NEMZETI KÖZSZOLGÁLATI EGYETEM

Katonai Műszaki Doktori Iskola

Ambrus Éva

Kiberhadviselési képességek a jelen tükrében

Doktori (PhD) értekezés tervezet

Témavezető:

Prof. Dr. Kovács László ddtbk.

.....

Budapest, 2023

Tartalomjegyzék

Bevezetés

„A jövő már itt van – csak nem egyenletesen oszlik el”[1] *[1]*

A modern hadseregek képességfejlesztése elengedhetetlen a legújabb műveleti dimenzióban, a kibertérben. Ennek összeegyeztetése a hagyományos haderő szervezetével, kultúrájával, majd integrálása tudományos kutatómunkát igényel. Ezt a kutatómunkát végeztem el a Katonai Műszaki Doktori Iskola keretében, és valósul meg munkám során - osztályvezetőként közreműködve - a Magyar Honvédség Kiber és Információs Műveleti Központban.

A kibertér bővülése robbanásszerű volt az elmúlt évtizedekben. Az azt megalapozó technológia központi szereplővé válásával, az összekapcsoltságunk növekedésével a kibertér a többségünk életében egyre nagyobb szerepet kap: az e-ügyintézésnél, az online fizetésnél és a VoIP[2]-szolgáltatások használatakor. A mostani, egyetlen nagy kibertérben a katonai és a polgári „struktúrák” és „személyek” elkülönítése – már csak a hatásait tekintve, az összekapcsoltság okán – szinte lehetetlen.

Természetes, hogy a technológia fejlődéssel a kibertér saját jogán külön dimenzióvá vált a szárazföld, a légi, a vízi és az űr dimenziói mellett a hadviselésben. Azonban azt is figyelembe kell venni, hogy a kibertér átmetszi ezeket a dimenziókat, egyszerre „külön” dimenzió, és a többi dimenziót átszövő „háló”. Amennyire a digitalizáció haladt előre a társadalomban és a haderőben, úgy vált létszükségletté az infrastruktúrák védelme, ezért a tudományos és a gyakorlati életben a hangsúly sokáig a kiberbiztonságon és a kibervédelmen volt elsősorban. Az utóbbi években egy nyíltabb diszkurzus indult meg a támadó kiberképességekről, kezdve az Egyesült Államok ún. *defence forward*[3] elképzeléséről egészen Magyarország Nemzeti Biztonsági Stratégiájáig [2], amelyben megjelenik a kibertámadásra adott fizikai válaszreakció lehetősége is. E folyamat eredményeként mondhatjuk, hogy a kiberhadviselés képességei fejlődnek, megjelennek a kibertér katonai műveleti területein, a hagyományos hadviselés módszereit és eljárásait sajátosan alkalmazva. Disszertációmban ezt a képességfejlődést vizsgálom meg.

[1] Eredeti: "The future is already here – it's just not evenly distributed." [1]
[2] Voice-over-IP: chatszolgálatókon keresztüli hívások.
[3] Előretolt védelem.

Tudományos probléma megfogalmazása

Az információs társadalom változásai komoly hatással voltak a hadviselésre. Az egyik ilyen hatás maga a kibertér fejlődése, amely egyszerre jelent lehetőséget és fenyegetést. Egyfelől a kibertér adta összekapcsoltság, kíváncsiságunk, szerzési vágyunk azonnali kielégítésének könnyűsége vagy az otthoni munkavégzés elterjedése könnyítést és kényelmet ígér, másfelől azonban számtalan sebezhetőséget és kockázatot hordoz, amelyek ártó szándék mellett lehetőséget adnak károkozásra. A kibertér szereplői sokszínűek, lehetnek személyek és megszemélyesítések, nemzetállamok és szervezetek, támadók és védelmezők. A múltbeli fegyverekkel ellentétben a kiberhadviselés folytatásához szükséges technológia nem korlátozódik a rendszer egyes szereplőire, nincs olyasfajta technológiai monopólium az államok kezében, mint például a vadászrepülőgépek esetében. **A kritikus rendszerek (súlypontok) megtámadásának képessége megtalálható mind az állami, mind a nem állami szereplők kezében. Ennek az új hadviselési módnak a módszerei és eszközrendszere, valamint összetevői, szereplői összességében: az állami szereplők rendelkezésére álló képességek a katonai felhasználást illetően új problémákat, kihívásokat és lehetőségeket hoznak létre, melyek folyamatos elemzést igényelnek a kibertér sajátossága okán.**

A kutatásaim során egyértelművé vált, hogy képességfejlesztés nem egyszerű egy olyan hierarchikus, formaiságot és hagyományokat tisztelő szervezetnél, mint a hadsereg. A szakirodalom egyfelől a szervezeti kultúrából eredezteti ezt a nehézségét, másfelől rengeteg fejlesztési prioritása van egy ekkora szervezetnek, azokat összehangolni, beszerezni, teljesíteni idő- és adminisztráció igényes. **A hagyományos - ún. lépcsőzetes - képességfejlesztés azonban nem elég rugalmas a kiber haderőnem fejlesztéséhez.** A kibertérben végzett műveletek nem-kinetikus műveletek, támogató funkciót ellátva, és nem felelnek meg a hadsereg ethoszának: az ellenséges területen harcoló katona képének. A kulturális különbségeken túl, a kiberképességek területén igaz, hogy ott nem rendelkezik az állam monopóliummal, mint a kinetikus erőknél: ugyanazért a képességekkel rendelkező személyekért versenyez a közszféra, mint a magánszféra. Harmadszor, a kiberképesség-fejlesztéshez más fejlesztési modell szükséges (ún. agile módszertan), mint a hagyományos katonai képességfejlesztés. Egyszerűen gyorsabbá és alkalmazkodóképesebbé kell válnia ahhoz, hogy ellenállóbb legyen.

Hipotézisek

A kibertér megjelenése a hadviselésben – mint önálló ötödik dimenzió – sajátos problémákat és kérdéseket jelenít meg. Azáltal, hogy nem határolhatóak el élesen a kibertér katonai és a civil

részei, másrészt, hogy részben létezik fizikai (hardver) megjelenése, kérdésessé teszik, hogy alkalmazhatóak-e rá a többi dimenzióban ismert koncepciók és eljárások.

A XX. század elején kialakuló légierő támpontot adhat arra vonatkozólag, hogy szervezetileg hogyan integrálódhat egy új dimenzió a hadviselésben, és milyen hatással lehet arra. A megjelenő elméletek lecsapódtak a doktrínákban, melyek hatással voltak a szervezeti ki- és átalakításokra is.

A változáshoz több összetevő szükséges. A kiberképességek tekintetében öt főbb összetevőt azonosítottam: az akadályok megszüntetése, a befektetés/beruházás (finanszírozás), az befogadás/integrálás, a szabályozás és a védelem. Disszertációmban **kiemelten kezelem az akadályok megszüntetését, a kiberműveletek és képességek befogadásának fontosságát.** A kiberhadviselés integrálása a katonai szervezetrendszerekben eltérő képet mutatnak úgy szervezetileg (elhelyezkedés, kapcsolat más szakterületekkel), mint tartalmilag. Miután a kibertér nem-kinetikus, nehezen „látható", elvont terület, kiemelten fontos az ún. helyzetkép fejlesztése. A megértés, az együttműködés elősegítése a „technikai" és „nem-technikai" személyek között nélkülözhetetlen ahhoz, hogy gyakorlaton, misszióban vagy műveleten a döntéshozó meg tudja hozni azokat a jó döntéseket, amelyek a kiberteret (is) érintik.

A vonatkozó szabályozásban és együttműködésben jelenleg még több a kérdés, mint a válasz. A katonai kiberképesség-fejlesztés elismerten fontos terület, azonban csak nemrég került kimondásra az offenzív kiberképességek létrehozásának, fenntartásának fontossága. A kibertér sajátosságaiból fakadóan nagyobb koordinációra van (és lesz) szükség a katonai szervezeten belül, hogy az integráció sikeres legyen.

A hazai kiberképesség-fejlesztés tekintetében elmondható, hogy az előremutató, szervezetileg is megfelel a regionális fejlettségi szintnek. **A hazai fejlesztés során megjelenő problémák jellemzőek általánosságban minden nemzetállami katonai kiberszervezetre, ezek főként a szükséges humánerőforrás biztosításának és megtartásának nehézségei, a képesség fejlesztésének folyamatossága, a kiberelemek integrációja a művelettervezésben.**

A disszertáció témájával kapcsolatosan a kutatásaim a következő hipotézisek mentén haladtak:

H1: A főbb definíciók tisztázása és a releváns doktrínák követik a gondolkodásbéli változásokat, melyek megjelennek a szervezeti struktúrák átalakításában is. Párhuzam vonható a kiber és a légi dimenzió között.

H2: Az akadályok megszüntetése szempontjából eltérő rendszerek alakulnak ki a V4-es tagországok és Németország esetében.

H3: A szabályozás alatt a katonai koncepciók és doktrínák, az interoperabilitás biztosítására vonatkozó szabványok és a felelősségteljes használat elveit kiemelkedően fontosak.

H4: A magyar katonai kiberképességek állapota megfelel a környező országokénak, a szövetségi gyakorlatok és jó-gyakorlatok azonban szükségesek a műveleti területen történő alkalmazás kapcsán.

Kutatási célok

A kutatásom hozzájárul a nem-kinetikus képességfejlesztésről való gondolkodáshoz, illetve bemutatja azokat a főbb pontokat, amelyek továbbfejlesztést igényelnek a katonai szervezetek részéről.

A következő kutatási célokat tűztem ki:

A kiberhadviselés egyértelmű fogalmi meghatározása. Ennek érdekében átfogó irodalomkutatást végeztem, áttekintve a kibertérhez köthető fogalmak alakulását, illetve a légierő képességeinek integrációja történelmét. Kitekintést végeztem a légierő-elméletből fakadó súlypontelmélet felé is, és annak használhatóságáról a kiberműveletek során.

A kiberképességek fejlődését, integrációját akadályozó tényezők feltárása különböző országokban. A kiberképességek és az akadályok mérése esetében a DOTLMPF és PETIO leírást használtam a sajátosságaik jellemzése érdekében, megvizsgálva a képességfejlesztés akadályozó tényezőit. A képességfejlesztés területén feltártam annak lehetőségét, hogy az ún. agilis módszertannal egészüljön ki.

A légihadviselés és a kiberhadviselés kialakulásának összehasonlító vizsgálata. A légierővel való összehasonlítás egyik pontja a helyzetkép, amely a légierőben is kiemelt

szerepet tölt be. A helyzetkép kialakulásának hátterében szintén az IKT fejlődése állt, és jó megoldásnak bizonyult az emberi kezelőszemélyzet információs túlterheltségének csökkentésére, elősegítve a komplex döntéshozást. Hasonló motivációk állnak a kiberhelyzetkép fejlesztése mögött is. Bemutatom a kibertér láthatóvá tételének lehetőségét a kiberhelyzetkép által, valamint megvizsgálom annak komponenseit.

A kiberképességek fejlesztésének hazai állapotának vizsgálata és javaslattétel a hatékony hazai képességfejlesztésre. Célom megvizsgálni a kiberképesség-fejlesztés magyarországi helyzetét kiemelten azt, hogy ez hogyan illeszkedik a korábbi fejezetekben felvázolt fejlődési trendekbe. Ennek érdekében elemeztem a hazai doktrinális környezetet, a szervezeti hátterét és SWOT-analízist[4] végeztem. Kiemelt célom, hogy javaslatot tegyek a további fejlesztési lehetőségekre.

Kutatás lehatárolása

Kutatásom során nem érintettem a következő, önmagukban is külön, önállóan kutatható területeket:

- a műveletтervezés alapvetéseit, elméletét és gyakorlatát;
- az információs műveletek, a hálózatközpontú hadviselés, az információs hadszíntér, az információs fölény, annak kivívásának, elérésének és megtartásának részletes vizsgálatát;
- a kibertér civil entitásaira vonatkozó részletes vizsgálatokat.

A disszertációban megjelenik a kiberműveletek integrálásának nehézsége a katonai műveletтervezésben, azonban ez az integráció jelenleg is folyamatban van. Az Ukrajna ellen zajló háború több fontos tanulsággal is szolgál a kinetikus és nem-kinetikus műveletek összehangolásáról, sikerességéről és kudarcáról. Ennek a tapasztalati feldolgozása a jövőben remélhetőleg több kutatásban is megjelenik majd. Mindezek mellett a kutatásom során csak felvillantani kívántam ezt a nehézséget a kibertér, mint önálló műveleti területként való értelmezésének gyakorlatibb akadályát. Az információs műveletek és a kiberműveletek kapcsolatára ki fogok térni röviden, azonban a témát feldolgozta Haig Zsolt az *Információs műveletek a kibertérben* című alapművében [3]. Végezetül a kibertér civil oldalának

[4] SWOT-analízis: egy adott entitás erősségeinek (strength), gyengeségeinek (weakness), lehetőségeinek (opportunity) és kockázatainak (threat) megbecsülése, feltárása.

ismertetését, bemutatását érintem annak katonai megfelelőjének taglalásakor, amennyiben azt kiegészítette relevanciájával.

Kutatásmódszertan

A kutatási célkitűzéseimmel összhangban olyan kutatásmódszertant kerestem, amely az átfogó, általános ismeret-területtől halad a specifikus kérdésekig, ehhez egyfelől igyekeztem rendszerszemléletű, másfelől szisztematikus lenni. Ezért elindultam a kibertér fogalmától, majd a képességfejlesztésen és a kiberképességeken át eljutottam azok hazai állapotának felméréséig. Ezt az evolúciót tükrözik a kutatási kérdéseim és célkitűzéseim. Az általam kitűzött kutatási célok megvalósításához részt vettem a kiberbiztonsággal és -védelemmel foglalkozó, valamint a kiberműveleti képességekhez kapcsolódó tudományos rendezvényeken, konferenciákon, gyakorlatokon és képzéseken, majd feldolgoztam, elemeztem és értékeltem az ott szerzett tapasztalatokat, ismereteket.

A vonatkozó szakirodalom kutatását, tanulmányozását, feldolgozását végrehajtottam. Összegyűjtöttem és feldolgoztam a kutatásom által érintett részterületekhez kapcsolódó releváns szabályozói hátteret, törvényeket, rendeleteket. Az összegyűjtött szakirodalmat analitikus módszerrel, majd a rendszerezést követően szintetizálással dolgoztam fel. A szakirodalom feldolgozása során az indukció és a dedukció módszerét is alkalmaztam.

Folyamatosan nyomon követtem a kutatási témámmal kapcsolatos aktualitásokat, fejleményeket a mérvadó szakfolyóiratok tanulmányozásával, összegyűjtöttem és rendszereztem a megítélésem szerint a kutatási témámhoz kapcsolódó releváns fogalmakat. Másodelemzést végeztem az Egyesült Államok légierő-fejlődésének történetével, a kiberképességek fejlesztésével kapcsolatosan, így például a NATO CCDCOE által végzett kutatásokból vonok le következtetésetek, majd a fenti vizsgálatok eredményeire, illetve saját szakmai tapasztalatomra alapozva végrehajtom a hazai kiberképességek SWOT-elemzését.

Tudományos munkám során az általános kutatási módszert alkalmaztam, azon belül is a megfigyelést és az összehasonlító módszereket használtam fel az egybevetés során, illetve az akadályok megszüntetésének kutatásánál és a nemzetközi tapasztalatok vizsgálatánál is.

Kutatásom eredményeit folyamatosan publikáltam, a munkavégzésem során alkalmaztam is, illetve több tudományos és szakmai konferencián is részt vettem előadóként és hallgatóként egyaránt.

