatikai védelmét, a hírszerzést, valamint a kiberműveletek és elektronikai hadviselési műveletek végrehajtását,[167] valamint a német hadsereg geoinformációs támogatását kapta.[168]

A fentiekből világosan látszik, hogy a német Kiber- és Információsdomain-parancsnokság nemcsak a kibertérben végezhet műveleteket, köztük offenzív tevékenységeket, hanem az információs térben is, sőt az elektronikai hadviselés révén az elektromágneses spektrumban is. Érdemes ezzel kapcsolatban megjegyezni, hogy a német katonai gondolkodás a kibertér szerves részének tekinti az elektromágneses spektrumot, valamint a hatások miatt a kiberteret és az információs teret egymáshoz nagyon közelinek értékeli.

Ahogy a már bemutatott országok kiberparancsokságainál láthattuk, a német Kiber- és Információsdomain-parancsnokság is törekszik a nemzetközi kapcsolatok építésére. Ebben a munkában az egyik kiemelt cél a kibertérre vonatkozó minél szélesebb körű információcsere kialakítása.[169]

Németország számára is kiemelt kérdés az utánpótlás biztosítása. Ennek érdekében többek között a Münchenben található Bundeswehr Egyetemen kiberbiztonsági mesterképzést is indítottak,[170] továbbá a Bundeswehr támogatásával Berlinben megalakult egy kutatóintézet, amelynek egyik fő feladata a kiberbiztonság és a kiberműveletek kutatás-fejlesztési eredményekkel való támogatása.[171]

3.2.3. A NATO kiberszervezetei

Bár a NATO-nak nincs a fenti országokéhoz hasonló kiberparancsnoksága, mégis érdemes néhány pillantást vetnünk a szövetség kiberszervezeteinek felépítésére, illetve azok szerepére.

A 2002-es prágai NATO-csúcsértekezlet óta a kibervédelmi és kiberműveleti kérdések folyamatosan jelen vannak a szervezet gondolkodásában. Mégis kiemel-

[166] Zeit Online: Bundeswehr rüstet gegen Attacken aus dem Internet. *Die Zeit,* 2016. április 26.
[167] Bundeswehr: *Kommando Cyber- und Informationsraum* (2021a).
[168] Ludwig Leinhos: The German Cyber and Information Domain Service as a Key Part of National Security Policy. *Ethics and Armed Forces,* (2019), 1.
[169] Bundeswehr: *The Cyber and Information Domain Service* (2021b).
[170] Universität der Bundeswehr München: *Studiengang Cyber-Sicherheit* (2021).
[171] Bundeswehr: *Zentrum für Cyber-Sicherheit der Bundeswehr* (2021c).

hetünk két fontos dátumot a történetében ezzel kapcsolatban. Az egyik a már korábban bemutatott észtországi kiberkonfliktus 2007-ből, hiszen ekkor kellett először szembesülnie a NATO-nak azzal, hogy egy tagállamát nemcsak a fizikai térben, hanem a kibertérben is érheti olyan támadás, amely akár az egész szervezetre komoly kihatással jár.

A másik kiemelkedő esemény a 2016-os varsói csúcsértekezlet volt, amelyen a tagállamok a kiberteret műveleti térré nyilvánították. Ez az esemény kétségkívül történelmi jelentőségűnek tekinthető, hiszen a hagyományos négy fizikai dimenzióhoz – szárazföld, levegő, tenger, űr – hasonlóan a kibertérre vonatkozóan is megkezdődhetett azoknak a doktrinális alapoknak a kidolgozása, amelyek ezt követően lehetővé tették, hogy a tagállamok többé-kevésbé, de mégiscsak egységes álláspont és filozófiai háttér mentén fejlesszék – elsősorban katonai – kiberképességeiket és eljárásaikat. Ezen a csúcsértékezleten persze nemcsak az új műveleti tér hivatalos megjelenése, illetve elfogadása volt történelmi, hanem az úgynevezett kibervállalás *(NATO Cyber Defence Pledge)* is. Ez nem jelent mást, mint hogy

> „a kibervédelem kérdésére a szövetség alapvetően mint a tagországok kötelezettségére tekint. Ugyanakkor mivel az is teljesen világos, hogy a kibervédelmet egy-egy adott tagország […] nem képes nemzetközi együttműködés nélkül megvalósítani, ezért a tagországok összefogása és folyamatos párbeszéde elengedhetetlenül fontos. Ennek a párbeszédnek ki kell terjednie az olyan információcserére is, amely a veszélyek és a fenyegetések időbeni felismerésére vagy az ezek elleni technikai védekezés megoldásaira vonatkoznak."[172]

A kibervédelem tehát a NATO alapfilozófiájából fakadóan a kollektív védelem része. Annak érdekében pedig, hogy a szövetségen belül ez koordinált módon valósuljon meg, különböző testületek és szervezetek felállítására volt szükség. Ezek közül a szervezetek közül a kibervédelem tervezése és politikai szintű döntés-előkészítése érdekében két nagyon fontos testületet célszerű kiemelni. Az egyik a Kibervédelmi Bizottság (Cyber Defence Committee, CDC), amely az Észak-Atlanti Tanács (North Atlantic Council, NAC) tanácsadó testülete, valamint a Kibervédelmi Irányító Testület (Cyber Defence Management Board, CDMB), amely az új biztonsági kihívásokért felelős NATO-főtitkár-helyettes irányítása alatt működik. A Kibervédelmi Bizottság a NATO kibervédelmi politikájának kialakításáért felelős testület, amely közvetlenül a már említett NAC-nek van alárendelve, ezzel is biztosítva a gyors és hatékony munkát. Ezzel szemben

[172] Kovács (2018c): i. m. 100.

a CDMB a NATO polgári és katonai testületei közötti kibervédelmi koordinációért felelős. A CDMB a NATO egyes szervezeteinek, valamint a tagállamok politikai, katonai, műveleti és műszaki testületeinek kibervédelemért felelős vezetőiből áll. A CDMB munkáját a NATO úgynevezett újonnan felmerülő biztonsági kihívásokért felelős főtitkár-helyettese (Assistant Secretary General for Emerging Security Challenges) vezeti.[173]

A kibervédelem technikai szintű kérdéseit a NATO Konzultációs, Irányítási és Vezetési Testülete (Consultation, Control and Command, NC3) koordinálja. Ugyanakkor a szövetség központi szervezeteinek vezetési, információs és kibervédelmi rendszereit a NATO egyik speciális ügynöksége, a NATO Kommunikációs és Információs Ügynökség (NATO Communication and Information Agency, NCIA) tervezi, szervezi és tartja fent. Az NCIA a belgiumi Monsban létrehozott NATO Számítógép-vészhelyzeti Reagálócsoporton (NATO Computer Incidence Response Team, NCIRC) keresztül végzi a kiberbiztonsági események technikai kezelését az egész NATO-ban. Az NCIRC-nek kiemelt szerepe van a szövetséget vagy annak központi infokommunikációs szolgáltatásait érintő kiberincidensekhez kapcsolódó komplex feladatok ellátásában: „Kezeli és jelenti az incidenseket, terjeszti az incidensekkel kapcsolatos fontos információkat a rendszer-/biztonsági menedzsment és a felhasználók felé."[174] Továbbá a NATO-szervezeteken belüli és a tagországokkal közösen végzett kibervédelmi feladatok és tevékenységek koordinálásáért is felelős.[175]

A Szövetséges Transzformációs Parancsnokság (Allied Command of Transformation, ACT) felelős a legtöbb NATO-kibergyakorlat megtervezéséért, megszervezéséért és lebonyolításáért.[176] Ezek a gyakorlatok nemcsak a katonák felkészítését szolgálják, hanem a nemzeti és nemzetközi együttműködés gyakoroltatását is lehetővé teszik a civil és a katonai kibervédelmi entitások között. A kibervédelem mellett nagy hangsúlyt fektetnek ilyenkor a kritikus infrastruktúrák, ezeken belül is természetszerűleg a kritikus információs infrastruktúrák védelmének gyakoroltatására, valamint a jogi környezet értelmezésén és alkalmazásán dolgozó szakértők felkészítésére. A kibervédelmi gyakorlatok technikai megvalósításában kulcsszerepet játszik a már említett NATO Kibervédelmi

[173] NATO: *Cyber Defence* (2022a. március 23.).
[174] NATO (2022a): i. m.
[175] NATO (2022a): i. m.
[176] Ilyen NATO-kibergyakorlatok például a Cyber Coalition vagy a Locked Shields nemzetközi gyakorlatok.