Értekezés szerkezete és jelölésrendszere

Értekezésem az általam kitűzött célok megvalósításához, a kutatásom és az elért tudományos eredmények bemutatása érdekében az alábbi szerkezet szerint épül fel:

Az 1. fejezetben ismertetem a kibertér főbb jellegzetességeit, a szakirodalomban fellelhető kibertér definíciókat vetem össze, és megfogalmazom, mi tartozhat a kiberhadviselés körébe. A definíciók tisztázása azért is különösen fontos, mivel azon túl, hogy erősen technikai szókészlettel dolgozik a szakirodalom, a kibertér nehezen megfogható jellege miatt eltérések vannak azok tartalmában. A 2. fejezetben a DOTLMPF (angol rövidítése a következőknek: *doctrine, organization, training, materiel, leadership, personnel and facilities*, azaz doktrína, szervezet, képzés, felszerelés, vezetés, személyzet és létesítmények) és a PETIO (angol rövidítése a *people, exploits, toolset, infrastructure and organization*, azaz személyzet, kihaszálható sérülékenységek, eszközök, infrastruktúra és szervezet) keretrendszeren keresztül mutatom be a képességfejlesztést akadályozó tényezőket, majd bemutatom a IT-területen használt „agile" módszer adta lehetőségeket. Ezután a harmadik fejezetben összehasonlítom a kibertér dimenziójának fejlődését a légierő kialakulásával, például Douhet, Trenchard, Warden elméleteivel és olyan fogalmak mentén, mint a célrendszerek meghatározása, a különbségtétel harcoló és nem-harcoló entitások között, a támadás gyorsaságának és a morál támadásának fontossága. Ezek után bemutatom a helyzetképet, mint integrációt és befogadást elősegítő lehetőséget. Végezetül megvizsgálom – az akadályozó tényezőket figyelembe véve – a hazai kiberképesség-fejlesztés lehetőségeit.

Minden fejezet elején ismertetem a hipotézisemet, a kutatási céljaimat, a kutatásmódszertant és a kapcsolódó szakirodalmi áttekintést. Ezt követően mutatom be a részkutatást és összegzem az elért eredményeket, vonom le a részkövetkeztetéseket és mutatom be az elért új tudományos eredményeket.

Az értekezésben a lábjegyzetben tisztázó kiegészítéseket jelölök, a felhasznált irodalmat a törzsszövegben sorszámozott hivatkozással látom el, amelyet az irodalomjegyzékben részletesen kibontok. A *dőlt szövegrészek* idegen szakkifejezést, az idézőjelbe tett szövegrészek pedig szó szerinti idézést jelölnek.

Köszönetnyilvánítás

Szeretnék köszönetet mondani a témavezetőmnek, prof. dr. Kovács Lászlónak, aki az évek alatt irányította szakmai kutatásaimat, tanácsaival mederben tudta tartani szerteágazó érdeklődésemet. Köszönöm dr. Haig Zsoltnak, területi témavezetőmnek, hogy kérdéseivel és meglátásaival előrébb mozdította az elakadt gondolat-folyamjaimat. Köszönettel tartozom az egyetemi tanáraimnak, kutatótársaimnak, akiket egyenként nem tudok most itt felsorolni – vezetésük, társaságuk, barátságuk nélkülözhetetlen volt. Végezetül köszönöm a KMDI Titkárságának a segítségüket és nehéz időkben a vigasztalásukat.

Köszönettel tartozom jelenlegi és korábbi munkáltatóimnak, hogy lehetőséget biztosítottak tanulmányaim folytatására, és bátorítottak ez idő alatt.

Hála és köszönet szüleimnek, testvéremnek, páromnak, barátaimnak, hogy elviseltek a tanulmányok, cikkek, könyvfejezeket és végezetül a disszertáció írása folyamán. Nélkülük nem sikerült volna.

1. A kibertérhez és képességfejlesztéshez kapcsolódó definíciók bemutatása

A kibertér más, mint a többi hadműveleti dimenzió: összetettségében, a mindennapi élet átszövésében, mondhatni minden tekintetében kettős felhasználású technológiák terepe [4].
A kibertér polgári és katonai dimenziója közötti határvonalak sosem voltak annyira egyértelműek, mint a többi dimenzió tekintetében: míg a szárazföldi domén esetében léteznek (fizikai) műveleti területek, vezetési pontokkal, ember- és eszközállománnyal, addig a kibertérben ezek a területek elmosódnak, lehatárolásuk, azonosításuk nehezebb.

A kibertér, és az azt övező definíciók ennek okán sokrétűek és változatosak, nem utolsó sorban tartalmuk változik a gondolkodásmód változásával, ahogyan a katonai doktrínák fejlődnek [5]. A taktikák, technikák és eljárások (TTP)[5] gyors fejlődése okán a definíció lehatárolásának elég tágnak kell maradnia ahhoz, hogy a használt definíció lefedje. Mindezek figyelembe vételével úgy gondolom, hogy **meghatározható olyan definíció, amely az értekezésben használható**. A kibertér összefonódása az élet minden területével, a privát szféra által diktált fejlődés és fejlesztés, valamint nem-kinetikus volta olyan egyedi tulajdonságokkal ruházza fel, amely más képességeket igényel a haderőtől a sikeres képességfejlesztéshez, ha el akarják érni a doktrínákban hirdetett ambíciószintet.

A jelen fejezet célja egy definícióhalmaz bemutatásán keresztül egy olyan definíció megalkotása, amely jobban alkalmazható a kiberképességfejlesztés területén. A korábbi definíciók markánsan tükrözték a kibertér és a kiberhadviselés eltérését a többi megragadni a korábbi definíciók lényegi elemeit, elég teret hagyva a változás megtartására is.

A hipotézis igazolására irodalomkutatást végeztem a hazai és nemzetközi szakirodalomban, valamint megfogalmaztam a kiberhadviselés körébe tartozható képességeket.

A fejezet a következő struktúrát követi: először bemutatom az 1.1. alfejezetben a témakörhöz kapcsolódó szakirodalmat és főbb fogalmakat, majd az 1.2. alfejezetben a kibertér jellegzetességeit ismertetem. Az 1.3. alfejezetben az információsműveletek és kiberműveletek kapcsolatára térek ki, míg az 1.4. alfejezetben összegzem a részkövetkeztetéseimet.

[5] Az eredeti angol rövidítésből: tactics, techniques and procedures (TTPs).

1.1. Értekezéshez kapcsolódó definíciók áttekintése[6]

1.1.1. Adat, információ

Az összekapcsolt információs és tudásalapú világunk egyre inkább automatizált, és az „okos" megoldások életünk egyre több területére kiterjednek. Ennek következtében elektronikus módon történik a dokumentáltság – számítógépek rögzítik vásárlásainkat, internetezési szokásainkat, egészségügyi állapotunkat, azaz adatok keletkeznek. Az adat egy nagyon tág fogalom, gyakorlatilag bármilyen jel[7] potenciálisan adatnak tekinthető [6]. Az adat általában valamilyen médiumon keresztül közvetítődik, az információ egyik alap összetevője [7:98]. Összegezve, az információ értelmezhető adat, azaz jelentéssel bír, kontextusba helyezhető és felhasználható [7:101]. Az adatok jellemzését az *összadatforrású elemzés és prediktív modellezés* [8:181] című cikkemben foglaltam össze. A legáltalánosabb az ún. 5V kategorizálás, miszerint „volume" (mennyiség), „variety" (változatosság), „velocity" (sebesség), „veracity" (valódiság) és „viability" (életképesség), amelyhez esetünkben még hozzáadódik a „visualization", azaz a megjelenítés.

Az adatok fontossága a társadalom digitalizációja nyomán felértékelődött. Amennyire az adatokból kinyert tudás kényelmessebbé teszi az életünket, például egyből felkínálva a legutóbb vásárolt bevásárlólistát, annyi biztonsági kockázatot is rejt, hiszen a pontos profilozás nem csak marketing célokra használható.[8] Az egyénekről, csoportokról megszerzett és megszerezhető adatokból olyan információk nyerhetőek, amelyek alkalmassá tehetik a befolyásolásra.

1.1.3. Kibertér

A kibertér egy olyan széles körben elterjed fogalom, amelynek tartalmát illetően nincs konszenzus. Ebben a disszertációban a kibertér és a kiberdomén/kiberdimenzió fogalmakat szinonimaként használom.

A kibertér kifejezés maga a sci-fi-írótól, William Gibsontól származik [6:69]:

[6] Az áttekintés alapja. [6]

[7] Minden tekinthető jelnek, amely a kommunikációt szolgálja, a kézmozdulattól kezdve a tanult jelekig, mint amilyen az írás-olvasás.

[8] A sajtóban leginkább elterjedt botrány az elmúlt évtizedből a Cambridge Analytica nevű vállalathoz köthető, a közösségi médián keresztüli profilozással való befolyásolással hirdette magát.

> „Kibertér. Egy konszenzusos hallucináció, amelyet minden nemzet törvényes felhasználóinak milliárdjai használnak naponta, matematikai fogalmakra tanított gyerekek által... Az adatok grafikus ábrázolása az emberi rendszer minden számítógépének tárából. Elképzelhetetlen komplexitás."[9]

A „kibertér" kifejezés az 1990-es években kezdett az internet, majd később a világháló de facto szinonimájává válni. Ezzel egy időben a kibernetika, mint kifejezés, eltűnt a tudományos és politikai diskurzusból, holott valószínűleg szerepet játszott abban, hogy végül a „kibertér" mint kifejezést terjedt el, nem például a „mátrix" [10:7].

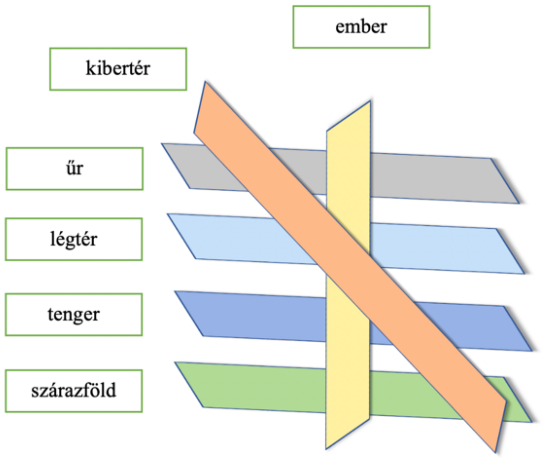
A kibertér különböző értelmezése az elektromágneses tér technikaibb definícióitól – ahol az információáramlás és a kibertér összekapcsolhatósága fejlődik (Cohen) – egészen az elméletibb definíciókig terjed (például Libicki vagy Ventre munkássága). Emellett olyan értelmezésekkel is találkozunk, amelyek a kiberteret a hatalmi viszonyok új tartományának tekintik (Kuehl, Sheldon).

A legtöbb katonai dokumentumban a kibertér-definíciók technikaibb megfogalmazása található meg, és az ezen szövetséges országok által adott értelmezések elemzése a kibertér ötödik stratégiai dimenziójaként való elismerése miatt jelentős, hiszen az legitimálja a kiberteret mint a háború új színterét [11]. Daniel Ventre [12] a kiberteret olyan tartománynak tekinti, amely átszeli a hagyományos doméneket. Ventre meglátása szerint a kibertér a hardverrétegből kiindulva a programok, alkalmazások és információk (szoftverek) virtuális rétegén át az azt kezelők felhasználók kognitív rétegéig terjed (ez az úgynevezett „peopleware"). Az általa megfogalmazott *peopleware* réteg léte *társadalmasítja* a kiberteret azáltal, hogy nem kizárólag elektronikus és/vagy mechanikai szempont alapján írja azt le. Ez teoretikusan amiatt jelentős, hogy ezáltal a kibertér egy társadalmi tér is, és mint olyan, a hatalom egyik tere.

A 1. ábra mutatja be a kibertér átható jellegét amelyet Ventre is leírt. A kibertér minden dimenzióban megtalálható, azonban jellegét tekintve nem elkülöníthető az embertől, a kognitív dimenziótól. Ahogyan a kibertér nem szétválasztható katonai és civil területekre, úgy az emberek tekintetében is összefolynak a határok a magánszféra és a munkahely között. Ez természetesen egy külön és nagy tématerület, azonban az elmúlt években több figyelem irányult

[9] Saját nyersfordítás, eredeti megfogalmazás: "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data"[9:69]

a kiberbiztonság részéről is erre a problematikára, nem utolsó sorban a COVID járvány alatt nagymértékben elterjedt otthoni vagy hibrid munkavégzés kapcsán. Általánosságban nincs ezekre uniform válasz, jó-gyakorlatok léteznek (például több faktoros autentikáció), azonban a "kiber-higénia" fenntartása, azaz a jelszavak megfelelő kezelése, a hálózatok külön tartása, a minősítések betartása, az adatok védelme szervezeti és személyes feladat és kötelesség is egyben.



1. ábra: a kibertér és a többi dimenzió kapcsolata [13]

Martin Libicki [14] is azt a nézetet vallja, hogy a kibertér a különböző rétegek közötti interakció eredménye. Szerinte a fizikai réteg (hardver) jelenti a kibertér alapját, hiszen az elektronikai komponensek jelen vannak minden intelligens és összekapcsolt eszközben. A második, ún. szintaktikai réteg azokból az utasításokból és parancsokból (kódokból) áll, amelyeket a fejlesztők adnak az eszközöknek. Végül jön a szemantikai réteg, amely a gépekben található információkat reprezentálja. Libicki megközelítése a kiberdomént is kevésbé kézzelfogható médiumként ismeri fel a szárazföldhöz, a levegőhöz és a tengerhez képest, mivel immateriális elemek konfigurálják bináris adatok formájában, amelyek a szintaktikai és szemantikai réteget alkotják.

Kuehl [15:28] a kibertér különböző értelmezéseinek tanulmányozása után mesterséges és egyedi tartománynak tekinti, amelynek fő megkülönböztető tényezője, hogy eredetileg a számítógépes hálózatok emberi felhasználása révén jött létre.

Kuehl a következő definíciót javasolja:

> „Globális tartomány az információs környezetben, amelynek jellegzetes és egyedi karakterét az elektronika és az elektromágneses spektrum felhasználása határozza meg az információk létrehozására, tárolására, módosítására, cseréjére és kiaknázására az információs-kommunikációs technológiákat használó, egymástól függő és összekapcsolt hálózatokon keresztül."

Fang [16:24] szerint a *kiber* és a *tér* együttes használata már komplex jelentésű szóösszetétel, és négy alapvető elem együttesét jelöli:

(1) Az információs és kommunikációs infrastruktúrát;
(2) az adatok összességét;
(3) a felhasználók és a szerepkörök összességét;
(4) a műveletek és tevékenységek összességét.

„A kibertér mint működési környezet, meghatározza a paramétereket, hogy milyen tevékenység – legalábbis rövid távon – megvalósítható. Lucas Kello szavaival élve a kibertér a legelemibb fogalom a kiberterületen, mivel meghatározza azokat a technikai jelzőket, amelyeken belül a virtuális fegyver működhet. A kibertér nem rögzített, de ahogy Ron Deibert mondja, folyamatosan fejlődő elemek keveréke, amelyek közül néhány lassan mozgó és állandónak tűnik, míg mások gyorsan mutálódnak. Ezenkívül nem csupán technikai, számtalan fizikai és nem fizikai tulajdonságról van szó; egyben szociológiai rendszer is, egyeztetett protokollokkal, eljárásokkal és intézményi hálózatokkal." [17:41]

Az Észak-atlanti Szerződés Szervezete (NATO) kifejezések és definíciók szójegyzéke szerint a kibertér „A globális tartomány, amely minden összekapcsolt kommunikációs, információs technológiai és egyéb elektronikus rendszerből, hálózatból és adataikat, beleértve azokat is, amelyek elkülönültek vagy függetlenek, amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak." [18]

A hazai kiberbiztonsági stratégiában a következőként van megfogalmazva: „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."

1.1.3. Kiberműveletek

A kibertérben megvalósuló műveletek tekintetében mély és sokrétű a „fogalmi sokszínűség" a nemzetközi irodalomban. A korábbi definíciókat összegezve, egyfajta fogalmi keretként úgy tekinthetünk a kibertérre, mint az internet, a számítástechnikai eszközök, a rajtuk futó szoftverek, sőt az őket használó, mindinkább hálózatokba szerveződő egyének (perszónák) összességére.

A három legalapvetőbb művelettípus – a kibertérben is – az offenzív, a defenzív és az információszerzés (hírszerzés) [19:57][10]. Jellegzetessége, hogy a műveletet indító szervezettől lesz egy kiberművelet katonai, nem az elért hatásától [20:3]. Nem minden kibertérben elért hatás katonai művelet, hiszen a kibertérben több szereplő is jelen van, mint adott nemzetállamok katonai egységei. Egyes kutatók szerint a kibertérműveletek egyik jellegzetessége, hogy az eleinte pusztán technikai jellegtől[11] mára egy, a politikum által hatalmába kerített térré változott, ahol eltérő (nemzeti) érdekek, eltérő normák és eltérő értékek formálják a viszonyokat [22:72]. Az információs műletekről és a kiberműveletekről való gondolkodás általánosságban az Egyesült Államok, az Orosz Föderáció és a Kínai Népköztársaság eltéréseit mutatják be [23], azonban ezeknek a különbségeknek a kibontása nem fog megtörténni a disszertációban. A vizsgált kiberképességek mind a NATO szövetségi rendszerében lévő országokat érinti, és az ahhoz igazodó doktrinális hozzáállást tükrözi.

A NATO CCDCOE[12] által használt taxonómia szerint négy főbb kategóriába sorolhatóak a kibertérben végzett katonai műveletek:

(1) a kommunikációs és információs rendszerek infrastruktúráját érintő műveletek (CISIO: Communication and Information System Infrastructure Operations), melyek célja segíteni az adott ország védelmi minisztériumának tulajdonában és

[10] Kovács kifejti, hogy a hazai terminológia a felderítést használja az információszerzési eljárásokra, mely jelentés azonban magában foglalja – az adatok, információk megszerzésén túl – azok feldolgozását, elemzését, értékelését és az eredmény felhasználókhoz való eljutattását.
[11] Az amerikai terminológia kezdteben CNO-t, computer network operationst használt (számítógép-hálózati műveletek), majd „lecserélte" kibertérműveletekre.[21]
[12] NATO CCDCOE: NATO kibervédelmi együttműködési kiválósági központ (NATO Cooperative Cyber Defense Centre of Excellence)

kezelésében lévő hálózatok tervezését, kiépítését, konfigurálását, karbantartását, üzemeltetését és fenntartását.

(2) a hírszerzési, megfigyelési és felderítési műveletek (CISRO: Cyberspace Intelligence, Surveillance and Reconnaissance Operations) információgyűjtést biztosítanak, valamint operatív előkészítést végeznek.

(3) a védekező kiberműveletek (DCO: Defensive Cyber Operations) megőrzik és/vagy visszaállítják a kibertérben történő cselekvés szabadságát és a saját erők (adatok, hálózatok, hálózathoz köthető képességek) védelmét.

(4) az offenzív kiberműveletek (OCO: Offensive Cyber Operations) olyan aktív műveleteket jelentenek, amelyek elősegítik bizonyos katonai célok elérését a kibertérben vagy azon keresztül végrehajtott hatásokkal [24:16].

Az alábbi, 2.sz. ábra kifejti e műveletek funkcióit és feladatait. A széles portfolió miatt a legtöbb esetben nem egyetlen szervezet felel minden művelettípusért, hanem kettő, három szervezet is. Sok esetben a katonai felderítésért felelős szervezet és egy, kifejezetten kiberműveletekért felelős szervezet között oszlanak meg ezek a feladatok. Emellett az elektronikai hadviselésnek is fontos szerepe van ezeken a területeken. Amennyiben a civil szférából ismert védekező, ún. "blue team", és támadó, "red team" hasonlatot használnák, úgy a CISIO és DCO lehetne a "blue team" megfelelője, míg a CISRO és OCO a "red team"-é. Ez az összehasonlítás is egyszerűsítés eredménye, mert sok esetben nem különíthető el ennyire a szerepkör, de mindenképp hasznos analógia a funkciókat illetően a tipológiai besoroláshoz nem-technikai szakemberek számára.

Műveletttípus	Szervezet	Funkció	Feladatok
CIS infrasktruktúrát érintő műveletek (CISIO)	Kiberbiztonsági ellenőrzési (audit) csoport Sérülékenységvizsgálatok vizsgálatáért felelős csoport	Eljárások ellenőrzése Technikai ellenőrzések	Konzultáció és akkreditáció Sérülékenységvizsgálatok és penetrációs vizsgálatok (tesztek)
Kibertér ISR műveletek (CISRO)	ISR Csoport	Adatok kinyerése (Data exfiltration) Rendszerek kompromittálása Célmegfigyelés	Szkennelés, lehallgatás, kémprogramok használata (Backdoor, Spyware, Keylogger programok)
Védekező kibertér műveletek (DCO)	"Contact" Csoport ("Embedded" ("beágyazott" csoport) Gyorsreagálás Csoport	Digitális bizonyítékok (digital forensics) gyűjtése Válaszadás a kiberincidensekre	Hálózatok monitorozása Digitális bizonyítékok gyűjtése Malware analízis
Támadó kibertér műveletek (OCO)	OCO Csoport	Adatok manipulálása Rendszerek kompromittálása A cél semlegesítése	(D)DOS támadások Adat és kód injektálása Shell szintű hozzáférés elérése

2. ábra: A kiberműveletek osztályozása [24]

1.1.4. Kiberhadviselés

Nem is olyan régen a kiberháború csak amolyan ijesztő feltételezéseket jelentett: Mi lenne, ha államilag támogatott hackerek olyan széles körű támadásokat indítanának, amelyek egész városokat borítanának sötétségbe? Ha megbénítanák a bankrendszert? Esetleg megszakadnának az ellátási láncok? [25] Ma ezek a forgatókönyvek már nem elméleti spekulációk, hanem valós kockázatok.

A kiberháború kifejezés egy populáris, hatásvadász kifejezés, amelyet eleinte az irodalomban, illetve a politikában használtak. A sci-fi-irodalomban úgy jelent meg, mint a jövő háborúja robotokkal, autonóm repülő járművekkel és autonóm fegyverrendszerekkel. A robotikus kiberháború terminátorszerű ötlete azonban az 1990-es években átadta helyét egy olyan elképzelésnek, amely inkább a számítógépekre és az internetre összpontosított. A RAND [26][13] 1993-ban adott ki egy „Jön a kiberháború!" című cikket, amelyben leírták, hogy a katonai hackereket hamarosan nemcsak felderítésre fogják használni, hanem az ellenség számítógépeinek megtámadására és rendszereinek (akár kritikus infrastruktúrájának) megzavarására is. Egy újabb évtizedet ugorva egyre inkább elterjedt, hogy a hackelés nem csak a háború perifériájára korlátozódik. Bill Clinton elnök fogalmazta meg 2001-ben, amikor egy beszédében arra figyelmeztetett, hogy „ma a kritikus rendszereink – a hatalmi struktúráktól a légiforgalmi irányításig – számítógépekkel vannak összekötve és működtetve", és hogy valaki ülhet egy ilyen számítógép mögött, és potenciálisan megbéníthat egy vállalatot, egy várost vagy egy kormányt." [27]

2010-ben jelent meg Clarke és Knake könyve [28:6], amelyben a kiberháborút a következőképpen definiálták: „egy nemzetállam intézkedései egy másik nemzet számítógépeibe vagy hálózataiba való behatolás céljából károk vagy zavarok okozása céljából". Clarke Clinton és Bush elnök nemzetbiztonsági tanácsadója volt, míg Knake Obama kiberbiztonsági tanácsadója. Ez a megfogalmazás leegyszerűsítve a kinetikus gondolkodás digitális eszközökre való alkalmazása. Azonban két tétellel nem számoltak: a hibrid hadviselés megjelenése a kibertérben, azaz nem csak nemzetállamok intézhetnek ilyen támadásokat, illetve hogy a hatásokat illetően azok nemcsak a számítógépes hálózatban okozhatnak kárt, hanem valós, fizikai, gazdasági értelemben is. Az első jelentős, kiberhadviselésben megjelenő eset a 2007-es Észtország elleni kibertámadások sorozata volt.

A kiberhadviselés „számítógépekben és az azokat összekötő hálózatokban folytatott háború, amelyet államok vagy proxyk[14] vívnak más államok ellen. A kiberhadviselést általában

[13] Egyesült Államokbeli think tank.
[14] Egy entitás helyében eljáró másik entitás, megbízott.

kormányzati és katonai hálózatok ellen vívják, hogy megzavarják, korlátozzák vagy megakadályozzák használatukat. A kiberhadviselést nem szabad összetéveszteni a kibertér terrorizmusra való felhasználásával, kiberkémkedéssel vagy a kiberbűnözéssel, annak ellenére, hogy mindegyik tevékenységtípusban hasonló taktikákat alkalmaznak." [29]

Cameran Ashraf cikkében [30] összesítette a kiberhadviselés definícióit, és három fő attitűdöt különböztetett meg:

Változók	**Magyarázat**	**Vészmadár**	**Szkeptikus**	**Realista**
Cselekmények	Az ellenséges műveletek természete a kibertérben	Olcsó és elterjedt	Költséges és bonyolult	Mindkettő
Támadók	A kiberháború „törvényes" szereplői	Bárki/bármi; a végső felelősség az államoké	Államok	Bárki/bármi
Hatások	A kiberháború lehetséges hatásai	Nagyfokú rendbontás vagy pusztítás	Kis léptékű, helyi zavarok	Jogi következmények a nemzetközi rendszerre
Fizikai tér	Hol zajlik a kiberháború	A kibertér különálló, de keresztezheti a fizikai teret	A kibertér csak a fizikai tér proxyja	A kibertér és a fizikai tér jogilag és gyakorlatilag megkülönböztethetetlen
Célpontok	A kiberháború célpontjai	Állami, katonai kritikus infrastruktúra vagy információ	Kritikus infrastruktúra, információ, emberek	Katonai célpontok, magánszemélyek, vállalatok, államok

3. ábra: kiberhadviselés definíciók [30]

A „vészmadár" típusú teoretikusok nemzeti határokban gondolkodnak, a kibertér elkülönül a fizikai és a politikai földrajztól, de az ezen a területen fennálló konfliktusok offline súlyos következményekkel járhatnak. A nemzeti terület online és offline is létezik, és az olcsó és széles körben elérhető kibertámadásokkal felvértezett külső támadók fenyegetik. A tét a kritikus infrastruktúra, amely megsemmisülhet, ami a társadalom normális működésének súlyos megzavarásához vezethet [30].

A szkeptikus kutatók (például Rid) megkérdőjelezik azoknak az állításoknak a helytállóságát, amelyek szerint a kiberháború egzisztenciális fenyegetést jelent. A kiberháború egy spektrumon létezik, vagy különálló összetevők összessége – kémkedés, szabotázs vagy felforgatás –, és inkább zavart okoz, semmint pusztítást. Ezek a cselekmények drágák és speciális tudást igényelnek, így csak az államoknak állnak rendelkezésre ehhez erőforrások. A legtöbb kritikus infrastruktúra esetében már érvényben lévő óvintézkedések miatt a kiberháború hatásai korlátozottak és helyiek. A kibertér a fizikai tartomány és a benne előforduló politikai cselekvések kiterjesztése. A különálló (kiber)háborús tartomány létezése a kiberbiztonsági cégek, a katonai és a politikai elit lobbitevékenységét tükrözi [30].

A realisták (mint a Tallinn kézikönyv szerzői) a kiberháborúnak a nemzetközi jogra és gyakorlatra tett hatásaival foglalkoznak. A cselekvések által létrehozott precedensek előre nem látható következményekkel járhatnak a nemzetközi stabilitásra nézve, és alapos elemzést kell végezni a megfelelő megértéshez. A realizmus nem a cselekvések költségével vagy összetettségével foglalkozik, hanem a kiberháború „ki, mit és hol" kérdésével. Itt az államok azért fontosak, mert ők alkotják és védik a nemzetközi rendszert, és tetteik hatással vannak a jogi precedensekre és normákra [30].

1.1.4. A kibertérről való gondolkodás fontosságának bemutatása.

A mai katonai kiberműveleti erőfeszítések elsősorban a védelmi műveletekre és a műveleti támogatásra összpontosulnak, nem pedig a támadóképességek fejlesztésére. Az egyik fontos kérdés az attribúció, azaz az egyes kibertámadások elkövetőjének kiléte. A kibertérben elkövetett támadások más-más megvilágításba kerülnek aszerint, hogy azokat állami szervezet, illetve nem-állami szereplő hajtja végre. Az elkövetőknek megfelelően fontos a közös vonások, meghatározottságok tisztázása, s azoknak megfelelő, összehangolt szabályokat és irányelveket alkotni. Ezek után lehetséges a válasz taktika, a technikák és az eljárások egységesítése, tisztázva a szerepeket és a felelősséget a szereplők között. Miután egy-egy támadás, sérülékenység kihasználása gyorsan végbe mehet, vagy gyors reagálást igényel, a kártétel megakadályozása vagy enyhítésének sikere az időveszteség minimálisra csökkentésétől függ. A sikeres védekezés/támadás miatt fontos a döntési, felelősségi körök világos, előre mutató meghatározása. Mivel a kiberműveletek folyamatosan fejlődnek és egyre újabb területekre terjed(het)nek ki, úgy a kihívások és fenyegetések is változnak, és ez a folyamatosan változó bizonytalan tér hozzájárul a korábban említett „háború ködéhez".

Az, hogy a szereplők hogyan gondolkodnak a (kiber)háborúról, azt is meghatározza, hogy hogyan reagálnak rá. Amennyiben elsősorban támogató haderőnemként tekintünk a kiberművetelekre, úgy a defenzív oldala lesz fejlettebb. A katonai kiberműveletek számára kihívást jelent az, hogy a kibertér egy megosztott dimenzió, és szoros együttműködés szükséges a polgári hatóságokkal és a privát szférával is. Ez azonban szintén elmossa a határokat aközött, hogy mi számít támadásnak, mi nem, ki a támadó és ki asszisztált ehhez, akár önkéntelenül? Egy nem-béke állapot alakulhat ki, amely a (nyílt) konfliktus küszöbe alatt zajlik.

Az elrettentés egy másik lehetőséget kínál, amely továbbra sem offenzív, de az adott állam rendelkezik a megtorlás képességével és hajlandóságával. Az elmúlt években ilyen

stratégiai reorientációt hajtott végre többek között az Egyesült Államok, amikor a kitartó elkötelezettség és előre védekezés (Persistent Engagement & Defend Forward) elveit helyezte a kiberstratégiája középpontjába. Az elrettentés azt is jelenti, hogy egy államnak támadó képességgel kell rendelkeznie, amellyel kárt okozhat egy támadás esetén. Figyelembe véve az attribúciós problémát, az elrettentés-képesség jelenleg korlátozott [31:112].

Az Encyclopedia of cyber warfare c. könyvben a kibervédelmet [32:47] a kiber ellenálló képesség szükséges, de nem elegendő részeként definiálták. Elsősorban az Egyesült Államok szemszögéből a fenyegetések elleni fellépést öt lépésre bontották le:

1) a támadások megelőzése;
2) az infrastrukúra megóvása a támadásoktól, amikor azok bekövetkeznek;
3) tompítani a támadások hatását;
4) válaszolni a támadásokra;
5) helyreállítani a megtámadott infrastruktúrát.

Általánosságban az adott állam felelős a kiberbiztonsági jogszabályok, szakpolitikák, szervezetek fejlesztéséért és fenntartásáért. Emellett szükséges összehangolnia szakstratégiákat az oktatási és képzési rendszerrel az elegendő és megfelelő szakemberképzés érdekében. A 2. fejezetben részletesen bemutatott módszertan alapján elmondható, hogy a kibertámadást komoly fenyegetésként kezelik a tagállamok, a szakdoktrínákban is egyre inkább megjelennek az offenzív képességek (utalva a korábban említett elrettentésre is).

1.1.5. Képességfejlesztés

A képesség a NATO meghatározása szerint olyan „kritikus tulajdonság, amely ahhoz szükséges, hogy a NATO védelmi tervezési folyamata által kifejlesztett katonai tevékenység sikeres legyen. […] A képességek leírják, hogy a NATO katonai szervezeteinek mit kell tudniuk teljesíteni, hogy lefedjék a Szövetség katonai küldetéseinek teljes skáláját, és garantálják a NATO katonai hatékonyságát és szabad mozgását.” [33:57]

Kibontva „az a képesség, hogy hatást érjünk el olyan szempontok integrált halmazának alkalmazásával, amelyek a következő kategóriába sorolhatók: doktrína, szervezet, képzés, a szükséges anyagi erőforrások, vezetésfejlesztés, személyzet, létesítmények és interoperabilitás” [34]. A kiberképességfejlesztés e követelmények megjelenése a kibertér dimenziójában.