Kiválósági Központ, amely az ACT mellett a megtervezésben, a megszervezésben és a lebonyolításban egyaránt közreműködik.

A NATO parancsnoki struktúrájában kiemelt kibervédelmi feladatokat lát el a Szövetséges Erők Európai Főparancsnokságának (Supreme Headquarters Allied Powers Europe, SHAPE) Kibertérműveleti Központja (Cyberspace Operation Center, CyOC), amely a szövetség katonai műveleteiben a kiberműveletek stratégiai szintű koordinációját végzi.

A NATO kibervédelmi szervezetei mellett nagyon röviden szót kell ejtenünk a NATO kibertérműveleti doktrínájáról *(Allied Joint Doctrine for Cyberspace Operations)* is. Az AJP-3.20 szövetségi kóddal ellátott szabvány meghatározó a NATO kiberműveleteinek politikai-doktrinális dokumentumai között, hiszen ez az első kiberműveleteket szövetségi szinten szabályozó kiadvány. A doktrína világos eligazítást ad a kiberműveletekkel kapcsolatos terminológiára vonatkozóan, kategorizálja a kiberműveletek fajtáit – a jelen könyv 6. ábráján is bemutatott formában –, valamint meghatározza a kiberműveletek legfontosabb jellemzőit. A dokumentum leírja a kiberműveletek tervezéséhez és végrehajtásához szükséges elveket, beleértve a kiber-, az információs, valamint a fizikai tér legfontosabb olyan jellemzőit is, amelyek hatással vannak a kiberműveletekre. Természetesen mindezeken kívül a kiberműveletek és a kinetikus katonai tevékenységek közötti kölcsönös együttműködési elvekre is kitér.

Mivel a NATO alapvetően védelmi jellegű politikai és katonai szövetség, kibertámadó képességei a korábban már említett tagállami képességekre és így a tagállamok felajánlására épül (az úgynevezett, korábban már említett SCEPVA, azaz a szuverén kiberképességek önkéntes szövetségesi átadása révén), ami nem jelenti azt, hogy adott esetben a szövetség ne élne ezzel a kiberműveleti formával.

4. fejezet

A kiberműveletek fegyverei, eljárásai és várható jövője

4.1. A kiberműveletek és a kiberhadviselés fegyverei, eljárásai

A kibertérben alkalmazott fegyverek esetében hasonlóan nehéz problémába ütközünk, mint a kibertér meghatározásának során. Nincs ugyanis olyan kiberfegyverdefiníció, amely általánosan elfogadott lenne. Ennek megfelelően jelen alfejezetünk célja nem a kiberfegyverek problematikájának teljes vertikumú feltárása, hanem csak a problémakör egyes részeinek felvillantása. Ezek mentén lehetséges a további, akár tudományos igényű kérdések megfogalmazása, esetenként azok kutatása.

Az teljesen biztos, hogy minden olyan eszköz, amellyel informatikai vagy tágabb értelemben kibertámadást lehet elkövetni, nagy valószínűséggel kiberfegyverként is alkalmazható. Persze, mint sok minden más a kibertérben, ez sem teljesen fehér vagy fekete, hiszen egy *script kiddie,* azaz egy programozói tudással nem vagy csak alig rendelkező fiatal kezében, aki hozzáfér egy rosszindulatú programhoz, az még nem feltétlenül válik kiberfegyverré. Nagyon fontos tehát a korábban már említett motiváció, illetve a kibertámadás céljának kérdése. Ugyanakkor talán éppen erre a két tényezőre nem derül egyértelműen fény, amikor egy-egy kibertámadást vizsgálunk.

Abban azonban a nemzetközi közösség egyetért, hogy fegyveres támadásnak minősíthető kibertámadás esetén a megtámadott országnak joga van önvédelemre. Ezt a jogot sok esetben az ENSZ Alapokmányának 51. cikkelyéből vezetik le.[177]

A *Tallinn Manual II* a hagyományos fegyverek körébe sorolja, és hozzájuk hasonló tartalommal határozza meg a kiberfegyverek fogalmát: „olyan kiberhadviselési eszközök, amelyeket személyek sérülésének, illetve halálának, valamint tárgyak károsodásának, illetve megsemmisítésének érdekében használnak, arra hoztak létre vagy terveztek használni, azaz amelyek a kiberművelet támadásként való minősítéséhez szükséges következményekkel járnak."[178] Ugyanakkor a jelenlegi

[177] 1956. évi I. törvény az Egyesült Nemzetek Alapokmánya törvénybe iktatásáról, 51. cikk.
[178] Schmitt (2016): i. m. 103. szabály. 452.

nemzetközi jog nagyon szigorúan definiálja a fegyver fogalmát, illetve annak alkalmazását. E szerint alapvetően a fegyveres támadás az, amelyet egy adott ország követ el másik ország ellen (benne az erre vonatkozó irányítás, utasítás, ellenőrzés szabályaival). Ennek megfelelően a kiberműveletek esetében annak eldöntése, hogy adott esetben fegyveres támadásnak minősülnek-e, alapvetően inkább az intenzitásuk alapján lehet inkább eldönthető, hiszen a kibertámadások mögött nem mindig államok állnak közvetlenül.[179] Ezt erősíti a *Tallinn Manual I* 13. szabályában kifejezett vélemény is, amely szerint a nemzetközi szakértői csoport egyhangúlag arra a következtetésre jutott, hogy egyes kiberműveletek elég súlyosak lehetnek ahhoz, hogy kimerítsék az ENSZ Alapokmánya értelmében vett „fegyveres támadás" fogalmát. Ez a következtetés összhangban van a Nemzetközi Bíróság nukleáris fegyverek legalitásáról szóló tanácsadó véleményében megfogalmazottakkal, miszerint a támadás eszközeinek megválasztása nem befolyásolja azt a kérdést, hogy egy művelet fegyveres támadásnak minősül-e.[180] Ugyanakkor a *Tallinn Manual II*-ben a kiberfegyverekre adott meghatározás közelebb vihet minket ahhoz, hogy egy adott kiberművelet esetében azonosítani tudjuk, mit is jelent a fegyver egy ilyen művelet során.

Sok szakértő mindemellett azon a véleményen van, hogy a nemzetközi jog hagyományos alkalmazása helyett inkább az alkalmazott eszközök, illetve eljárások kibertérműveletek során jelentkező közvetlen vagy közvetett hatásai alapján lehetséges meghatározni azok fegyver jellegét. Ehhez egyébként nagyon hasonló gondolat jelenik meg az új magyar nemzeti biztonsági stratégiában (amelyet más vonatkozásban korábban már idéztünk), amely szerint „Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat fegyveres agressziónak tekinti, amelyre a fizikai térben megvalósuló válaszadás is lehetséges".[181]

Mindezeket összefoglalva – a teoretikus diszkussziók mellett, vagy éppen azok helyett – kijelenthetjük, hogy gyakorlatilag bármely olyan kibertérben alkalmazható eszköz fegyvernek minősíthető, amely a célzott eszközt vagy rendszert elpusztítja vagy működésképtelenné teszi. Így a kiberfegyverek gyakran ugyanazok az eszközök, mint amelyeket a kibertéri tevékenységek – akár a kiberbűnözés – kapcsán már ismerünk. Ezek közül mutat be néhányat a következő táblázat.

[179] Kelemen (2015): i. m. 81.
[180] Schmitt (2013): i. m. 54.
[181] 1163/2020. (IV. 21.) Korm. határozat, 101. pont.