Mindamellett, hogy a NATO mindig is védte információs és kommunikációs rendszereit, a 2002. évi prágai csúcstalálkozón került először napirendre a kibervédelem ügye, miszerint a Szövetségnek *meg kell erősítenie a kibertámadások elleni védekezési képességeit [35].* A 2014. szeptemberi walesi csúcstalálkozón jóváhagyták az új kibervédelmi szakpolitika irányvonalait és az ahhoz kapcsolódó cselekvési tervet. Ezek mellett a kibervédelmet a NATO alapvető kollektív védelmi feladatának részeként ismerték el, és arra a nemzetközi jog alkalmazandó [36]. A varsói csúcson (2016) a kiberteret műveleti területként ismerték el, kiemelve a szövetség védelmi jellegét, hangsúlyozva, hogy a kibertérben ugyanolyan hatékonyan kell tudnia megvédenie magát a Szövetségnek, mint a többi műveleti térben. Ezen a csúcstalálkozón került elfogadásra az úgynevezett Kibervédelmi Vállalások csomag is, amelyben a tagállamok kötelezték magukat arra, hogy nemzeti kibervédelmüket, beleértve a hálózatokat, infrastruktúrákat, erőforrásokat, együttműködéseiket, oktatást és képzést, erőteljesen fejlesztik [37].

2017-ben a szövetséges védelmi miniszterek jóváhagytak egy frissített kibervédelmi cselekvési tervet a kibertér mint műveleti területté való fejlesztéséről [38]. 2018-ban, a brüsszeli csúcstalálkozón döntöttek arról, hogy az európai műveleti parancsnokságon belül (NATO SHAPE) létrehozzák a kiberműveleti központot (Cyber Operational Center, CyOC), amelynek feladata a NATO kiberműveleteinek koordinálása [38]. Jens Stoltenberg NATO-főtitkár egy 2019-es cikkben pontosította, hogy „egy súlyos kibertámadás aktiválhatja az 5. cikkelyt a kollektív védelemről (amely értelmezés szerint egy szövetséges tagállam elleni támadást a teljes szövetség elleni támadásként értelmez) – ez egyben ellenlépéseket is feltételez [39].

A támadó jellegű kiberképességek deklarált megléte és azok esetleges felhasználása ellentmondásos megítélésű. A NATO és szövetségesei elismerik a nemzetközi jog érvényességét a kibertérre, alkalmazása mégis felvet egyedi problémákat. Ilyen például a kibertámadások attribúciója, azaz annak bizonyítása, hogy „ki az elkövető”, és hogy „ki a megrendelő”. A technikai kérdéseken túlmenően a megtévesztés is jelen van például az ún. „false flag” taktikában [40], és szerepet játszhatnak diplomáciai érzékenységek is.

1.2. A katonai kibertér főbb jellegzetességei

1.2.1. A kibertér mint önálló domén a hadviselésben

Általánosan elfogadott – és a NATO által deklarált[15] – tény, hogy a kibertér számít az ötödik műveleti doménnek, hadszíntérnek, amely egyenlő a szárazföldi, légi, tengeri és űr dimezióval. A Merriam–-Webster szótár a tartományt, a domént a tudás, befolyás vagy tevékenység szférájaként határozza meg [41]. Azonban míg a többi négy domén fizikailag körül határolható, a kibertér határtalan. Doktrinálisan elfogadottá vált a kibertér ezen besorolása, azonban a korábban leírt megkülönböztető jegyeke, és a fejlődő doktrinális gondolkodást (multi-domén műveletek[16]) figyelembe véve figyelemre méltó Michael P. Kreuzernek [42] az az elgondolása, hogy a kibertérre ne különálló hadszíntérként gondoljunk, hanem a többi négy domént átszövő, önálló, ám nem különálló képességként (4. ábra).

Azzal érvelve, hogy a kiber nem egy domén, nem kicsinyíteni akarja azt a szerző, vagy azt sugallani, hogy kevésbé fontos, mint a szárazföld, a tenger, a levegő vagy az űr, hanem azt, hogy bizonyos tekintetben sokkal fontosabb. A szerző által javasolt tipológiában a működési környezet két fő területre oszlik: a hadviselés rétegeire és a hadviselés területeire. A hadviselés rétegei a működési környezet olyan közegei, amelyeken keresztül a hadműveletek végrehajthatók, és a hadviselés minden területére kiterjedő műveleti hatások érhetők el. A hadviselés területe a működési környezet olyan szférája, amely olyan fizikai jellemzőkkel rendelkezik, amelyek egyedi doktrínákat, szervezeteket és felszerelést igényelnek a katonai erők számára. A fizikai tartományok rögzített jellege az egységesített szolgáltatások alapjául szolgál, míg a tartományok és rétegek kölcsönhatása a fejlődő technológiával szervezetileg rugalmasabb, több tartományra kiterjedő működési konstrukciókat alakítana ki [42].

[15] 2016. július 8-án, a wales-i csúcson ismerte el a NATO a kiberteret, mint önálló műveleti domént. [36]
[16] A „2018-tól érvényben lévő többdimenziós műveletek koncepciót az amerikai Kiképzési és Doktrinális Parancsnokság (US Army Training and Doctrinal Command – TRADOC) dolgozta ki, mely szerint a jövő hadszínterén többféle művelet folyik majd egyszerre, a hagyományosnak vett (légi, szárazföldi, tengeri) műveletek mellett az űrhadviselés, illetve az információs és kiberműveletek is megjelennek. Az MDO elméletet dimenziókon átívelő, integrált és együttműködő rendszerek jellemzik”.[16]

Háborús domének		
Háború rétegei	Domének átívelő régiók	Multi-domén műveletek
fizikai	szárazföld	különleges műveletek
elektromágneses	tengeri	kiberműveletek
információs	légi	hírszerzés-felderítés
kognitív	űr	globális logisztikai műveletek

4. ábra: Egy alternatív elmélet a kiberdomén helyéről [42].

A hadviselés rétegei részei annak a természetes környezetnek, amelyben a katonai műveletek zajlanak, mind fizikai, mind társadalmi környezetben. Az információs és kognitív rétegek a közös működési környezet humán és technológiai oldalára fókuszálnak, az előbbi adat- és kommunikációközpontú, az utóbbi pedig a kultúrára, pszichológiára, szociológiára és más kontextuális tényezőkre fókuszál, amelyek meghatározzák az államok és szervezetek működését. Az elektromágneses réteg szintén a csatatér fizikai, bár láthatatlan és nem newtoni része.

A négy tartomány továbbra is a korábban meghatározott négy fizikai tartomány marad, három doméneket átívelő részleggel együtt, amelyek eltérő megoldásokat eredményeztek a kihívások okozta kockázatok enyhítésére. Ebben a tipológiában a kibertér egy multi-domén konstrukció, amely jobban hasonlít a különleges műveletekhez vagy hírszerzési műveletekhez, mint az űrdoménhez. Ezekben közös, hogy funkció- és képességközpontúak, gyakran a modern hadviselés szempontjából kritikus kérdésekkel foglalkoznak, de nem mindig a hagyományos katonai környezetben. Ezek a multi-domén műveleti képességek (kiber, hírszerzés, különleges művelet) a hadviselés minden rétegében és területén működnek, a fő különbségek az elsődleges hangsúlyból adódnak: nem a terület ellenőrzésére vagy megszerzésére összpontosítanak, hanem a kiváltott műveleti hatásokra, gyakran bizonytalan vagy komplex környezetekben.

A gondolkodás azonban a doktrinális háttérrel együtt a külön domén felé haladt. Hasonlósága – ahogyan a disszertációmban kifejtem – a légierőhöz kapcsolódik, az alábbi két, inkább filozófiai kontextusban: a 'mindenhollevőség' és a „digitális határvonal” [43]:

- Mindenhollevőség: a kiberdomén osztozik a „mindenhol jelenlévő” jellemzőjén a légi dimenzióval. Maga a légi tartomány, akárcsak a kiberdomén, egy nyitott és viszonylag korlátlan környezet, ahol műveletek sokasága mehet végbe.
- A digitális határvonal: a levegőtől eltérően a kiberdomén csak adott pontokon érintkezik a többi doménnel. Ily módon a kibertartomány hasonló a tengerhez: egy hadihajó nem célozhatja meg a szárazföld középpontját anélkül, hogy rakétákkal át ne lépne a „légi” tartományba. Hasonlóképpen, a kibertámadások csak olyan objektumokat célozhatnak meg, amelyek vagy a kibertéren belül vannak, vagy a kibertér határvonalán, ahol a kiber találkozik a fizikai világgal.

A katonai kibertérre, kiberműveletekre – amúgy a kiber különböző aspektusainak megvizsgálására sem, úgy általában – nincsenek végleges, a közösség által elfogadott definíciók. A kiberműveletek súlyának, fontosságának növekedésével elengedhetetlenné válik, hogy a fogalmak minden szereplő számára félreérthetetlenül ugyanazzal a tartalommal bírjanak.

1.2.2. A kibertér jellegzetességei

A kibertér kötődik a fizikai világhoz, és a két „világban” történt eseményeknek kihatásaik lehetnek egymásra nézve. Abban a legtöbb teoretikus egyetért, hogy a két világ között létezik egy határ, amelyet négy rétegként határoznak meg. Ezek a rétegek a (1) kiberperszóna (kiberszemélyiség), a (2) logikai réteg, a (3) fizikai réteg és a (4) földrajzi réteg. A kiberszemélyiség a kibervilágban nemcsak fizikai személy lehet, hanem bármilyen identitás – egy csoport, egy „okos” eszköz is akár. A logikai réteg alatt minden szoftvert, operációs rendszert, applikációt értünk. A fizikai réteget jelenti a hardver, a router, az áramszolgáltatás. A földrajzi réteg ebben az értelmezésben azt a lokációt jelenti, ahol a kibertérben végzett műveletek fizikailag megjelennek [44:7]. A NATO értelmezésében [45] a fizikai és a földrajzi réteg egynek tekintendő.

	Definíciók	Forrás
1.	Egy mesterségesen létrehozott tartomány (domén), amely dinamikusan változik, amelyen keresztül és által az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek	[46:15]

2.	Egy konszenzusos hallucináció, amelyet minden nemzet törvényes felhasználóinak milliói, milliárdjai használnak naponta, matematikai fogalmakra tanított gyerekek által. Az adatok grafikus ábrázolása az emberi rendszer minden számítógépének tárából. Elképzelhetetlen komplexitás.	[9:69]
3.	A „kibertér” értelmezhető, mint egy kialakulóban lévő, hálózatba kapcsolt térhez kapcsolódva és azon belüli rész összegzéseként, amelyet valódi, megtestesült felhasználók laknak, és amelyet a tapasztalatok révén fogunk fel. Konkrétan, mind a hálózatos tér, mind a hálózatos/testesült tér folyamatosan formálódik a köztük lévő dinamika és kölcsönhatások által. Nem azt kell eldöntenünk, hogy milyen (külön) tér a kibertér, hanem inkább azt kell megvizsgálnunk, hogyan változtatja meg a kibertér a tapasztalt teret.	[47:255]
4.	A kibertér egy virtuális médium, sokkal kevésbé kézzelfogható, mint a föld, a víz, a levegő vagy akár az űr és a rádiófrekvencia spektrum. Külön rétegei vannak (fizikai, szintaktikai és szemantikai), amelyek mindegyikének meghódítása merőben eltérő jelentéssel bír.	[14:8]
5.	A kibertér meghaladja a többi domént. A többi fizikai térben több hozzáférési pont is van a kibertérhez, és hasonló módon a kibertéren keresztül a többi tartományra is ki lehet hatni. Ily módon a virtuális környezetben végzett műveletek következményeket generálhatnak a fizikai környezetben. Az erőnek a virtuális közegből a fizikaiba való diffúziójának ezt a lehetőségét transzverzalitásnak nevezzük.	[12]
6.	A kibertér az információs környezet egy globális tartománya, amelynek jellegzetes és egyedi jellegét az elektronika és az elektromágneses spektrum használata határozza meg, amelynek célja az információ létrehozása, tárolása, módosítása, cseréje és kiaknázása információs-kommunikációs technológiákat használó, egymástól függő és összekapcsolt hálózatokon keresztül.	[15]
7.	A kibertér elektromágneses rendszerekre (EMS) támaszkodik, ember alkotta objektumokat igényel, folyamatosan reprodukálható, a kibertérbe való belépés költsége viszonylag olcsó, a támadás dominánsabb, mint a védekezés, négy	[48:96–98]

	rétegből áll (infrastruktúra, fizikai, szintaktikai, szemantikai), és az egyik irányítása nem jelenti a többi feletti irányítást.	
8.	„Fizikai tartomány, amely olyan információs rendszerek és hálózatok létrehozásából származik, amelyek lehetővé teszik az elektronikus interakciók létrejöttét. ... A kibertér egy ember alkotta környezet különféle formátumú információk létrehozására, továbbítására és felhasználására. ... A kibertér elektronikus hajtású hardverekből, hálózatokból, operációs rendszerekből és átviteli szabványokból áll.”	[49:17]
9.	Három perspektíva meghatározása: nyilvános, normatív (akadémiai) és nemzetközi. Publikus: a kibertér ember alkotta elektromágneses tér terminálokkal, számítógépekkel, hálózati berendezésekkel, mint hordozóval, amelyen az emberek létrehoznak, tárolnak, változtatnak, továbbítanak használati és megjelenítési adatokat, és egyéb dolgokat végeznek dátummal meghatározott tevékenységek elvégzése érdekében. Ebben a térben az emberek, a gépek és a tárgyak szervesen összekapcsolódhatnak egymással, hogy kölcsönhatásba léphessenek, és különféle információkat állíthassanak elő, amelyek befolyásolják az emberek életét. Akadémikus: a kibertér egy ember alkotta tér, ahol az emberek „általános jelek” alapján „műveleteket” hajthatnak végre, az „IKT rendszerre” támaszkodva a „kiberszerep” révén. A „kiberszerep” arra a szubjektumra vonatkozik, aki generálja és továbbítja az általánosított jeleket, tükrözve az emberi akaratot. Az IKT-rendszer magában foglalja az internetet, a különféle távközlési hálózatokat és kommunikációs rendszereket, rádió- és televízióhálózatokat, különféle számítástechnikai rendszereket, optikai, elektromágneses vagy digitális információfeldolgozó eszközöket a különféle kulcsfontosságú ipari létesítmények között. (...) Nemzetközi: a kibertér egy IKT infrastruktúrára épülő mesterséges tér, amely segíti az embereket a különböző IKT-val kapcsolatos információs tevékenységek elvégzésében az oldalon. Az IKT-infrastruktúra magában	[16:49–51]

	foglalja az internetet, a különféle távközlési hálózatokat és kommunikációs rendszereket, a különféle rádió- és televízióhálózatokat, számítógépes rendszereket, beágyazott processzorokat és vezérlőket a különböző kulcsfontosságú ipari létesítmények között. Az információs tevékenységek közé tartozik az információ létrehozása, tárolása, megváltoztatása, továbbítása, felhasználása, megjelenítése és egyéb információra irányuló műveletek.	
10	A kibertér maga az általános távközlési hálózaton keresztül elérhető objektumok közötti kapcsolatokra és kapcsolatok halmazára utal, valamint magukra az objektumok halmazára, ahol olyan interfészeket mutatnak be, amelyek lehetővé teszik távvezérlésüket, távoli hozzáférésüket az adatokhoz vagy az azokon belüli vezérlési műveletekben való részvételüket. Kibertér: a kibertér a tárgyi és immateriális javak időfüggő halmaza, amely elektronikus információkat tárol és/vagy továbbít.	[50]
11	A globális tartomány, amely minden összekapcsolt kommunikációs, információtechnológiai és egyéb elektronikus rendszerből, hálózatból és azok adataiból áll, beleértve azokat is, amelyek elkülönültek vagy függetlenek, és amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak.	[45]
12	„Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatók, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.”	[51]
13	Kibertér: felhasználók, eszközök, szoftverek, folyamatok, tárolt vagy átvitel alatt lévő információk, szolgáltatások és rendszerek gyűjtőfogalma, amelyek közvetlenül vagy közvetett módon számítógép-hálózathoz vannak kapcsolva.	[52:18]