8. táblázat: Program típusú malware-ek és jellemzőik

Kategória	Jellemzők
Vírusok	A vírusok olyan rosszindulatú programok, amelyek saját programkódjukat egy másik programhoz hozzáfűzik, vagy azokba beépítik, önnön terjedésüket is biztosítva ezáltal. A gazdaprogramhoz való kapcsolódás módja változatos lehet: például a vírus saját programkódját beleírja a gazdaprogram kódjába, így módosítva azt. Korábban a vírusok egyik nagyon virulens és veszélyes fajtái a makróvírusok voltak. Ugyanakkor a ransomware-ek terjedése során látható, hogy ez ma újra igaz, hiszen egyes zsarolóvírusok sok esetben szintén makróvírusokkal nyitnak utat az áldozat számítógépén. A vírusok családján belül külön helyet foglalnak el a makróvírusok, amelyek valamely egyszerű (makró) programozási nyelvben megírva egy hasznos programhoz (például valamelyik Office-alkalmazáshoz) kapcsolódnak, és annak indításakor lefutnak.
Programférgek (worms)	A programférgek olyan önállóan futó, gazdaprogramot nem igénylő szoftverek, amelyek képesek saját maguk megsokszorozására. Másolataikat részben a megtámadott számítógép merevlemezén készítik el, részint pedig a hálózaton keresztül juttatják el a megfertőzni kívánt számítógépekre vagy hálózati elemekre.
Ransomware-ek	Zsarolóvírusok. A megfertőzött számítógépre jutva titkosítják a felhasználó fájljait. A titkosítás feloldását lehetővé tevő kódért váltságdíjat – pénzt vagy bitcoint – kérnek cserébe.
Trójai programok	A trójai programok látszólag hasznos szoftverekbe elrejtve fertőzik meg a számítógépet. Adatokat módosítanak, könyvtárakat, adatállományokat törölnek, backdoort nyitnak stb.
Backdoor-programok	A backdoorprogramok eredetileg a rendszer-adminisztrátorok vagy rendszerfelügyeleti jogokkal rendelkező személyek részére nyitottak olyan lehetőségeket, hogy a kívánt számítógépet távolról is elérhessék, és azon különböző javításokat, illetve beállításokat végezzenek. A rosszindulatú backdoorprogramok azonban jogosulatlanul próbálnak meg „hátsó ajtókat" nyitni a rendszerhez. Többségük e-mail- vagy egyéb letöltési „mellékleteként" érkezik. Az igazi veszélye a backdoorprogramoknak az, hogy remek megoldásokat nyújtanak a rendszeradminisztrációs jogok megszerzésére.
Dropperek	A dropperek a trójai programok speciális fajtájának tekinthetők, mivel hasonló elven kerülnek a számítógépbe. Ott azonban legyártanak kettő vagy több, az operációs rendszer által futtatható vírust, majd elindítják azokat. Mivel nem saját magát másolja a program, hanem új programot állít elő, ezeket nem lehet a klasszikus vírusok kategóriájába sorolni. A dropperek egyfajta vírushordozó vagy vírustároló programok.
Spyware	A kémprogramok a rendszerbe jutva, ott elrejtőzve, a háttérből figyelik a rendszer eseményeit, és ezekről jelentéseket, illetve adatokat küldenek.
Keyloggerek	A keyloggerek a háttérben települve a billentyűleütéseket – így akár a jelszavakat, bankkártyaszámokat, azonosítókat is – rögzítik, és kijuttatják ezeket az információkat a hálózaton keresztül.

Kategória	Jellemzők
Adware	Olyan programok, amelyek a felhasználó internetes szokásait figyelik és rögzítik, majd ezek alapján valamilyen szolgáltatást reklámoznak számára hirdetési bannerekkel vagy pop-upokkal. Sok esetben spyware-ként is viselkednek.
Scareware	Hamis vírusirtó szoftver, amely úgy tesz, mintha egy felhasználó eszközét ellenőrizné, és ott rosszindulatú programokat vagy biztonsági fenyegetéseket keresne. Ehelyett titkosítja a merevlemezt, így a felhasználónak fizetnie kell a titkosítás eltávolításáért. Egyfajta ransomware-ként működik.
Swiper	Általában valamely más malware egyéb funkcióját jelenti, amely különböző, jól meghatározott adatok (például banki bejelentkezési adatok, VPN-beállítási adatok, mentett bejelentkezési adatok) törlését végzi.
Rootkit	Olyan szoftvereszközök együttese, amelyek rendszergazdai jogosultsághoz juttatják a támadót az áldozat számítógépén. (A Unix/Linux rendszerek legfelsőbb szintű könyvtárának elnevezéséből – root- vagy gyökérkönyvtár – ered a kifejezés.)

Forrás: Kovács (2018b): i. m.

A fentiekben felsorolt – alapvetően informatikai – eszközök mindegyike minősülhet tehát kiberfegyvernek. Természetesen ez az adott eszköz alkalmazási módjától, céljától, illetve a felhasználás nagyságrendjétől is függ.

A kiberműveletek eddigi történetében már civil oldalon is jó néhány alkalommal volt arra példa, hogy kimondva vagy kimondatlanul, de egyértelműen kiberfegyverek alkalmazására került sor (anélkül természetesen, hogy ezt fegyveres támadásnak minősítették volna). Egy ilyen esemény volt a már említett Anonymous hacktivistacsoport által bevetett, úgynevezett *Low Orbit Ion Cannon* (LOIC) nevű szoftver alkalmazása. A LOIC alapvetően DDoS-támadások kivitelezésére alkalmas eszköz volt, amelyet megalkotója nyilvánosan elérhetővé tett az interneten 2008-ban.[182]

Azonban ennek az eszköznek a nyílt elérése is felhívja a figyelmet a kiberfegyverek kontroll nélküli proliferációjának és a kiberfegyverkezés versenyszerűvé válásának problémájára. Az ismert kiberbiztonsági szakember, Bruce Schneier ezzel kapcsolatban már 2012-ben kifejezte aggodalmát, miszerint bár akkor még csak a kiberfegyverkezési verseny korai szakaszában jártunk,

[182] Kovács László: Kiberháború? Internetes támadások a Wikileaks ellen és mellett. *Nemzet és Biztonság,* 4. (2011), 1. 3–8.

a helyzet önmagában mindenkire és mindenre, benne az internet teljes működésére nagy veszélyt jelentett.[183]

Ez a félelem nem volt és jelenleg sem teljesen alaptalan, amire a már idézett Stuxnet-ügy, illetve annak utóhatásai is rávilágítottak. A Stuxnet egyes elemeit ugyanis az Irán elleni támadás után, még jóval később is számos más országban detektálták.[184]

És akkor még nem is beszéltünk a kibertérben megvalósuló kémkedésről, amelynek legalábbis vegyes a megítélése, hiszen a jogtudósok egy csoportja szerint ezt nem tiltja a nemzetközi jog, míg mások szerint a kiberkémkedés csak addig nem tiltott, amíg nem gazdasági adatok ellopását szolgálja.[185]

Összefoglalva a fentieket kijelenthetjük, hogy a kiberfegyvereket és azok alkalmazását szükséges pontos és a kibertérre értelmezhető nemzetközi szabályozásnak alávetni. Olyan események tanúi lehettünk az elmúlt években, illetve évtizedben – mint az említett 2010-es, iráni atomlétesítmények elleni Stuxnet-támadás –, amelyek már önmagukban is rámutatnak: a kibertérben olyan stratégiai szintű támadások történhetnek, amelyek mögött államok állnak.[186] Hasonló példa a NoPetya zsarolóvírus támadássorozata is 2017-ben. Ez a ransomware-támadás, ellentétben a néhány héttel korábban világszerte hatalmas károkat okozó WannaCry vírussal, nem véletlenszerűen, hanem célzottan támadott meg számítógépeket. 2017. június végén a NoPetya (más néven PetrWrap) ransomware Ukrajnában egy könyvelőszoftver automatikus frissítésével terjedt, elsősorban belföldi számítógépeket megfertőzve. A háttérben ebben az esetben is egy ország – elemzések szerint Oroszország – állt.[187]

[183] Bruce Schneier: Cyberwar Treaties. *Schneier on Security,* 2012. június 14.
[184] Kovács–Sipos (2010): i. m.
[185] Mitnick (2012): i. m.
[186] Gary D. Brown – Andrew O. Metcalf: Easier Said Than Done: Legal Reviews of Cyber Weapons. *Journal of National Security Law & Policy,* 7. (2014). 115–138.
[187] Anton Ivanov – Orkhan Mamedov: In ExPetr/Petya's Shadow, FakeCry Ransomware Wave Hits Ukraine. *SecureList,* 2017. július 4.

9. táblázat: A kiberműveletek eszközeinek alkalmazás szerinti lehetséges csoportosítása

Kiberhírszerzés és -felderítés	Kibertámadás	Védelmi célú kiberművelet
Social engineering	DoS/DDoS	Sérülékenységvizsgálat
Keylogger	Ransomware	Hardveres és szoftveres biztonsági rendszerek
Spyware	Egyéb malware	Szabályozás
Információszivárogtatás	APT	

Forrás: a szerző szerkesztése

Ugyanakkor nem csak ezek az eszközök, illetve a bevetésükre használt leggyakoribb informatikai támadási módok vagy eljárások okozhatnak komoly károkat a kibertérben működő rendszereinknek. A fizikai térben történő pusztítás hasonló – ha nem nagyobb – károkat jelenthet. Ráadásul a fizikai pusztítás következményeinek felszámolása időben is jóval tovább tarthat, mint az informatikai eszközökkel elkövetett támadásoké. A kinetikus, illetve az elektromágneses fegyverek ezért különösen nagy veszélyt jelentenek a kibertéri rendszereink biztonságára. Ennek megfelelően ezek védelme ki kell hogy terjedjen a fizikai és az elektromágneses térből érkező fenyegetések elleni védelemre is.

A fentiek alapján arra a következtetésre juthatunk, hogy nemcsak a kiberfegyverek mibenlétét és alkalmazását szükséges pontosan és egyértelműen megfogalmazni a nemzetközi jogban, hanem a kiberhadviselés szabályait is le kell fektetni. Ezeket a kiberhadviselési szabályokat nemzetközi konszenzus alapján kell kialakítani, és a lehető legtöbb országban kell alkalmazni.

4.2. A kiberműveletek és a kiberhadviselés várható jövője

A kiberműveletek és a kiberhadviselés várható jövőjére vonatkozó teljesen biztos predikcióba bocsátkozni nagy felelőtlenség lenne. Ugyanakkor néhány olyan trend felvázolása, amely mentén a terület további fejlődése várható, talán nem öncélú.

Mielőtt ebbe belevágunk, fontos annak hangsúlyozása, hogy a jövő várhatóan még inkább a digitális technikára épül majd. Egyes becslések szerint a mai munkahelyek közel 50%-a meg fog szűnni a jövőben, legalábbis abban az értelemben, ahogyan ma ezekre a munkákra gondolunk. Ezzel párhuzamosan azonban olyan munkahelyek jönnek majd létre, amelyeket ma még csak részben tudunk előrejelezni. Ilyenek a digitális technika, a robotika vagy akár

az adattudományokhoz kapcsolódó munkakörök. Mindehhez természetesen a munkaköröket majdan betöltők oktatása, képzése és felkészítése is szükséges lesz. Az ezekhez szükséges eszközök, rendszerek és megoldások szintén digitális technikára és a mesterséges intelligenciára fognak épülni.

Biztonsági szempontból azonban az is nagy bizonyossággal előrejelezhető, hogy minél inkább digitalizált a társadalom, minél inkább átszövi a mindennapokat a technológia, annál inkább szükséges ezek lehető legmagasabb szintű biztonságáról gondoskodni. És éppen ez az a pont, amely jelenlegi tudásunk szerint a társadalom Achilles-inát jelentheti.

A kiberműveleti és -hadviselési trendek felvázolása három olyan főbb jellemző mentén történhet meg, amelyek már eddig is igen jól mutatják a kiberműveletek és a tágabb értelemben vett kiberhadviselés eddigi és várható természetét. Ez a három jellemző: a legfontosabb célpontok, a katonai jellemzők, illetve a technikai jellemzők. Mielőtt ezek elemzésére rátérnénk, az kijelenthető, hogy a nyílt, fegyveres támadásnak is minősíthető összecsapásokat a lehető legtovább fogja kerülni minden ország a jövőben is. Ez azt is jelenti, hogy jellemzően a mostani hibrid vagy szürke zónás műveletekhez hasonló, a fegyveres konfliktusok szintjét még el nem érő műveletekre kell készülnünk. (Amellett, hogy akár nagyobb méretű fegyveres konfliktus kitörése sem zárható ki teljes bizonyossággal Európában sem.)

Elnagyolt jövőkutatásunkat a várható jellemző célpontokkal kezdve kijelenthető, hogy azok szintén három nagy csoportra lesznek oszthatók a jövőben. Az első csoportba azok a civil célpontok tartoznak, amelyek leginkább a kritikus infrastruktúrák körébe sorolhatók be. Mivel várhatóan a digitális ökoszisztéma fejlődése és így a társadalom digitális ökoszisztémát alkotó rendszerektől való függősége még tovább fog nőni, a kibertámadások egyértelmű célpontjai továbbra is ezek a rendszerek lesznek. Az ezek ellen indított komplex, egymással összehangolt, esetleg több domainben is bekövetkező támadásokra nem vagyunk és várhatóan a közeljövőben sem leszünk teljes mértékben felkészülve. Ezek között külön kiemelt célpontokat fognak jelenteni azok a kritikus információs infrastruktúrák, amelyek a leginkább nélkülözhetetlenek, azaz valóban létfontosságúak a társadalom egészének működése szempontjából. Ilyenek az energiaellátás, azon belül is kiemelten a villamosenergia-ellátás vezérlőrendszerei. Rögtön e rendszerek után fog célpontként jelentkezni a kommunikációs és adatátviteli rendszerek összessége. Ezek szintén olyan célpontok, amelyek valódi Achilles-ínt jelentenek a digitális társadalom számára, hiszen nélkülük – az általuk megvalósuló, korábban már többször említett kölcsönös

függőség, azaz interdependencia miatt – számos más, egyébként önmagában is fontos rendszer működése fog ellehetetlenülni. A harmadik célpontcsoport várhatóan a közigazgatás lesz. Ennek támadásához a már most is tapasztalható APT-támadások során megszerzett információszerzés eredményei nyújtják majd a kiinduló adatokat. Ugyanakkor a közigazgatást ellehetetlenítő támadások csak akkor fognak bekövetkezni, amikor a nyílt, akár fegyveres összecsapás már elkerülhetetlenné válik. A közigazgatás megtámadása, kombinálva az említett kritikus infrastruktúrák, illetve a kommunikációs rendszerek elleni műveletekkel, hatalmas kihívás elé állíthatja a célországot, illetve akár az egész régiót, hiszen a kritikus infrastruktúrák országhatárokon átnyúló összekapcsoltsága révén a kiterjedt és komplex támadások hatásai nem csak az adott országban jelentkeznek. A közigazgatás nélkül viszont sem a helyreállítási, sem a kölcsönös segítségnyújtáshoz szükséges nemzetközi együttműködés nem lesz elérhető. A célpontok negyedik csoportját a bankrendszer digitális infrastruktúrája fogja jelenteni. Egy adott országban, sőt a többi kritikus infrastruktúra-ágazathoz hasonlóan a banki és pénzügyi szolgáltatások támadása, illetve azok működésének ellehetetlenítése az ország működőképességének teljes leállásához vezethet. A jelenlegi és a közeljövőben várható biztonságpolitikai helyzetben a banki és pénzügyi szolgáltatások támadása sokkal nagyobb előnnyel és haszonnal kecsegtet a támadó részére, mint ha a katonai vagy nemzetbiztonsági rendszereket támadná közvetlenül, hiszen az ország gazdasági rendszerének gerincét a bankrendszer szolgáltatja.