5. ábra: A kibertér definícióinak összesítése. (saját szerkesztés)

A 5. sz. táblázatban felsorolt, nem teljes körű definícióhalmazból a következő főbb kifejezések megtalálhatóak: mesterséges/elektronikus, dinamikus/változó, összekapcsolt/globális. Az alábbi, CCDCOE által készített táblázat összeveti több entitás kibervédelmi dokumentumaival a kibertér meghatározását, illetve a hivatkozott elemeit (implicit vagy explicit módon). Ezeket többek között az 5. ábrában foglaltam össze alább.

kibertér													
	kézzelfogható			nem megfogható						hálózathoz kapcsolódó			
	fizikai infrastruktúra	IKT / IT	Hardver	információ	adat	kapcsolódás	szoftver	társadalmi/ emberi	virtuális	internet	háló	összekap-csoltság	kommunikáció
ISO		O	O		O	X	X	X	O	X	X	X	O
NIST 1		X	X	O			O	O	O	X	X	O	O
NIST 2	O	X	X				O			X	X	O	O
NIST 3		O	X	O		X	X	X	O	X	X	O	O
EU	O	O	O	O		O	O	O	O		O	O	O
NATO		X	O	O	X	O	O		O		X	X	X
CCDCOE		O	O		O	O	O	O	O		O	O	
Cseh Közt.		X	O	X		O	O		O		X	O	X
Észtország		X	O	O			O		O		X	X	O
Portugália	X	X	X	X			O		O	X	X	O	X
Szlovákia		X	O			X	O	X			X		
Állam 1	O	O	X	O			O			X	X	O	
Állam 2	O	O	O	O		O	O	O	O			O	O
Állam 3		X	O	X			O	O	O		X		O
Állam 4	X	O	O		X	O	X	X	X		X	O	X
Egyesült Királyság	X	X	X	O	X		O	O	X	X	X	O	O
	X definíció explicit tartalmazza						O definíció implicit tartalmazza						

6.ábra: Különböző szervezetek, államok kibertér definícióinak tartalma [5]

A vizsgált doktrínák tartalmát három főbb kategóriába sorolták: a kézzelfogható, fizikai rétegbe tartozik a fizikai infrastruktúra, az információstechnológiai (IT) struktúra és a konkrét hardverek. Míg az IT explicit módon megjelenik a legtöbb doktrínában, addig a fizikai infrastruktúra alig - és inkább implicit módon, míg a hardverek inkább implicit módon, de jelen vannak. A fizikai infrastruktúra és az IT közötti különbség oka lehet értelmezésbeli különbség, miszerint az IT-ba bele érthető annak fizikai infrastruktúrája is. A fizikai réteg megnyilvánulása a doktrínákban azonban azért fontos, mert védelem szempontjából kritikus infrastruktúráknak számítanak.

A második nagyobb kategória a nem megfogható elemeket tartalmazza: adat, információ, kapcsolódás, szoftver, társadalmi - emberi aspektus és virtualitás. Ezek közül legkevesebbszer az adat jelenik meg, holott az adat az információ alapja, és az adatvédelem kiemelt fontosságú. Azonban ez a hiányosság magyarázható azzal, hogy az adatvédelem felett más szervezetek őrködnek. Általánosságban elmondható, hogy a nem megfogható elemek implicit módon jelennek meg a különböző doktrínákban.

A harmadik, egyben utolsó halmaz a hálózathoz kapcsolódást, összekapcsoltságot tartalmazza. Míg az internet és a háló fogalmai expliciten, addig az összekapcsoltság és a kommunikáció impliciten jelenik meg a dokumentumokban - ennek oka elsősorban abban kereshető, hogy alapvetés az internet korában, hogy azt kommunikációra használjuk, és hogy az eszközeink összekapcsoltak.

A nemzeti kiberbiztonsági stratégiák általában kevés információt adnak az államok tényleges kiberbiztonsági felkészültségéről. Ehelyett „elsősorban szándéknyilatkozatként kell

rájuk tekinteni, amely meghatározza és jelzi a kiberbiztonsági politika általános irányát a hazai és a nemzetközi közönség számára egyaránt" [53]. A hadseregek támadó kiberképessége gyakran kimarad vagy homályosan szerepel a stratégiákban, azonban erősödő tendencia, hogy kifejezetten megemlítik a katonai kapacitás fejlesztésének szükségességét a támadóműveletek végrehajtásához.

A katonai célú kiberműveletek iránti növekvő közérdeklődés a kiberparancsnokságok létrehozásában is megnyilvánul, az elmúlt évtizedben legalább negyven [17:9] nemzetállam hozott létre valamilyen formában kiberműveleti egységet a fegyveres erők berkein belül. Ezeket a katonai kiberszervezeteket, amint azt Piret Pernik írja, gyakran „a korábban széttöredezett képességek és szervezetek központosításának, konszolidációjának és észszerűsítésének szükségessége, ugyanakkor az átfedő szerepek és felelősségek kiküszöbölése" alapozza meg, hogy hatékonyan működhessenek ezen az új „műveleti területen" [54].

„A kibertér, mint működési környezet, meghatározza a paramétereket, hogy milyen tevékenység – legalábbis rövid távon – megvalósítható." Lucas Kello szavaival élve a kibertér „a legelemibb fogalom a kiberterületen, mivel meghatározza azokat a technikai jelzőket, amelyeken belül a virtuális fegyver működhet" [17:41].

1.2.3. A kibertér megkülönböztető jelei

A kibertérnek négy megkülönböztető jelét sorolom fel [24]. Az első kettő kapcsolódik a korábban 4. sz. táblázatban felsorolt definíciók összesítéséhez, az utolsó kettő pedig inkább a kiberműveletekhez kötődik.

Az **első megkülönböztető jele** a kibertérnek az, hogy teljes mértékben emberi alkotás. A kibertér egyik alapvetése, hogy az egy mesterségesen felépített és folyamatosan fejlesztés alatt álló, számítógépen alapuló környezetet foglal magában, és amelynek infrastruktúrája nagyrészben összekapcsolt. Attól függetlenül, hogy az internet határtalan érzést kelthet, a földrajzi határok joghatósági felelősségi területei érvényesek, és annak betartása és betartatása az adott nemzet felelőssége. Ahogy később többször látni fogjuk, az a tény, hogy az internet kvázi határtalan, és hogy a civil és katonai oldalának elkülönítése az összefonódások miatt szinte lehetetlen, nem alkalmazhatók rá például egyértelműen a többi dimenzióban (szárazföldi, légi, tengeri és űr) ismert (katonai) műveleti terület adta lehetőségek. A kibertérben rejlő kockázatok és sebezhetőségek magának ennek a térnek a manipulálásával kezelhetők, a fölény elérésén túl a teljes uralom elérése kétséges [16].

A kiberteret három dimenzióval szokás leírni: a fizikai (infrastruktúra), a logikai réteg (kódok) és a kibertérben megjelenő személy (kiberperszóna).

A fizikai réteg fontossága abban rejlik, hogy bármely entitásnak (hardverelem) földrajzi elhelyezkedése van. Ilyen hardverelemek szükségesek az adatok tárolásához, feldolgozásához és továbbításához, ezek képezik az architektúrát. Ide tartoznak katonai szempontból fontos érzékelők, fegyverrendszerek, a vezetési és irányítási rendszerek és az ún. kritikus kiber-infrastruktúrák is. Kritikus kiber-infrastruktúra alatt értjük az olyan integrált információs és kommunikációs technológiai komponenseket (fizikai objektumok, hardverelemek), amelyek kiesése komoly hatással lenne egy adott ország társadalmára, gazdaságára, közbiztonságára, energiabiztonságára, alapvető ellátásbiztonságára. A korábban jelzett, földrajzilag meghatározott joghatóság miatt fontos emlékeztetni, hogy a virtuális valóság nagyon is létező fizikai valóságban gyökerezik és hatása is ott megjelenik.

A logikai réteg tartalmazza a programok és adatok elemeit, olyan mindennaposan használt dolgokra kell gondolni, mint az operációs rendszerek, az alkalmazások vagy a szoftverek. A logikai réteg együtt jár a fizikai réteggel, hiszen az információ vezetékes hálózatokon vagy elektromágneses spektrumon (EMS) keresztül áramlik, kommunikál. Ez a két réteg együtt teszi lehetővé a kibertérben megjelenő személynek, hogy kommunikáljon és cselekedjen.

A kibertérben megjelenő személyi réteg nem valós személyekből és szervezetekből áll, hanem azok virtuális identitásaiból. A virtuális identitás lehet egy e-mail-cím, egy felhasználói azonosító, egy közösségimédia-fiók. Fontos kiemelni, hogy egy embernek lehet több „kiberperszónája” és egy „kiberperszóna” mögött állhat több ember is.

A **második megkülönböztető jele a folyamatos változása,** az állandó mozgás. A támadó és védekező képességek nem örökérvényűek, az előny bármikor elillanhat. A támadó tevékenységek, műveletek állandóak, hiszen költségeik viszonylagosan alacsonyak és hozzáférésük széles. A folyamatos technológiai megújulás azt jelenti, hogy a védekezést is folyamatosan szinten kell tartani fejlesztésekkel, ismeretekkel.

A **harmadik megkülönböztető jel** az, hogy a kibertér műveletei nemcsak a konfliktus kezdetétől fogva vannak jelen, hanem békeidőben is, szemben a hagyományos katonai műveletekkel. Ehhez az is hozzátartozik, hogy a kibertérben ugyanúgy tud tevékenyen részt venni katonai szervezet, mint egy egyén. Erre példa jelenkorunk egyik meghatározó

konfliktusa, az orosz–ukrán konfliktus (2022. február 24. – jelen), amelyben mindkét oldalon megjelentek kiberszereplők [55].

A **negyedik megkülönböztető jele** a viszony a térhez és időhöz. Egy adott országban zajló kibereseménynek a tőle kilométerekre lévő helyeken is okozhat (közvetett) károkat. Az elért hatásokat figyelembe véve ez a kiberműveleteknél – a céltól függően – lehet jelentősen rövidebb vagy hosszabb idő. És ez a (kibertérbeli) hatás lehet azonnali vagy szándékosan késleltetett. Szintén a jelenleg is folyó ukrán–orosz háborúban megfigyelhető, hogy az orosz fél a kinetikus támadás előtt akár hónapokkal elkezdte előkészíteni a műveletet, többek között az ún. Whispergate-tel [49]. 2022. január 15-én a jelentések szerint egy WhisperGate nevű rosszindulatú programot telepítettek ukrán célpontok ellen. A jelentések szerint az incidens három különálló összetevőt tartalmaz: (1) egy rosszindulatú rendszerbetöltőt, amely megrongálja az észlelt helyi lemezeket, (2) egy Discord-alapú letöltőt és (3) egy fájltörlőt. A tevékenység nagyjából egy időben történt több, az ukrán kormányhoz tartozó weboldal megrongálásával [56].

1.2.4. Műveletttervezés a kibertérben

A dolgozatom elején kizártam, hogy mélységében foglalkozzak a műveletttervezéssel – mondjuk integrálásával a COPD keretrendszerbe –, azonban mint olyan „erősokszorosító" elem, amely mindegyik dimenzióban megjelenik, nem kerülhetem meg, hogy említést tegyek róla. „Gyakran számít a kiberműveletek időzítése is, különösen akkor, ha a kiberhatás-műveletek más katonai osztályok műveleteit támogatják. A haderő-integráció szükséges jellege – és így a kiberműveletek időzítésének fontossága – a támadó kiberműveletek és a hagyományos katonai műveletek közötti kölcsönös függés formájától függ." [17:45]

Először is létezhet az, amit „egyesített kölcsönös függésnek" neveznek, amikor a kiberműveletek és a hagyományos katonai műveletek külön funkciókat látnak el. Bár a tevékenységek közvetlenül nem támogatják egymást, mindegyik egyéni hozzájárulást nyújt ugyanahhoz a célhoz. Az ilyen típusú műveletek időzítésének nem kell nagyon pontosnak lennie [17:44–45]. Másodszor, létezhet „szekvenciális kölcsönös függés", amely akkor következik be, amikor egy kiberművelet olyan eredményt produkál, amely a későbbi hagyományos képesség sikeréhez szükséges. Az ilyen típusú műveleteknél sokkal fontosabb, hogy pontosan mikor érjük el a hatást. A kiber erősokszorosító hatása nagyobb lehet a szekvenciális esetében, ugyanakkor a kockázatok is magasabbak. Egy sikertelen kiberművelet

súlyos következményekkel járhat a következő műveletre nézve, ami az egész folyamat kudarcához vezethet" [17:44].

A kibertéri műveletek – ha egyszer beindulnak – gyorsan bontakoznak ki, dinamikusan változó terepen és végtelenül módosítható fegyverrendszereket használnak, amelyek szoros együttműködést követelnek meg a tervező/fejlesztő és a felhasználó között. Ezt a szoros együttműködést teszi lehetővé a disszertációban később bemutatott „agilis" módszertan. Mind a fegyverek, mind a terep menet közben is változhatnak, így szoros döntési ciklusokat igényelnek. A kiberműveletek azonban hosszabb előkészítést követelnek, amely függ a kiválasztott cél összetettségétől, elérhetőségétől. A technikai szakértelem kiemelten fontos, a tisztektől és a legénységtől egyaránt magas szintű műszaki alkalmasságot várnak el. Ezenkívül a sebezhetőségek azonosításának, a kiberfegyverek tervezésének és a műveletek végrehajtásának folyamata a kreatív inspiráció és a módszeres szigor egyedülálló egyensúlyát követeli meg, így a kibertérben dolgozók nagyfokú egyéni autonómiát várnak el munkájuk végzésében [57:186–187].

1.3. Információs műveletek és kiberműveletek kapcsolata

A címben szereplő kapcsolat meghatározása korántsem olyan egyszerű, mint amilyennek elsőre tűnhet. Bár manapság szinte mindenhonnan hallani a "kiberművelet" és "információs művelet" kifejezéseket, mégis, tapasztalataim szerint igen kevesen vannak azok, akik valóban értik és átlátják a kettő közti összefüggéseket és különbségeket. Alapvetően a kapcsolat adja magát, hiszen mindkét terület meghatározó eleme a mai modern hadviselésnek, és - nem utolsó sorban - a biztonságpolitikának is. A két terület között nem ritkák az átfedések, sem az, hogy egymást kiegészítve, támogatva működjenek. De miről is van szó pontosan?

Ahhoz, hogy érdemben elemezhessem a kettő közötti kapcsolatot, fontos ismertetni a két kifejezés pontos definícióját, ehhez pedig szükséges némi magyarázat. Az információs műveletek helyszíne az információs tér, pontosabban a globális információs környezet, amelynek része többek között a katonai információs környezet is. Az információs műveletek létrejöttével a katonai műveletek csoportja is tovább bővült, így most már fizikai, információs és kognitív dimenziókat is számon tart a szakirodalom. Az USA összhaderőnemi információs műveletek doktrínája szerint: „Az információs környezet mindazon egyének, szervezetek és rendszerek összessége, akik, és amelyek az információ gyűjtésével, feldolgozásával, szétosztásával foglalkoznak." (JP 3-13 2014, I-1) [7:149]

A NATO összhaderőnemi információs műveletek doktrínája az alábbiak szerint definiálja: „információs környezet egy olyan környezet, amely magában foglalja magát az információt, az egyéneket, szervezeteket és rendszereket, amelyek gyűjtik, feldolgozzák és továbbítják az információt, valamint a kognitív, a virtuális és a fizikai teret, amelyekben mindez megvalósul”. (AJP-3.10 2015, LEX-7) Fentiek ismeretében érdemes pár szót szólnom az információs műveletek kialakulásáról.