A katonai jellemzők esetében az nagy valószínűséggel előrejelezhető, hogy a hadseregeknek egyszerre kell helytállniuk a katonai rendszerek védelme és támadása, valamint a civil rendszerek védelme és támadása területén. Ez azonban szintén hatalmas kihívás elé fogja állítani katonai erőket, hiszen ezek érdekében a legaktuálisabb technikai eszközrendszerrel, a szükséges legfrissebb információkkal, valamint a legújabb eljárási módokkal kell rendelkezniük. Ehhez olyan civil és katonai mérnöki tudásra lesz szükség, amely a hadseregek jelenlegi finanszírozási és humánerőforrás-kezelési gyakorlatán jóval túlmutat. Magyarul ez azt jelenti, hogy a hadseregeknek is legalább olyan számú és olyan tudású mérnöki állományt kell alkalmazniuk, mint a civil szereplőknek, hogy ezt a kihívást kezelni tudják. Ehhez még hozzájárul a tény, amely szintén hatalmas anyagi erőforrásigénnyel jelentkezik, hogy a legaktuálisabb kibertéri információkat, trendeket, kihívásokat és veszélyeket, valamint az ezek kezelésére szolgáló információkat meg kell ismerni – jellemzően civil forrásból –, ami folyamatos kapcsolattartást igényel a civil kiberbiztonsági vállalatokkal. Ennek keretében

aktuális és releváns adatbázisokhoz kell hozzáférni, mérnöki szolgáltatásokat kell igénybe venni.

A fentiekhez adódik még a digitalizált harcmező révén megjelenő multidomain-műveletek összessége, illetve az elosztott műveletek már ma is meglévő problematikája. Az egy időben, több domainben és több fizikai helyen történő művelet-végrehajtáshoz megfelelően robusztus és rugalmasan alakítható, magas szintű kibervédelemmel rendelkező digitalizált vezetés-irányítási rendszerek működtetése lesz szükséges.

Ugyanakkor a fegyverrendszerekben is óriási változás várható, hiszen katonai területen mind a levegőben, mind a szárazföldön egyre inkább elterjednek az önvezető járművek, amelyek a jövőben már nemcsak logisztikai, szállítási és egyéb támogatási feladatokat látnak el, hanem ahogy a drónok esetében már közel egy évtizede látható, egyre inkább harci, azaz fegyveres feladatokat vesznek át a katonáktól. Ehhez járul még a mesterséges intelligencia megjelenése, amely a hadseregek vonatkozásában nemcsak etikai kérdéseket vet fel – azaz dönthet-e a számítógép, illetve annak egyik algoritmusa például arról, hogy emberrel szemben fegyvert használjon-e –, hanem komoly kibervédelmi kérdéseket is. A mesterségesintelligencia-alapú fegyverirányítás maximális biztonsága elengedhetetlen lesz a jövőben.

Mindezekkel párhuzamosan megjelenik annak a problematikája, hogy az igen fejlett, a fenti technológiákat magukban foglaló fegyverrendszerek természetszerűleg önmagukban is célpontok lesznek. Ez egyrészt jelenthet közvetlen fenyegetést magukra a fegyverrendszerekre, mert az azokban alkalmazott számítógépek, számítógép-hálózatok és elektronikai eszközök esetleges sérülékenységeiken keresztül támadhatók. Másrészről közvetett fenyegetést hordoz a korábban már említett beszállítói láncba, illetve annak egyes elemeibe történő, a későbbi károkozás céljából történő rosszindulatú beavatkozás.

Külön ki kell emelni a hadseregek és a civil vállalatok kapcsolatát. Azt már ma is látjuk, hogy a beszállítói lánc, illetve annak biztonsága kiemelt fontosságú. A hadseregekben alkalmazott információtechnológiai eszközök jelentős része nem haditechnikai cégek kutatás-fejlesztése és gyártása révén áll rendelkezésre, hanem civil cégek akár több tucat beszállító közreműködésével történő gyártása jelenti ezeknek a hátterét. Az így kialakuló beszállítói láncban a biztonság fenntartása és folyamatos ellenőrzése komoly feladat lesz.

A harmadik nagy jellemző a technikai kihívások és azok kezelésének csoportja. Talán ez az egyik legnehezebben előrejelezhető problémaegyüttes. Persze rögtön meg kell vallanunk, hogy a jövő technikai és technológiai jellemzői

minden bizonnyal kihatással lesznek a kiberműveletek célpontjaira, csakúgy, mint a katonai terület minden egyes jellemzőjére is.

A technikai terület részletes előrejelzése helyett három kérdésre kell felhívnunk a figyelmet. Mind a három egyben kihívást és nagyon éles, országok közötti versenyt is jelent. Az első kérdés a mesterséges intelligencia kérdése. Az MI a fentiekben eddig jellemzett mindkét területen, tehát a kiberműveletek, valamint a katonai műveletek területén is hatalmas kihívást jelent, hiszen aki a versenyben először ér el eredményeket, az technikai fölényre tesz szert. A verseny pedig rendkívül nagy, mert Kína tudatosan MI-nagyhatalommá kíván válni 2030-ra, ami természetszerűleg az olyan versenytársak, mint az Egyesült Államok vagy akár az Európai Unió e területen folytatott tevékenységére hatással kell hogy legyen.

A második kérdés a kvantum-számítástechnika kérdése. Az eddigi kezdeti eredmények birtokában már kijelenthető, hogy aki előbb éri el a kvantumfölényt, azaz előbb képes valóban működő és a gyakorlatban is használható kvantumszámítógépet építeni, az már-már behozhatatlan előnyre tesz szert. A kvantumtechnológia komoly kihívást, a másik oldalról nézve persze komoly előnyöket jelent többek között a titkosítás, illetve a kriptográfiára épülő biztonsági megoldások, így akár az online banki szolgáltatások, online kereskedelem vagy például a biztonságos kommunikáció területein. Ennek oka a kvantumszámítógépekben van, amelyek jelenlegi tudásunk szerint a ma alkalmazott kriptográfiai algoritmusokat rendkívül gyorsan képesek megfejteni, azokat dekódolni.

Ezzel el is jutottunk a harmadik nagy technikai kihíváshoz, amelyet a blokklánc-technológia jelent. Ez persze szintén nemcsak kihívást, hanem lehetőségeket is jelent, hiszen a mai, alapvetően kriptovaluták esetében megismert blokklánc-technológia számos helyen, akár a logisztikában, akár kommunikációban nagyon erős biztonsági megoldások kialakításához vezethet.

A jövőben az 5G mobilkommunikációs technológia segítségével az IoT-re épülő eszközök és rendszerek további térnyerése várható. Ebben a biztonság, ha lehet, még fontosabb kérdéssé fog válni, mint ma, hiszen számos helyen emberi beavatkozás nélkül zajlanak majd a fizikai térre is kiható interakciók. Az 5G mobilkommunikációs technológia így egy következő technikai kihívás elé állítja a jövő kiberműveleteinek harcosait, mind támadó, mind védelmi szempontból.

Kiberbiztonsági szempontból az 5G technológia előretörése és többek között az IoT-rendszerek alapját képező megvalósításai olyan kihívásokat jelentenek majd, mint például a decentralizált hardver- és szoftverösszetevők, a korábbi hardveres környezet helyett alkalmazott szoftveres virtualizációs környezet,

valamint maga a vezeték nélküli, viszonylag könnyen elérhető és alacsony költségekkel zavarható összeköttetés megvalósítása.[188]

10. táblázat: A kiberműveletek egyes jövőbeni lehetséges célpontjai és azok jellemzői

	Célpontok	Jellemzők
Civil célpontok	5G rendszerek	Komplex hatás azokra a szolgáltatásokra és rendszerekre, amelyeknek alapjait képezik
	Mesterségesintelligencia-alapú rendszerek, kritikus infrastruktúrák	Sérülékenységeik révén támadhatók
Katonai célpontok	Vezetés-irányítási rendszerek	A támadó információs fölénybe kerül
	Fegyverirányítási rendszerek	A támadó műveleti fölénybe kerül

Forrás: a szerző szerkesztése

Az 5G, illetve az IoT jellemezte technológia az ipart sem kerülte el. Az Ipar 4.0 – mint az ipari fejlődés, ha tetszik, az ipari forradalom negyedik szakasza – abszolút módon az információtechnológiára épül. Az ebben megjelenő sérülékenységek, illetve azok rosszindulatú kihasználása egyre nagyobb kihívást és veszélyt jelent nemcsak egy adott rendszerelemre, hanem az összekapcsoltság révén az egész komplex rendszerre vagy rendszerekre. Ennek megfelelően a jövőben az ipar és az ipari termelés minden egyes szakasza kibertámadások célpontjává válhat.

A technikai jellemzők előrejelzése során azonban nem szabad elfelejtenünk Ray Kurzweil szingularitáselméletét.[189] Ez nagyon komoly figyelmeztetés arra, hogy a technikai fejlődés eljuthat arra a szintre, amikor már nem az emberek a motorjai, hanem maga a technika és a technológia. Gépek terveznek gépeket, emberi beavatkozás és – ami még nagyobb kihívás – emberi kontroll nélkül. Ennek hatásai kiszámíthatatlanok.

Mindezek alapján a jövő kiberműveleteire és a tágabb értelemben vett kiberhadviselésre is nagy valószínűséggel olyan hatással lesz a technológiai változás, amely a jelenleginél még jobban felértékeli e területek fontosságát.

[188] Tom Wheeler – David Simpson: Why 5G Requires New Approaches to Cybersecurity. *Brookings,* 2019. szeptember 3.

[189] Ray Kurzweil: *A szingularitás küszöbén.* Budapest, Ad-Astra, 2013.

A jövőről való gondolkodásunknak mindenképpen része kell hogy legyen az olyan szervezetek kiberbiztonsággal és kiberműveletekkel kapcsolatos jövőjéről szóló elmélkedés, mint például a NATO. A szövetség az 1949-es megalakítása óta számos olyan kisebb-nagyobb átalakítást ért már meg, amelyek többsége a geopolitikai és/vagy a nemzetközi katonai erőviszonyok átalakulása miatt következett be. Egy azonban nem változott a NATO életében, ez pedig a szövetség elkötelezettsége a tagállamok és ezen keresztül a nemzetközi biztonság iránt. Ez várhatóan a jövőben is így lesz, ami megköveteli, hogy a NATO is reagáljon az olyan kihívásokra, amelyeket jelen könyv lapjain is igyekeztünk számba venni. A kiberbiztonsággal és a legutóbbi időkben a kiberműveletekkel kapcsolatban a NATO hatalmas lépéseket tett a szövetség egységes képességeinek megteremtése érdekében. Mindez várhatóan a jövőben is igaz lesz, hiszen a 2030-as kitekintéssel készült jövőelemző dokumentum előkelő helyet szentel a kiberbiztonságnak és a kiberműveleteknek: „A NATO-tagállamok lakossága elvárja, hogy megvédjék őket az olyan új fenyegetések ellen, mint amit a kiberveszélyek és a félretájékoztatás jelent, továbbá hogy kormányaik a NATO támogatásával eszközöket dolgozzanak ki az elkövetők megnevezésére és az elrettentésre. A rezilienciának a társadalmakban és az államban is meg kell lennie."[190]

[190] NATO: *NATO 2030: United for a New Era* (2020. november 25.).

Felhasznált irodalom

Aselsan: *Next Generation Main Battle Tank Upgrade Solutions* (2022). Online: www.aselsan.com.tr/Next_Generation_Main_Battle_Tank_Upgrade_Solutions_8232.pdf

Bergman, Ronen – Rick Gladstone – Farnaz Fassihi: Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage. *The New York Times,* 2021. április 11. Online: www.nytimes.com/2021/04/11/world/middleeast/iran-nuclear-natanz.html

Broad, William J. – John Markoff – David E. Sanger: Israeli Test on Worm Called Crucial in Iran Nuclear Delay. *New York Times,* 2011. január 16. Online: www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&scp=2&sq=stuxnet&st=cse

Brown, Gary D. – Andrew O. Metcalf: Easier Said Than Done: Legal Reviews of Cyber Weapons. *Journal of National Security Law & Policy,* 7. (2014). 115–138. Online: http://jnslp.com/wp-content/uploads/2014/02/Easier-Said-than-Done.pdf

Bundeswehr: *Kommando Cyber- und Informationsraum* (2021a). Online: www.bundeswehr.de/de/organisation/cyber-und-informationsraum

Bundeswehr: *The Cyber and Information Domain Service* (2021b). Online: www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service

Bundeswehr: *Zentrum für Cyber-Sicherheit der Bundeswehr* (2021c). Online: www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-informationstechnik-der-bundeswehr/zentrum-fuer-cyber-sicherheit-der-bundeswehr

Burgess, Matt: The UK Created a Secretive, Elite Hacking Force. Here's What It Does. *Wired,* 2020. november 20. Online: www.wired.co.uk/article/national-cyber-force-uk-defence-gchq

Castells, Manuel: *A hálózati társadalom kialakulása. Az információ kora. Gazdaság, társadalom, kultúra.* I. kötet. Budapest, Gondolat–Infonia, 2005.

Cicvaric, Petra: Cyber Security – A Strategic Security Priority for NATO. *Atlantic Forum,* 2019.

CISA: Ransomware 101. *Stop Ransomware,* 2022. Online: www.cisa.gov/stopransomware/ransomware-101

Colonial Pipeline Boss Confirms $4.4m Ransom Payment. *BBC News*, 2021. május 19. Online: www.bbc.com/news/business-57178503

Corera, Gordon: UK's National Cyber Force Comes out of the Shadows. *BBC News*, 2020. november 20. Online: www.bbc.com/news/technology-55007946

Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps. *Times of Israel,* 2020. július 17. Online: www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/

Cyber Security Training Centre of Excellence: *What We Do* (2021). Online: https://cstcoe.mil.pl/en/pages/what-we-do/

Ertan, Amy – Kathryn Floyd – Piret Pernik – Tim Stevens (szerk.): *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2020. Online: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

Európai Bizottság: *Közös közlemény az Európai Parlamentnek és a Tanácsnak. Az EU kiberbiztonsági stratégiája a digitális évtizedre.* JOIN(2020) 18 final (2020. december 16.).

Európai Közösségek Bizottsága: *Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról.* COM(2005) 576 végleges (2005. november 17.). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52005DC0576&from=IT

Európai Közösségek Bizottsága: *A Bizottság közleménye a létfontosságú infrastruktúrák védelmére vonatkozó európai programról.* COM(2006) 786 végleges (2006. december 12.). Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:52006DC0786

European Commission: *Digital Economy and Society Index (DESI). 2019 Country Report. Hungary.* Online: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59898

European Commission: *Digital Economy and Society Index (DESI) 2020. Thematic Chapters.* Online: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=67086

European Union Agency for Cybersecurity: *ENISA Threat Landscape 2021. April 2020 to Mid-July 2021* (2021a. október). Online: www.enisa.europa.eu/publications/enisa-threat-landscape-2021

European Union Agency for Cybersecurity: *Methodology for Sectoral Cybersecurity Assessments. EU Cybersecurity Certification Framework* (2021b. szeptember). Online: www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment

European Union Agency for Cybersecurity: *National Cybersecurity Strategies: With a Vision on Raising Citizens' Awareness* (2021c. november 29.). Online: www.enisa.europa.eu/news/enisa-news/national-cybersecurity-strategies-with-a-vision-on-raising-citizens2019-awareness

European Union Agency for Network and Information Security: *ENISA Overview of Cybersecurity and Related Terminology.* 1. változat (2017. szeptember).