Ma már igen elcsépelt közhely, hogy az információ, a tudás hatalom, ahogyan az is, hogy az információ az egyik legértékesebb dolog a világon. A technológia fejlődésével, a digitalizáció előrehaladtával elképesztő mértékben felgyorsult életünk, s az informatikai és infokommunikációs eszközök hamar mindennapjaink részévé váltak. Bár az információs környezet létrejöttét a ’70-es évekre teszik a szakirodalmak, az ARPANET megjelenésnek idejére, ennyire nem ugrom vissza az időben, pusztán annyit jegyeznék meg, hogy 1976-ban az USA védelmi minisztériumának egy magyar származású kutatója, Thomas P. Rona használta először az információs háború kifejezést[58]. Elmondható tehát, hogy bár a mai 21. századi kontextusban lett felkapott a kifejezés, eredete régebbre nyúlik vissza. A különféle infokommunikációs és egyéb okoseszközök elterjedésével és használatával (IoT) létrejött egy olyan, folyamatosan változó adathalmaz, amely hatalmas léptékben bővül minden egyes percben. Ezek tárolására és nem utolsósorban védelmére komoly összegeket fordítanak az abban érdekelt felek, s ebből, valamint a fentiekből adódóan mind a civil, mind a katonai célú információk biztonságos tárolása és felhasználása kritikus kérdés lett.

Mindannyian tapasztaltuk már, milyen következményekkel járhat, ha nem áll rendelkezésre a megfelelő mennyiségű információ akkor, amikor szükségünk van rá, mint ahogyan azt is tapasztalni minden nap, hogyan jelennek meg álhírek az éppen aktuálisabb témákról. Kialakult egy információs környezet, amely nélkül ma már a civilizált társadalom nem képes létezni. Egy másik meghatározás szerint „az információs művelet egy olyan katonai funkció, ami tanácsot ad és koordinál a katonai információs tevékenységek vonatkozásában annak érdekében, hogy létrehozza a kívánt hatásokat az ellenség, potenciális ellenség és más Észak-atlanti Tanács által jóváhagyott csoportok akaratában, megértésében és képességeiben a Szövetség küldetésének támogatására.” [45]

Ezzel el is érkeztem a kiberműveletek kérdésköréhez. A kibertér már kissé nehezebben meghatározható fogalom ahogyan azt az előző alfejezetekben kifejtettem. Mint ismeretes, kinetikus műveleteknek hívjuk az ellenség elsősorban fizikai energián alapuló fegyverek által történő pusztítását (például lövedék által), míg nem-kinetikusnak azokat a műveleteket,

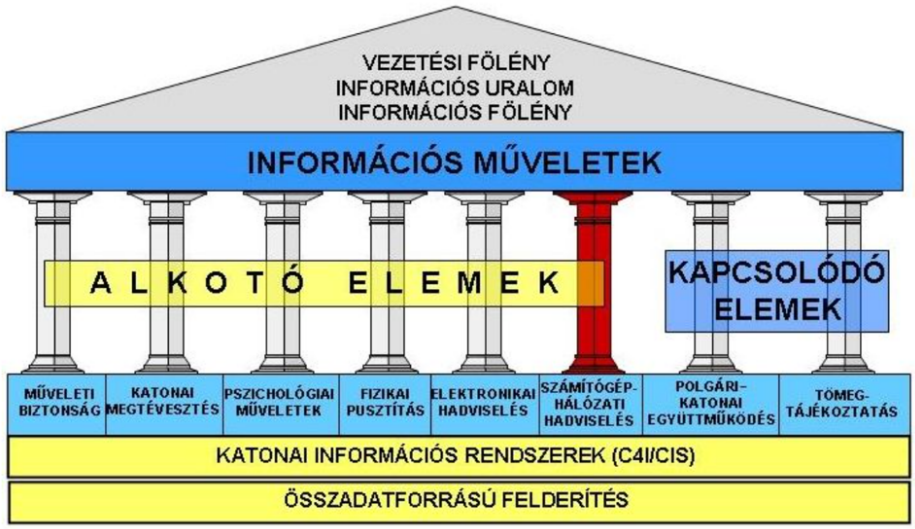
amelyek nem ezen alapulnak (például információs vagy kiberműveletek). A kibertérben, mint műveleti területet érintően, négy művelettípust különböztet meg a szakirodalom:

- A kommunikációs és információs rendszerek infrastruktúráját érintő műveletekért (Communication and Information Systems Infrastructure Operations – CISIO) a CIS-rendszerek támogatásáért felelős szervezet felel. A CISIO-műveletek célja, hogy segítsék az adott ország védelmi minisztériumának tulajdonában lévő és általa üzemeltetett hálózatok tervezését, kiépítését, konfigurálását és biztonságossá tételét, valamint a hálózatok üzemeltetését és fenntartását.
- A kibertérben végzett hírszerzési, megfigyelési és felderítési műveletek (Cyberspace Intelligence, Surveillance and Reconnaissance Operations – CISRO) információgyűjtést biztosítanak, valamint a környezet operatív előkészítését végzik.
- A védekező kiberműveletek (Defensive Cyber Operations – DCO) megőrzik és/vagy visszaállítják a baráti kibertér használásának képességét, valamint az adatok, hálózatok, továbbá a hálózatokhoz köthető képességek és más kijelölt rendszerek védelmét.
- Az offenzív kiberműveletek (Offensive Cyber Operations – OCO) a kibertérben végzett aktív műveleteket jelentenek, amelyek elősegítik bizonyos katonai célok elérését a kibertér képességeinek alkalmazásával.

Az AJP-3.20 doktrína úgy definiálja a DCO-műveleteket, mint védekező tevékenységeket a kibertérben (vagy azon keresztül), annak érdekében, hogy annak végrehajtója megőrizhesse a (baráti – friendly freedom of action) cselekvési szabadságát a kibertérben. [45] Még pontosabban, a DCO magában foglalja a fenyegetések és az ellenséges kibertérműveletek megelőzése, enyhítése vagy azokra való reagálás érdekében tett intézkedéseket a kibertérben vagy azon keresztül, megőrizve ezzel a katonai művelet végrehajthatóságát (mission assurance). Erre a mission assurance-re a harmadik fejezetben visszatérek.

A kibertérben végzett információs műveletek technikai és kognitív összetevőinek felhasználásával egy személy vagy szervezet fölénybe kerülhet ellenfelével szemben, és hatást gyakorolhat más szereplőkre. Az összehangolt információs műveleteknek ez az alkalmazása

nagy előnyt jelenthet a hagyományos konfliktusokban, mivel a sikerhez elengedhetetlen a saját oldalról előnyös hálózati konfiguráció végrehajtása vagy az ellenféléinek mérséklése. Bizonyos forgatókönyvekben a kiberműveletek és az információs műveletek keresztezhetik egymást, ilyen például a kibertámadás során szerzett információk felhasználása a közvélemény befolyásolására vagy politikai döntések irányítására. Létezhetnek olyan kiberműveletek, amelyek nem feltétlenül kapcsolódnak az információs taktikákhoz; ilyenek például az adatok megsértése vagy a vállalati hálózatok elleni támadások. [59]



7. ábra: Információs műveletek típusai. Forrás [7]]

A kibertér megfelelő védelme érdekében számos tevékenységet össze kell hangolni. A védelmi műveletek létfontosságú elemei a kiberbiztonsági rendszernek, de önmagukban nem elegendőek a teljes és átfogó biztonság biztosításához. A hálózatok és rendszerek alapos védelme érdekében további offenzív kiberműveleteket is alkalmazni kell. Hogy a védelem miért különösen fontos, arra remek példa a már fenn említett Big Data, hiszen a Cisco elemzése alapján 2021-ben az IP alapú adatforgalom már elérte a 3.3 zettabyteot, sőt, a DELL EMC becslése alapján ez jóval több, 44 zettabyte]7: 78].

A következőkben a CISIO-n keresztül mutatom be az információs művelet kapcsolatát a kiberműveletekkel.

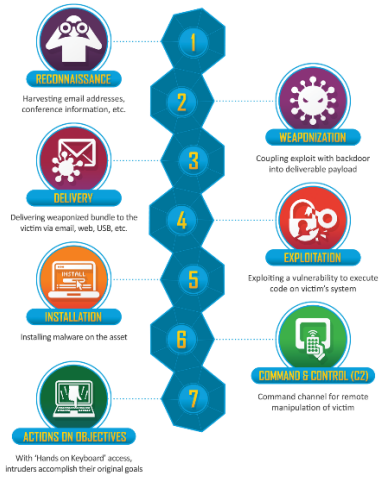
A kommunikációs és információs rendszerek infrastrukturáját érintő műveletek (Communication and Information Systems Infrastructure Operations – CISIO) A

kommunikációs és információs rendszerek infrastruktúráját célzó tevékenységek számos célkitűzést és módszert foglalnak magukban. Ezek a műveletek mélyreható hatással lehetnek a kommunikációra, az adatáramlásra és a digitális szolgáltatásokra. A védekező műveletek célja az információs és kommunikációs infrastruktúra biztosítása, míg a zavaró műveletek célja e rendszerek akadályozása vagy megbénítása. Emellett egyes műveletek a digitális struktúrák feltörését, hatástalanítását, felderítését vagy manipulálását is magukban foglalják. [60]

A hacker műveletek során az elkövetők engedély nélkül törnek be az információs és kommunikációs rendszerekbe, hogy hozzáférjenek az adatokhoz, míg a felderítő műveletek az ilyen rendszerek megfigyelésére és tanulmányozására szolgálnak. A manipulációs műveletek magukban foglalják az információs és kommunikációs rendszerekben tárolt adatok megváltoztatását, hamisítását vagy torzítását. A hagyományos információs fölényt gyakran a klasszikus katonai műveletek szemszögéből vizsgálják, mivel a technológiai és kommunikációs képességek közötti különbség döntő lehet az eredmény szempontjából.

Ez a megközelítés azonban messze nem technológiafüggő, mivel célja az adatgyűjtés, az adatok tárolása, feldolgozása és továbbítása terén való kiválóság elérése. Az információs fölény gyakran a katonai műveletek minden aspektusára vonatkozik. [7] Kialakult az infokommunikációs konvergencia fogalma, amely "az adatok gyűjtését, előállítását, tárolását, feldolgozását, továbbítását biztosító különböző elektronikai, informatikai eszközök és rendszerek közötti legátfogóbb, legmeghatározóbb jelenség ezen területek konvergenciája, amelyet infokommunikációs technológiai konvergenciának nevezünk" [7:80].

Azt azonban fontos leszögezni, hogy minden kiberművelet információszerzéssel kezdődik, amelynek számos módja létezik. A Lockheed féle Cyber Kill Chain, bár bizonyos elemeiben már elavult, szépen példázza, hogyan is épül fel egy-egy komolyabb támadás CISI ellen.



8. ábra: Lockheed Martin Cyber Kill Chain. Forrás [61]

A fenti lánc a leginkább APT (Advanced Persistent Threat) támadások esetén érvényes, főleg közigazgatási és egészségügyi kritikus infrastruktúrák ellen használják, de ez persze korántsem kizárólagos. Az APT támadások remek példái a kiberműveletek és információs műveletek kapcsolatának, hiszen azt komoly felderítő/információszerző hadművelet előzi meg. Az angol terminológiában a fejlett támadásokat APT-nek vagy Advanced Persistent Threat-nek nevezzük, melyből az „Advanced" jelenti, azt, hogy a támadó olyan fejlett technikákat használ, amelyek mások – beleértve a biztonsági megoldásokat szállító vállalatok – számára sem ismertek.

A „Persistent" jelenti azt, hogy a támadó hosszabb ideig fenn kívánja tartani jelenlétét a megtámadott rendszerben és ott hosszabb ideig akarja tevékenységét végezni. A magyar terminológiában az APT, fejlett támadásként terjedt el, ami csak részben felel meg az APT-nek, mivel számos olyan támadás van, amely például nulladik napi sérülékenység kihasználásával követnek el, de egyszeri alkalomra szólnak (például az ukrán energiarendszer elleni támadás).[62]

A fejlett támadások során a támadó olyan eszközöket alkalmaz, (sérülékenységeket úgynevezett 0-napi vagy zero-day exploit) használ ki, amelyek általában egyediek, így a hagyományos védelmi megoldások nem képesek a támadás felismerésére. A komolyabb erőforrással rendelkező bűnözői csoportok, vagy az államok által támogatott támadók hozzájuthatnak olyan sérülékenységi információkhoz, sérülékenységet kihasználó kódokhoz is, amelyek biztosíthatják a támadás sikerességét, illetve, hogy a támadás hosszabb távon rejtve maradjon. A támadók megismerve a célpont védelmi megoldásait, beszerezhetik a célpont által használt védelmi megoldásokat, így lehetőségük van kipróbálni a megoldások kikerülésére alkalmazandó technikák. Az első lépés - amint már említettem - az információszerzés (ez lehet OSINT, vagy zárt forrású keresés, esetleg social engineering útján megszerzett információ, stb.) a lényeg, hogy minden rendelkezésre álló adatot összegyűjt a támadó a célpontról. A nyilvános forrásokból történő felderítést egészíti ki a vállalati hálózat megismerése, a nyilvánosan elérhető szolgáltatások, az azokat kiszolgáló szoftverek és azok gyenge pontjainak feltérképezése. A feltérképezésnek része lehet a reakcióképesség, reakció idő tesztelése, például egy hálózati feltérképezés végrehajtása. [63]

A nemzetközi relevanciája ezeknek a támadássorozatoknak óriási. Amellett, hogy ezek egy részét állami támogatással állami megbízásból is elrendelik, a külsős hacktivista csoportoknak is jut némi szerep. Utóbbira legjobb példa az Anonymous nevű hackercsoport tevékenysége, amely a kibertér eszközeit felhasználva harcol az általa igazságtalannak vélt

rendszerek működése ellen. Ilyen tevékenység többek között az Ukrajna mellett történő kiállásuk is, amely nemzetközi szinten is nagy port kavart. [64]

A növekvő fenyegetésre válaszul a NATO, az EU, és az ENSZ, valamint számos kisebb nemzetközi szervezet is erősen fejleszteni kezdte kibervédelmi képességeit. A sorozatos támadások, valamint a 2007-es észtországi események nem múló hatására megalakultak a különböző tagállamok kiberbiztonsági szakembereiből álló CSIRT-ek, (Cyber Security Incident Respone Team) és az EU - NATO együttműködés területén is jelentős előrelépések történtek.

Az EU globális stratégiájának elfogadását követő végrehajtási folyamatban a két nemzetközi biztonsági szervezet között a kiberbiztonság és kibervédelem területén egyre intenzívebb kapcsolat jött létre. épviselői aláírták az EU hálózatbiztonsági vészhelyzeteket elhárító csoportja (Computer Emergency Response Teams – CERT) és a NATO hálózatbiztonsági incidenskezelő csoportja (NATO's Computer Incident Response Capability – NCIRC) közötti technikai megállapodást. 2017-ben Helsinkiben létrejöhetett a Hibrid Fenyegetések Elleni Kiválósági Központ (European Centre of Excellence for Countering Hybrid Threats), amelynek feladata az elsősorban Oroszország felől érkező kiberbiztonsági kihívások, a dezinformációs műveletek és a stratégiai kommunikáció elemzése, valamint a kihívásokra hatékony és közösen koordinált válaszok kidolgozása.

A kiberműveletek és információs műveletek kapcsolata az APT-k bemutatásán keresztül tehát több szempontból is érdekes:

- Adatgyűjtés és hírszerzés: APT-csoportok fő célja gyakran érzékeny információk vagy titkos adatok megszerzése. Az információs műveletek keretében a támadók megpróbálják befolyásolni, manipulálni vagy zavarni a célpont információs rendszereit és kommunikációját.

- Befolyásolás és dezinformáció: Az APT-csoportok információs műveletek keretében kiberműveleteket hajthatnak végre, hogy befolyásolják a közvéleményt, politikai döntéseket vagy gazdasági folyamatokat. Ilyen tevékenységek közé tartozhat a hamis hírek, dezinformáció vagy manipulatív tartalmak terjesztése.

- Kiberhadviselés: Az APT-csoportok lehetőséget biztosítanak a kiberhadviselésre, ami azt jelenti, hogy a támadók katonai, politikai vagy gazdasági célokat érhetnek el a kiberműveletek és információs műveletek összehangolásával. A kiberhadviselés lehetővé teszi a támadó számára, hogy titokban és nyom nélkül maradjon, miközben jelentős kárt okoz a célpontnak.