Online: www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology/at_download/file

FireEye: *Advanced Persistent Threat Groups. Mandiant,* 2021. Online: www.fireeye.com/current-threats/apt-groups.html

FireEye–Mandiant: *M-Trends. 2021. FireEye Mandiant Services – Special Report.* 2021. Online: https://content.fireeye.com/m-trends/rpt-m-trends-2021

Fleming, T. Casey – Eric L. Qualkenbush – Anthony M. Chapa: The Secret War Against the United States. The Top Threat to National Security and the American Dream. Cyber and Asymmetrical Hybrid Warfare. An Urgent Call to Action. *The Cyber Defense Review,* 2. (2017), 3. 25–31. Online: https://cyberdefensereview.army.mil/Portals/6/Documents/CDR-FALL2017.pdf?ver=2017-11-21-092725-887

GCHQ: *Cyber Security. Making the UK the Safest Place to Live and Do Business Online* (2021). Online: www.gchq.gov.uk/section/mission/cyber-security

Global Research & Analysis Team: BlackEnergy APT Attacks in Ukraine Employ Spearphishing with Word Documents. *SecureList,* 2016. január 28. Online: https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440

Gyányi Sándor: DDOS-támadások veszélyei és az ellenük való védekezés. *Hadmérnök,* (2007), különszám. Online: http://hadmernok.hu/kulonszamok/robothadviseles7/gyanyi_rw7.html

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

Haig Zsolt – Kovács László – Munk Sándor – Ványa László: *Az infokommunikációs technológia hatása a hadtudományokra.* Budapest, Nemzeti Közszolgálati Egyetem, 2013.

Haig Zsolt – Kovács László – Ványa László: Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata. *Felderítő Szemle,* 10. (2011), 1–2. 183–209.

Haig Zsolt – Kovács László – Vass Sándor – Ványa László: *Felderítési és zavarási technikák vizsgálata. Tanulmány a Jedlik Ányos Program – 2. alprogram: Versenyképes Ipar NKFP_07_2-HT28_SAJ program keretében kidolgozásra tervezett integrált elektronikai felderítő és zavaró rendszerhez.* Budapest, ZMNE, 2008.

International Institute for Strategic Studies: *Cyber Capabilities and National Power: A Net Assessment* (2021. június 28.). Online: www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

Interpol: *Cybercrime:Covid-19 Impact.* Lyon, Interpol General Secretriat, 2020. Online: www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

ITU: *ITU-T Recommendations* (2012. június 15.). Online: www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

ITU: *Definition of Cybersecurity* (2021a). Online: www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

ITU: *Global Cybersecurity Index 2020.* Geneva, International Telecommunications Union, 2021b. Online: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Ivanov, Anton – Orkhan Mamedov: In ExPetr/Petya's Shadow, FakeCry Ransomware Wave Hits Ukraine. *SecureList,* 2017. július 4. Online: https://securelist.com/in-expetrpetyas-shadow-fakecry-ransomware-wave-hits-ukraine/78973

Jaikaran, Chris: *Cybersecurity: Selected Cyberattacks, 2012-2021.* Washington (D.C.), Congressional Research Service, 2021. Online: https://crsreports.congress.gov/product/pdf/R/R46974

Jenkins, Luke – Sarah Hawley – Parnian Najafi – Doug Bienstock: Suspected Russian Activity Targeting Government and Business Entities Around the Globe. *Mandiant Blog,* 2021. december 6. Online: www.mandiant.com/resources/russian-targeting-gov-business

Kelemen Roland – Pataki Márta: A kibertámadások nemzetközi jogi értékelése. *Katonai Jogi és Hadijogi Szemle,* (2015), 1. 53–90. Online: http://epa.oszk.hu/02500/02511/00004/pdf/EPA02511_katonai_jogi_szemle_2015_01_053-090.pdf

Kiss Álmos Péter: A hibrid hadviselés természetrajza, *Honvédelmi Szemle,* (2019), 4. 17-37. Online: https://honvedelem.hu/files/files/116701/hsz_2019_4_017_037_4557.pdf

Kovács László: Kiberháború? Internetes támadások a Wikileaks ellen és mellett. *Nemzet és Biztonság,* 4. (2011), 1. 3–8.

Kovács László: Az elektronikai hadviselés jelene és lehetséges jövője. *Hadmérnök,* 12. (2017), 1. 213–232. Online: www.hadmernok.hu/171_17_kovacs.pdf

Kovács László: *A kiberbiztonság stratégiai megközelítése.* Doktori értekezés. Budapest, Magyar Tudományos Akadémia, 2018a.

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

Kovács László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018c.

Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új nemzeti biztonsági stratégiájában. *Honvédségi Szemle,* 148. (2020), 5. 3–18. Online: https://doi.org/10.35926/HSZ.2020.5.1

Kovács László – Krasznay Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Elemzések,* (2017), 9.

Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van: tények és a cyberháború hajnala. *Hadmérnök,* 5. (2010), 4. 163–172. Online: www.hadmernok.hu/2010_4_kovacs_sipos.pdf

Leinhos, Ludwig: The German Cyber and Information Domain Service as a Key Part of National Security Policy. *Ethics and Armed Forces,* (2019), 1. Online: www.ethikundmilitaer.de/en/full-issues/20191-conflict-zone-cyberspace/leinhos-the-german-cyber-and-information-domain-service-as-a-key-part-of-national-security-policy/

Lété, Bruno – Peter Chase: *Shaping Responsible State Behavior in Cyberspace.* Washington, The German Marshall Fund of the United States, 2018. Online: https://nato-engages.org/wp-content/uploads/2018/07/Shaping-Responsible-State-Behavior-in-Cyberspace.pdf

Lockheed Martin: *The Cyber Kill Chain* (2021). Online: www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Maaten, Epp – Toomas Vaks: *National Cyber Security in Practice.* Tallinn, E-Governance Academy, 2020. Online: https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf

Magyar Honvédség: *Információs műveletek doktrína* (2014). 1. kiadás. MD 3.10.1 (1), Ált/57.

Mitnick, Kevin: *Ghost in the Wires.* New York, Back Bay Books, 2012.

Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány,* (2018), 1. 113–131.

National Cyber Force Transforms Country's Cyber Capabilities to Protect UK. Gov.uk, 2020. november 19. Online: www.gov.uk/government/news/national-cyber-force-transforms-countrys-cyber-capabilities-to-protect-uk

National Cyber Security Centre: *Defining Artificial Intelligence* (2019. április 18.). Online: www.ncsc.gov.uk/collection/intelligent-security-tools/defining-artificial-intelligence

National Security Archive: *USCYBERCOM 30-Day Assessment of Operation Glowing Symphony: Executive Summary* (2016. december 13.). Online: https://nsarchive.gwu.edu/dc.html?doc=6655596-National-Security-Archive-5-USCYBERCOM

National Security Archive: *Cyber Brief: Cyberspace Solarium Commission Recommendations in the FY21 National Defense Authorization Act* (2020. december 21.). Online: https://nsarchive.gwu.edu/news/cyber-vault/2020-12-21/cyberspace-solarium-commission-recommendations-in-fy21-ndaa

NATO: *Media – (Dis)Information – Security* (é. n.). Online: www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal2-troll-factories.pdf

NATO: *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation Adopted by Heads*

of State and Government in Lisbon (2010. november 19./2022. július 1.). Online: www.nato.int/cps/en/natolive/official_texts_68580.htm

NATO: *Cyber Defence Pledge* (2016a. július 8.). Online: www.nato.int/cps/su/natohq/official_texts_133177.htm

NATO: *Warsaw Summit Communiqué* (2016b. július 9.). Online: www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO: *High Level Taxonomy of Cyberspace Operations.* A 3400 TSC FCX-0010/TT-180202/Ser:NU0171. sz. dokumentum „A" melléklete (2018).