Az APT csoportokról ismert, hogy számos területen - például kiberkémkedés, kiberhadviselés, befolyásszerzés, dezinformáció és ellenséges hírszerzési műveletek - célzott támadásokat hajtanak végre. Ezek a cselekmények összefonódnak egymással annak érdekében, hogy jobb eredményt érjenek el az APT-csoport céljainak elérésében, és ezáltal megzavarják a célpontjaik tevékenységét. A modern kibertér a kiber- és információs műveletek egyedülálló keveréke, és a fejlett, tartós fenyegetések csoportjainak támadásai veszélyeztetik a kormányokat, a vállalkozásokat és az egyéneket. A kibertámadások elleni hatékony védelem érdekében figyelembe kell venni, hogy e két művelet milyen módon kapcsolódik egymáshoz, és integrált megközelítéssel kell kezelni őket. Ez magában foglalja a kiberbiztonsági ismeretek és technológiák fejlesztését, a szervezetek és az egyének kiberbiztonsági tudatosságának növelését, valamint a nemzetközi együttműködést és a jogszabályok és szabályozások kidolgozását a kiberműveletek és információs műveletek megelőzésére és kezelésére.

Mindezek katonai alkalmazása az információs műveletekben valósul meg. Haig Zsolt az *Információs műveletek a kibertérben* című könyvében az alábbi definíciót használja:

> 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 résztvevő célközönség szándékára, helyzetértelmezésére és képességeire.” [7:15]

Kibontva ezt a definíciót, láthatjuk, hogy az információs műveletek része a technikai oldal, amelyet az egyszerűség kedvéért kibertérnek fogunk hívni. A kibertér egyik definíciója „egy mesterségesen létrehozott tartomány (domén), amely dinamikusan változik, amelyen keresztül és által az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek” [5:15]. A célközönség az információs

műveletekben túlterjed a katonai „közönségen”, a civileket is érinti, az ő befolyásolásuk az újabb definíciók szerint a dezinformáció. A dezinformációra ebben a disszertációban nem fogunk kitérni, azonban visszahivatkoznék az adatoknál említett 5V-re, és arra, hogy milyen fontos képesség az egyének szintjén is az adatok, információk valódiságának ismerete.

Az **információs hadviselés**[17] az információ felhasználását és kezelését jelenti a az információs fölény elérése érdekében. Az információs hadviselés támadó és védelmi jellegű lehet. Komplex információs támadás/védelem céljai elérése érdekében fizikai-, információs- és tudati dimenziókban fejti ki hatását [65]. Az **információs műveletek**[18] az amerikai megközelítés szerint (JP 3-13) öt pillérből állt: számítógépes hálózati műveletek[19], (amelyek magukban foglalják a számítógépes hálózati támadásokat, a számítógépes hálózatok védelmét és a számítógépes hálózatok kihasználását); pszichológiai műveletek[20]; elektronikus hadviselés[21]; műveleti biztonság[22]; és katonai megtévesztés[23].

A **fizikai dimenzióban** azon valós, fizikailag megfogható infrastruktúrák és eszközök találhatók, amelyek lehetővé teszik az egyének és a szervezetek számára az információkezelési folyamatok végzését. Emellett a különböző információs infrastruktúrák, infokommunikációs rendszerek elemei elleni fizikai támadások, illetve azok védelme is e dimenzióban valósul meg. Ennek megfelelően a fizikai dimenzió magában foglalja a vezetési és irányítási eszközöket és létesítményeket, az írott és nyomtatott papír- alapú információhordozókat (újságokat, könyveket), az adatgyűjtő eszközöket és szenzorokat, a kommunikációs eszközöket és létesítményeket, valamint az adattárolást és feldolgozást végző számítógépeket.

Az **információs dimenzió** az információs hadszíntér azon nem megfogható dimenziója, ahol a különféle információkezelési folyamatok zajlanak. E dimenzióban történik meg a fizikai dimenzióban értelmezett eszközökkel és infrastruktúrákkal az információ gyűjtése, tárolása, feldolgozása, továbbítása. Ezen kívül e dimenzióban értelmezzük egyrészt a különféle információs folyamatok többnyire elektronikus úton való támadását, másrészt a szemben álló fél saját információs folyamatainkra irányuló támadásának megakadályozását is.

A **tudati dimenzió** az információs hadszíntér azon dimenziója, ahol az emberek tudati tevékenységet folytatnak, amely az emberek vagy egyes csoportok információfeldolgozását, -

[17] Information Warfare (IW)
[18] Information Operations (IO)
[19] Computer Network Operations (CNO)
[20] Psychological Operations (PSYOPS)
[21] Electronic Warfare (EW)
[22] Operational Security (OPSEC)
[23] Military Deception (MILDEC)

észlelését, -értelmezését és döntéshozatalát jelenti. Az emberi döntéshozatali folyamat mellett e dimenzióban zajlik a szemben álló fél politikai és katonai döntéshozóinak, valamint a személyi állomány és a lakosság gondolkodásának, döntésalkotó képességének befolyásolása, másrészről a szemben álló fél ilyen irányú tevékenységével szembeni védelem is. Ezt a dimenziót a kulturális és vallási hiedelmek, normák, erkölcs, motivációk, érzelmek, tapasztalatok, képzettség, mentális egészségi állapot és ideológiák jelentősen befolyásolják. E tényezők meghatározása egy adott környezetben kritikus fontosságú annak megértéséhez, hogy hogyan lehet a legjobban befolyásolni egy adott célközönség gondolkodását és elérni a kívánt hatásokat. Mivel a döntéshozatal alapvetően kognitív folyamat, ezért ez a dimenzió képezi az információs környezet legfontosabb elemét. [7:151-152]

Összefoglalva az információs műveletek az információs környezetben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, kognitív (tudati) képességekkel közvetlenül, illetve technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire.[7:210]

A **kibertér erőszorzót kínál az IW tevékenységekhez**, hiszen napjaink információinak nagy része a kibertérben zajlik. A közösségi média és a botnetek felerősíthetnek egy üzenetet vagy narratívát, felhasználva az információ mindhárom elemét, hogy megosztottságot vagy zűrzavart szítsanak a célközönségben.

A kibertéri műveletek felhasználhatók stratégiai információs hadviselési célok elérésére; egy kibertámadás például felhasználható pszichológiai hatások elérésére egy adott célpopulációban. A kiberműveleteket egyéb információs műveletek céljára is végrehajthatják, így az ellenfélnek a saját kommunikációs vonalaihoz való hozzáférésének akadályozására vagy zavarására. Az IO lehet nyílt, például olyan anyagokat állít elő és terjeszt a kormány, amelyek célja a demokratikus értékek közvetítése. Ebben az esetben az ilyen tevékenység állami támogatása ismert. A titkos műveletek azok, amelyekben az állami szponzorációt tagadják, ha kiderül. A kibertér által biztosított anonimitás ideális terepet jelent a titkos információs műveletek végrehajtásához.

1.4 Következtetések

Az előző alfejezetek előkészítették az első hipotézisem megválaszolását. Meghatároztam annak keretét, hogy miben más a kibertér a többi hadviselési doméntől: időtől és tértől független, mindenhol jelenlévő, mesterséges (ember alkotta) és folyamatosan változik. Az egyik leglényegesebb egy nehezen megfogható eleme az emberi hozzáállás: hogy minden lehetséges, hiszen egy határtalan dimenzióban mozognak. Itt nem került explicit kifejtésre, azonban egy másik nagy hasonlóság a technológiához való viszony: használói függnek tőle, és ők a különböző új technológiáknak általában ún. *early adopter*-ei, azaz másokat megelőzve elkezdik őket alkalmazni, használni, kísérletezni velük.

A kibertér definíciójára nincs széles körben elfogadott, egységes változat. Ez megnehezíti azt, hogy „egy nyelvet beszéljünk", akár kutatásról, akár szakpolitikáról legyen szó. Azonban álláspontom szerint nem várható a jövőben egy egységes definíció meghozatala – egész egyszerűen azért, mert a nemzetállamoknak nem érdekük korlátozni saját lehetőségeiket, elősegítve ezzel az elrettentést [56], illetve olyan pragmatikus okokból is, mert gyorsabban változik a technológia, mintsem az szabályzókkal, doktrínákkal lekövethető lenne.

Mindezek mellett azonosítottam azon részterületeket, amelyek szükségesek a kiberhadviselési képességek meghatározásához, és összegeztem őket az alábbi definícióban:

> *A kiberhadviselés a kiberműveleti képességek teljes spektrumának használata, összhangban a hazai jogszabályokkal, valamint a mindenkori Tallinn-kézikönyv normáival.*

Jelen fejezet a [6] és [31] saját publikációra épül, amely hozzájárult a kutatási céljaim eléréséhez. A fejezethez nagyban hozzájárult a NATO CCDCOE *Integrating Cyber Considerations into Operational Planning*[24] c. kurzusa, elsősorban a kiberműveleti terület és a kiberműveletek részletezésénél.

[24] A kiberműveletek aspektusainak integrálása a művelettervezésben.

2. A kiberképesség fejlesztésének akadályai, azok megszüntetése

A változtatás többirányú erőfeszítést igényel. A kiberképességekre vonatkozóan öt ilyen összetevőt azonosítottam: a döntést gátló akadályok megszüntetését, a befektetés (finanszírozás) biztosítását, a változtatások elfogadását és beillesztését, annak leszabályozását és a védelmét. Az innovációt, az új technológiák befogadását többféle akadály nehezítheti. Ezek lehetnek szervezetiek például egy szervezet kialakulása után nehéz annak irányultságát vagy struktúráját megváltoztatni. Ez az úgynevezett *path dependency*[25], a „mi így szoktuk, eddig bevált" háttere. Ahhoz azonban, hogy egy ilyen „felforgató" technológiákat tartalmazó terület katonai szervezetként sikeresen beépüljön és fennmaradjon, szükséges az innováció akadályait megszüntetni.

2.1. Bevezetés

A katonai innováció a doktrínák fejlődésén, a működési háttér pedig a szervezeti szubkultúrák mechanizmusán keresztül mérhető, amelyek alakítják a bennük levők viselkedését és meggyőződését. A különböző szubkultúrák tanulmányozása azért fontos, mert külső bizonytalanságok esetén - mint amilyen egy szervezeti átalakítás - az innováció pályájának elsődleges meghatározója a kutatás alapján az adott szervezet (szub)kultúrája – aminek az átalakítás bukására vagy sikerére döntő hatása lesz. Jól ismert tény a szakirodalomban, hogy a külső korlátok hatnak az innováció folyamatára[26], és hagyományosan úgy tekintik, hogy ezek a korlátok vagy megakadályozzák, vagy ösztönzik az innovációs folyamat beindítását, azonban kevéssé foglalkoznak azzal, hogy hogyan fog kinézni a képességfejlesztési folyamat, ha már egyszer elkezdődött.

[25] Útfüggősség: közgazdasági és társadalomtudományi fogalom, olyan folyamatokra utal, ahol a múltbeli események vagy döntések korlátozzák a későbbi eseményeket vagy döntéseket. Az útfüggőséget az intézmények, a technikai szabványok, a gazdasági vagy társadalmi fejlődés mintái, a szervezeti viselkedés leírására használták. [66]

[26] Többek között: Barry R. Posen, *The Sources of Military Innovation: France, Britain, and Germany Between the World Wars* (New York: Cornell University Press, 1985); Stephen P. Rosen, *Winning the Next War: Innovation and the Modern Military* (New York: Cornell University Press, 1991); Kimberly Marten Zisk, *Engaging the Enemy: Organization Theory and Soviet Military Innovation 1955-1991* (Princeton University Press, 1993); Deborah D. Avant, *Political Institutions and Military Change: Lessons From Peripheral Wars* (Ithaca: Cornell University Press, 1994); Elizabeth Kier, *Imagining War: French and British Military Doctrine Between the Wars* (Princeton University Press, 1999); Deborah D. Avant, "From Mercenary to Citizen Armies: Explaining Change in the Practice of War," *International Organization* 54, 1 (Winter 2000): 41-72; Thomas G. Mahnken, *Uncovering Ways of War: U.S. Intelligence and Foreign Military Innovation*, 1918-1941 (New York: Cornell University Press, 2002).

A katonai kiberszervezetek létrehozásának, fenntartásának egyik sarokköve az akadályok megszüntetése. Ezalatt értjük a doktrinális környezet kialakítását, az ebből fakadó törvénymódosításokat, egészen odáig, hogy a kiberképességek megjelenjenek a műveletтervezésben és végrehajtásában. A második fejezethez kapcsolódóan azt feltételeztem, hogy **az akadályok megszüntetése szempontjából eltérő rendszerek alakulnak ki a V4-es tagországok és Németország esetében.** Ennek bizonyítására szükségem volt egy keretrendszerre, amelyben értelmezhetők az információk. Kutatásom elején a PMESII[27]–ASCOPE keretrendszert terveztem használni, azonban hamar kiderült számomra, hogy nem ez lesz a megfelelő eszköz, ezért helyette a DOTMLPF[28], később pedig a PETIO[29][30]

[27] A PMESII és az ASCOPE elemzési módszerek, amelyeket általában a műveleti környezet elemzésére használnak. A PMESII a következő tényezőket fedi le: politikai, katonai, gazdasági, társadalmi, információ, infrastruktúra. Az ASCOPE pedig: területek, struktúra, képességek, szervezetek, emberek és események.

[28] A kiberképesség-fejlesztés szintéziseként a DOTMLPF amerikai betűszó használatát alkalmazom [67], miután egyfelől kellőképpen részletes és árnyaltan közelíti meg a kérdést, másfelől a NATO által használt megközelítéshez kapcsolódik, amely biztosít egyfajta konvergenciát. Az eredeti betűszót az Egyesült Államok használta: a Közös Képességek Integrációs Fejlesztési Rendszerben (Joint Capabilities Integration Development System – JCIDS) van meghatározva. Az Egyesült Államok által használt eredeti DOTMLPF-hez a NATO az interoperabilitás követelményét illesztette (DOTMLP-I) [15], illetve később az Egyesült Államok is kiegészítette a szakpolitikai irányelvvel (Policy, DOTMLPF-P). A disszertációban az Egyesült Államok által használt rövidítést fogom használni.

A doktrínákban és szakpolitikai dokumentumokban lefektetett tervek megvalósításához képességekre van szükség. A vezetőknek a tervek áttekintésekor fel kell mérniük, hogy rendelkeznek-e a megfelelő képességgel. Ha a képességek és a követelmények nem egyeznek, akkor kockázatértékelést kell végezni, és ha a követelmények meghaladják a képességeket, és a kockázat túl magas ahhoz, hogy elfogadjuk, akkor képességfejlesztés szükséges. A DOTMLPF azonosítja azokat az elemeket, amelyeket figyelembe kell venni a képesség biztosításához.

[29] PETIO: people, exploits, toolset, infrastructure, organizational strucutre, azaz emberek, sérülékenységek kihasználásának képessége, eszközrendszer, infrastruktúra, szervezeti felépítés.

[30] Max Smeets az ún. PETIO-keretrendszerbe foglalja össze a támadó kiberképességek kiépítésének és fenntartásának szükséges elemeit. Ahogyan összefoglalja: „Az első és legfontosabb elem a hatékony kiberművelet végrehajtásához szükséges emberek (humán erőforrás). Másodszor, egy államnak el kell gondolkodnia azon, hogyan tudja kihasználni a számítógépes rendszerek sebezhetőségeit a hozzáférés megszerzésére, fokozására és fenntartására. A harmadik elem az eszköztárra vonatkozik, amely más programok vagy alkalmazások létrehozására, karbantartására vagy egyéb támogatására szolgáló számítógépes programok összessége. A PETIO-keretrendszer negyedik eleme az infrastruktúrára. Megkülönböztettem az irányítási infrastruktúrát – a műveletek lebonyolításához közvetlenül használt folyamatokat – és az előkészítő infrastruktúrát – azokat a folyamatokat, amelyek segítségével az ember készen áll a kiberműveletek végrehajtására. Míg az előbbi típusú infrastruktúrát egy-egy művelet után gyakran lebontják, addig az utóbbit ritkán cserélik le az üzemeltetési tevékenység után. Az utolsó elem a szervezeti felépítésre vonatkozik. A

keretrendszereket használtam. A nemzetállamok közötti eltérések feltérképezése során azt tapasztaltam, hogy az akadályokat illetően alig van különbség az előzetesen kiemelt nemzetállamok között. Miután a kiberképesség-fejlesztés IT-intenzív terület, ahol ráadásul a fejlesztések egy jó része a privát szférában történik, az ottani képességfejlesztési módszert (agilis módszertan[31]) megvizsgáltam, és felmértem annak használhatóságát a katonai képességfejlesztésben.