NATO: *NATO 2030: United for a New Era* (2020. november 25.). Online: www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

NATO: *Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise* (2021. július 19.). Online: www.nato.int/cps/en/natohq/news_185863.htm

NATO: *Cyber Defence* (2022a. március 23.). Online: www.nato.int/cps/en/natohq/topics_78170.htm

NATO: *Deterrence and Defence* (2022b. július 6.). Online: www.nato.int/cps/en/natohq/topics_133127.htm

NCSI Project Team: *National Cyber Security Index* (2021). Online: https://ncsi.ega.ee/ncsi-index/

Nemzeti Kibervédelmi Intézet: *Riasztás Apache Log4j könyvtárt érintő kritikus sérülékenységgel kapcsolatban* (2021. december 12.). Online: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-apache-log4j-konyvtart-erinto-kritikus-serulekenyseggel-kapcsolatban/

Nemzeti Közszolgálati Egyetem: *Kiberbiztonsági mesterképzési szak* (2021). Online: https://antk.uni-nke.hu/oktatas/mesterkepzes/kiberbiztonsagi-mesterkepzesi-szak

Newman, Lily Hay: What We Know About Friday's Massive East Coast Internet Outage. *Wired,* 2016. október 21. Online: www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

NIST: *Artificial Intelligence* (2022). Online: www.nist.gov/artificial-intelligence

Nyman-Metcalf, Katrin: A Legal View on Outer Space and Cyberspace: Similarities and Differences. *The Tallinn Papers,* (2018), 10. Online: https://ccdcoe.org/uploads/2018/10/Tallinn-Paper_10_2018.pdf

Paganini, Pierluigi: Germany Makes Its Cyber Capabilities Available for NATO Alliance. *Security Affairs,* 2019. február 15. Online: https://securityaffairs.co/wordpress/81125/cyber-warfare-2/germany-nato-alliance-warfare.html

Paris Call for Trust and Security in Cyberspace. *Pariscall.international,* 2018. november 12. Online: https://pariscall.international/en/

Perlroth, Nicole: In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. *The New York Times,* 2012. október 23. Online: www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

Pomerleau, Mark: What Cyber Command's ISIS Operation Means for the Future of Information Warfare, *C4ISRNet,* 2020. június 18. Online: www.c4isrnet.com/information-warfare/2020/06/18/what-cyber-commands-isis-operations-means-for-the-future-of-information-warfare/

Pupillo, Lorenzo – Afonso Ferreira – Stefano Fantin: *Artificial Intelligence and Cybersecurity.* Brussels, CEPS, 2020. Online: www.ceps.eu/ceps-publications/artificial-intelligence-and-cybersecurity/

Rheinmetall: *MBT Revolution: Rheinmetall's Mission-Oriented, Modular Upgrade Package for Main Battle Tanks* (2010. június 14.). Online: www.rheinmetall-defence.com/en/rheinmetall_defence/public_relations/news/detail_1408.php

Samartsev, Dmitry: *Cybercrime Is Maturing. Here Are 6 Ways Organizations Can Keep Up.* (H. n.), World Economic Forum, 2020.

Sanger, E. David: After Russian Cyberattack, Looking for Answers and Debating Retaliation. *The New York Times,* 2021. február 23.

SANS: *Analysis of the Cyber Attack on the Ukrainian Power Grid* (2016. március 18.). Online: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

Sayfayn, Nabil – Stuart Madnick: Cybersafety Analysis of the Maroochy Shire Sewage Spill (Preliminary Draft). *Working Paper CISL,* 2017. május. Online: https://web.mit.edu/smadnick/www/wp/2017-09.pdf

Schmitt, Michael N. (szerk.): *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York, Cambridge University Press, 2013.

Schmitt, Michael N. (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* New York, Cambridge University Press, 2016.

Schneier, Bruce: Stuxnet. *Schneier on Security,* 2010. október 7. Online: www.schneier.com/blog/archives/2010/10/stuxnet.html

Schneier, Bruce: Cyberwar Treaties. *Schneier on Security,* 2012. június 14. Online: www.schneier.com/blog/archives/2012/06/cyberwar_treati.html

Slay, Jill – Michael Miller: Lessons Learned from the Maroochy Water Breach. In Eric Goetz – Sujeet Shenoi (szerk.): *Critical Infrastructure Protection.* Az International Conference on Critical Infrastructure Protection (ICCIP) című konferencia

anyaga. (H. n.), Springer, 2007. 73–82. Online: https://link.springer.com/content/pdf/10.1007/978-0-387-75462-8_6.pdf

Suits, Devon: Futures and Concepts Center Evaluates New Force Structure. *Army.mil,* 2020. április 22. Online: www.army.mil/article/234845/futures_and_concepts_center_evaluates_new_force_structure

The Lazarus Heist: How North Korea Almost Pulled off a Billion-Dollar Hack. *BBC News,* 2021. június 21. Online: www.bbc.com/news/stories-57520169

Tradoc: *The U.S. Army in Multi-Domain Operations 2028.* TRADOC Pamphlet 525-3-1 (2018. december 6.). Online: https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf

UK Ministry of Defence – NATO: *Allied Joint Doctrine for Cyberspace Operations.* AJP-3.20, „A" kiadás, 1. változat (2020. január). Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Universität der Bundeswehr München: *Studiengang Cyber-Sicherheit* (2021). Online: www.unibw.de/inf/studium/studiengang-cyber-sicherheit

U.S. Cyber Command: *Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command* (2018. április). Online: www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf

U.S. Department of Defence: *The DoD Cyber Strategy* (2015. április). Online: www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/dod_cyber_2015.pdf

U.S. Department of State: *Joint Statement on Advancing Responsible State Behavior in Cyberspace* (2019. szeptember 23.). Online: www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/

Ványa László: Út a szoftverrádiók és szoftverrádió-zavaró állomások felé. In Rajnai Zoltán (szerk.): *Kommunikáció – Communications, 2006.* Konferenciakötet. Budapest, ZMNE, 2006. 76–83. Online: www.puskashirbaje.hu/index_html_files/Kommunikacio_2006-NSZTK.pdf

Wakefield, Jane: One Fastly Customer Triggered Internet Meltdown. *BBC News,* 2021. június 9. Online: www.bbc.com/news/technology-57413224

Wheeler, Tom – David Simpson: Why 5G Requires New Approaches to Cybersecurity. *Brookings,* 2019. szeptember 3. Online: www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

Zeit Online: Bundeswehr rüstet gegen Attacken aus dem Internet. *Die Zeit,* 2016. április 26. Online: www.zeit.de/politik/deutschland/2016-04/ursula-von-der-leyen-bundeswehr-aufruestung-cyberkrieg-angriffe-internet

Zhao, Christina: SolarWinds, Probably Hacked by Russia, Serves White House, Pentagon, NASA. *Newsweek,* 2020. december 14. Online: www.newsweek.com/solar-winds-probably-hacked-russia-serves-white-house-pentagon-nasa-1554447

Jogi források

1139/2013. (III. 21.) Korm. határozat
1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról
2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
2013. évi L. törvény az állami és önkormányzati szervezetek elektronikus információbiztonságáról
2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról
65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
1956. évi I. törvény az Egyesült Nemzetek Alapokmánya törvénybe iktatásáról

Vákát

E könyv azoknak az érdeklődőknek szól, akik világosabb képet szeretnének kapni napjaink és a jövő egyik legperspektivikusabb biztonsági és védelempolitikai kihívásáról, a kiberhadviselésről.

A történelemben ősidők óta zajlanak háborúk, megvívásuk módjai pedig mindig összefüggtek az adott technikai és technológiai színvonallal. A hadviselés tehát utóbbiak fejlődésével változik ma is. A digitális kor célja már nem elsősorban az élőerő pusztítása: a támadó az infokommunikációs rendszerekkel a hadseregvezetés működésének korlátozását, bénítását igyekszik elérni. A digitális rendszerek globalitása révén a hadviselés ma már a mindennapokban is jelen lehet: főként a befolyásolásban és a hétköznapi élethez szükséges létfontosságú rendszerek támadása által. A mesterséges intelligencia és a robotok katonai alkalmazása, a számítógépes vezetés és fegyverirányítás vagy éppen az ezek ellen intézett támadások szintén egyre inkább a katonai gondolkodás, a katonai műveletek szerves részeivé válnak.

E kötet a mindennapok részévé vált kiberműveletek és a tágabb értelemben vett kiberhadviselés összetevőit, eljárásait, várható eredményeit és hatásait vizsgálja meg. Elemzi a hagyományos és a kiberhadviselés kapcsolatát, a legfontosabb kibertéri eseményeket is. Górcső alá veszi, hogy a hadseregek milyen szervezetekkel készülnek fel a védelem mellett az offenzív kiberműveletek, a támadó jellegű kibertevékenységek végrehajtására.

9 789635 317653