A kutatáshoz egyfelől leíró jellegű megfigyelést végeztem nemzetközi irodalomkutatással, illetve több feltáró beszélgetést folytattam nemzetközi környezetben az agilis módszertan használhatóságáról, valamint a kiberképesség-fejlesztés akadályairól.

A fejezet első alpontjában bemutatom a az EU kiberképességeket, majd ismertetem a főbb akadályokat a képességfejlesztés területén. Minden részhez teszek kitekintő megjegyzéseket a V3-akra és Németországra vonatkozóan, mint az eredetileg vizsgált országokra. Végül áttérek az agilis módszertanra és annak katonai felhasználási lehetőségeire és a részkövetkeztetéseket mutatom be.

2.2 EU kiberképességek

Bár az Európai Unió (EU) régóta fejleszti a számítógép-biztonsággal és az elektronikus hírközléssel kapcsolatos tevékenységeket, csak az elmúlt évtizedben hozott tudatos döntést a kiberbiztonság növeléséről. Az egyéneket, vállalatokat és kritikus infrastruktúrákat érő számítógépes támadások növekvő számával szembesülve az EU diskurzusában lassan többségbe került az az elképzelés, hogy a társadalom technológiától való függése olyan, egyre gyorsabban növekvő biztonsági kockázatot jelent, amelyet megfelelően kezelni kell. Tekintettel arra, hogy a kiberteret és a kiberbűnözőket nem korlátozzák a nemzeti határok, ez a felismerés olyan jogi intézkedések elfogadását eredményezte, mint például az információs rendszerek

szervezetközi folyamatok szempontjából kulcsfontosságú dimenzió a hírszerzési és katonai folyamatok integrációja.” [17:92]

[31] Az agilis módszertan egy olyan projektmenedzsmenti szemlélet, amelynek fő erénye a rugalmassága. A fejlesztőcsapatok rövid időkre bontott részfeladatok eredményeit mutatják be, és ennek okán tudnak reagálni a változó elvárásokra, körülményekre.

A hagyományos projektmenedzsment alapfeltevése, hogy a rendszerspecifikációk könnyen azonosíthatók a projekt elején, megfelelő tervezés mellett megvalósíthatóak, és annak sikerét a költségek–minőség–idő hármasával mérik. Az agilis projektmenedzsment iteratív (ismétlődő) megközelítésként definiálható, amelybe közvetlenül bevonják a „megrendelőt”, és minél előbb működő terméket fejleszt [68:6775]. Az agilis projektek sikerének két legfontosabb mérőszáma továbbra is az üzleti/hozzáadott érték, valamint a vevő/felhasználó elégedettsége [68:6776].

elleni támadásokról szóló 2005-ös tanácsi kerethatározat. Emellett új szervezetek álltak fel, az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) vagy az Európai Kiberbűnözés Elleni Központ az Europolnál (EC3) [69:1261].

A koherencia különösen fontossá vált az EU kiberbiztonsági politikájában, mert annak irányítása hosszú ideig nagyon széttagolt volt, és az érintettek egymástól függetlenül dolgoztak olyan területeken, mint a bűnüldözés, a kritikus információs infrastruktúra védelme és a kibervédelem. Azóta előrelépés történt politikai, jogalkotási és képességi szinten is. A képességek megerősítését ösztönözték a kiberbiztonsági kutatási és innovációs finanszírozási források létrehozásával, a nemzeti infrastruktúrák továbbfejlesztése (annak érdekében, hogy például minden tagállam rendelkezzen kiberbiztonsági központokkal, govCERT-ekkel), valamint a köz- és a magánszféra közötti partnerségek létrehozásának elősegítésével.

A jövőre nézve, folyamatban van egy határozattervezet elfogadása, amely megerősítené az ENISA megbízatását, az EU Kiberbiztonsági Ügynökségévé alakítva azt, valamint kiberbiztonsági tanúsítási rendszer létrehozását tervezik termékek, szolgáltatások és folyamatok számára a digitális egységes piac támogatása érdekében. Emellett jóváhagyták az ún. kiberdiplomáciai eszköztárat, amelynek végső célja az EU e téren végzett tevékenységeinek megerősítése, valamint a kibertámadások esetén az összehangoltabb reagálás lehetővé tétele.

2023. április 18-án az Európai Unió Bizottsága elfogadta a **kiberbiztonsági szolidaritás**ról szóló uniós jogszabályra irányuló javaslatot, amelynek célja az EU kiberbiztonsági kapacitásainak erősítése. A főbb kiberfenyegetések gyors és hatékony felderítése érdekében a Bizottság javasolja egy EU-szerte működő nemzeti és határokon átívelő biztonsági műveleti központokból[32] álló pán-európai infrastruktúra, az európai kiberbiztonsági pajzs létrehozását. Az említett szervezetek feladata a kiberfenyegetések felderítése és az azokkal szembeni fellépés.

A javasolt jogi aktus előmozdítja a tagállamokban a kiberbiztonsági fenyegetések és események felderítését, javítja a kritikus fontosságú szervezetek felkészültségét, továbbá erősíti a szolidaritást, illetve az összehangolt válságkezelési és reagálási képességeket. A kiberbiztonsági szolidaritásról szóló jogszabály a meglévő együttműködési mechanizmus megerősítése mellett megteremti a szükséges uniós képességeket ahhoz, hogy Európa ellenállóbbá váljon és hatékonyabban tudjon fellépni a kiberfenyegetésekkel szemben. A javaslat biztonságos digitális környezetet biztosít a polgárok és a vállalkozások számára,

[32] SOC, security operations center

valamint elősegíti a kritikus fontosságú szervezetek és az alapvető szolgáltatások, így a kórházak és a közüzemi szolgáltatások védelmét.

A közös biztonság- és védelempolitika (KBVP) területén kiemelendők az ún. PESCO[33] projektek, amelyek elsősorban védelmi jellegű együttműködések. A kiber területén öt ilyen projekt fut jelenleg, ezek a Kiber- és Információs Domén Koordinációs Központ (Cyber and Information Domain Coordination Center, CIDCC, Magyarország részvételével), a Cyber Ranges Federáció (Cyber Ranges Federation, CRF), a Kiber Gyorsreagalású Csapatok (Cyber Rapid Response Teams, CRRT), a Kiberfenyegetések és incidensekre adott válaszok információmegosztó platformja (Cyber Threats and Incident Response Information Sharing Platform, CTIRISP) és az EU kiber akadémiai és innovációs központja (EU Cyber Academia and Innovation Hub (EU CAIH).

2021 novemberében fogadták el az EU kibertérre, mint műveleti területre vonatkozó katonai vízióját [70], melynek megvalósításához hét egymást kiegészítő lépésre van szükség a dokumentum szerint.

1. Biztosítani szükséges az EU stratégiai céljainak elérését a KBVP katonai műveletei és küldetései során, a hatékony és interoperábilis kibertér-képességek révén.
2. Integrálni kell a kiberteret, mint műveleti területet az EU KBVP katonai műveleteibe és küldetéseibe, **különösen a helyzetfelismerés**, a korai figyelmeztetés, az előrejelzés és a válságreagálás tervezése révén.
3. Az EU KBVP katonai műveleteinek biztosítását a kibertérben.
4. Hatékony és következetes kiber elrettentés biztosítása - az EU KBVP katonai műveleteinek és misszióinak potenciális ellenfelei ellen hatékony uniós kibervédelmi képességek összehangolt és prioritások szerinti létrehozása, alkalmazása és kommunikációja - révén.
5. Biztosítsa az EU katonai KBVP erőfeszítéseinek egységét a kibertérben, hatékony polgári-katonai kapcsolatok és szinergiák révén, összhangban az EU válságkezelésének integrált, több területet átfogó megközelítésével.
6. Erősítse meg az EU KBVP katonai műveleteinek és kibertérbeli misszióinak fenntarthatóságát és interoperabilitását a nemzetközi partnerekkel a kibertér

[33] Permanent Structured Cooperatoin, állandó strukturált együttműködés

képességeinek fejlesztése, megosztása és kölcsönösen támogató alkalmazása terén folytatott **PESCO együttműködés** révén.

7. Biztosítani kell az EU legkorszerűbb kibertér-képességeit annak közös és összehangolt kutatása és fejlesztése révén.

2.3 Az akadályok megszüntetése

„Először is stratégiai korlátok jelentkeznek a kiberműveletek végrehajtása során. A stratégiai itt a kiberműveletek felhasználását jelenti egy adott politikai cél elérése érdekében. Míg a legtöbb államot köti ez a megszorítás, úgy tűnik, nagyon eltérő nézetek vannak arról, hogy a kiberműveletek hogyan támogathatják a nemzeti stratégiát, vagy segíthetnek elkerülni és/vagy befolyásolni egy konfliktus stratégiai kimenetelét.” [71]

Mégis is egyre jobban felismerik, hogy a kiberműveletek sokoldalúak, és sokféle helyzetben alkalmazhatók [72]. Béke és háború idején, különböző intenzitású konfliktusokban, kinetikus erőkkel és anélkül is használhatók [73][74]. Másodszor, vannak lehetséges jogi és normatív korlátok, amelyeket figyelembe kell venni. A „kibernormák” kutatása, kialakítása sok éven át, több helyszínen zajlik, és a szereplők széles körét érinti. Noha hiányzik egy átfogó nemzetközi kibernormarendszer, ez nem jelenti azt, hogy az államok ne követnék saját hazai jogi rendelkezéseiket. Valójában a kiberparancsnokságokat (és a hírszerző ügynökségeket) gyakran szigorú jogi keretek kötik. Ez magában foglalhatja például azokat a körülményeket, amelyek között a kiberműveletek alkalmazhatók, hogyan kell erőszakot alkalmazni a fokozatos és arányos válasz érdekében, és hogyan lehet egyensúlyt teremteni a szükségesség és az arányosság között [17:45].

2.3.1 Doktrína

A doktrína[34] a katonai szolgálat teljes szervezeti felépítését is áthatja: befolyásolja, hogy egy szolgálat hogyan szerveződik, mit helyez előtérbe. A doktrína ideális annak megértéséhez, hogy egy szervezet hogyan látja önmagát és szerepét.

[34] Doktrínának nevezzük az olyan alapelvek összességét, amelyek irányítják egy nemzet katonai erőinek összehangolt fellépését egy közös cél érdekében. A doktrína annak formális kifejezése, hogy egy katonai szervezet hogyan szándékozik harcolni. Továbbá „fogalmi magként szolgál,

Egy specifikus kiberdoktrína értelmezhető úgy, hogy leírja a hadsereg viszonyát a kibertérhez és azon keresztül hogyan képzeli el a hadsereg a kiberteret, hogyan használja a katonai erő a kiberteret céljainak eléréséhez, és hogyan integrálja a kiberteret a katonai műveletekbe. Emiatt is fontos volt a korábbi fejezetben tisztázni, hogy mit értünk kibertér alatt, mint önálló domén. A domének a katonai stratégiákon belül azért fontosak, mert referenciakeretet adnak az elméleti elgondolásoknak, mely elgondolások mentén határoznak meg követelményeket és végső soron, készítik fel az állományt az adott doménben vívott harcokra.

Ugyanakkor a kiberműveletek nem tekinthetők „abszolút fegyvernek", és értékük sem egyértelműen nyilvánvaló [17:42]. A védelmi célú kiberberuházások, befektetések lehetővé teszik a vezetők számára, hogy nagyobb biztonságban érezzék magukat, és kisebb működési kockázatot vállaljanak. Így, ha a védelmi technológiák és műveletek kapnak prioritást, korlátozottak maradnak a cselekvési lehetőségek és a manőverezési képesség. A humántőkébe és a technológiába történő befektetéseknek kiegyensúlyozottnak kell lenniük – de nem feltétlenül egyenletesen – az offenzív és defenzív oldal között. Az egyik kulcskérdés, hogy mennyibe kerül a kiberbiztonság. A helyes megközelítés a következő: mi a nemzeti kiberstratégia, és hogyan használja fel a hadsereg az erőforrásait ennek elérése érdekében?" [76]

A regionális összesítésben (V4 és Németország esetében) egyedül a Szlovák Nemzeti Kibervédelmi Stratégiában jelenik meg explicit módon a finanszírozás kérdése: „A cselekvési tervben is meghatározott felelősök mindegyikének elegendő forrást kell elkülönítenie a költségvetési soron belül a jóváhagyott cselekvési tervben, valamint a kiberbiztonság elvein alapuló feladatok és tevékenységek teljesítésére. Ezen meghatározott feladatok végrehajtásában nemcsak az állami költségvetésre, hanem az Európai Közösségi alapok operatív programjaiból származó forrásokra is támaszkodhatnak." [77]

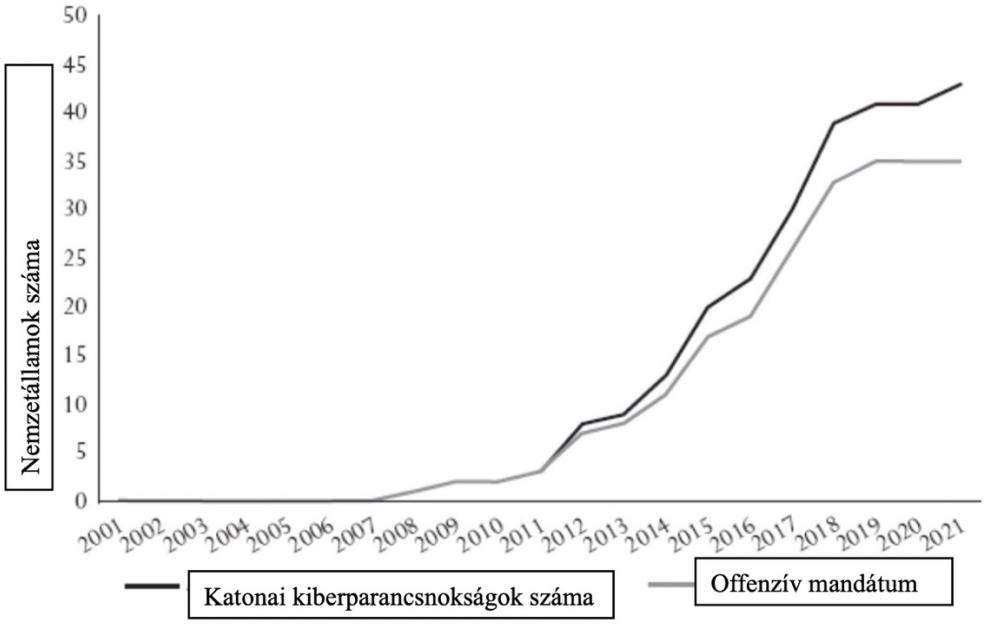
A doktrinális hátteret tekintve többségükben megjelenik az offenzív kiberképesség-fejlesztés. Lengyelország írja le a legrészletesebben a céljait („Kapacitás megszerzése a katonai műveletek teljes spektrumának végrehajtásához a kibertérben" [78]), valamint

amely körül döntéseket kell hozni az erő megszervezéséről, kiképzéséről és felszereléséről" [75].

következményeit egy ellenséges kibertámadásnak (gyakorlati szempontból a súlyos kibertámadásokra adott válasz koordinálható szükségállapot, természetikatasztrófa-állapot vagy hadiállapot kihirdetésével [78]).

2.3.2 A szervezet (O)

A 9. ábra bemutatja azt a trendet, miszerint 2007 - kibertörténelemből ismerten az Észtországi elleni támadás[35] - után kezdtek el megjelenni a katonai kiberszervezetek és kaptak mandátumot arra, hogy - jól körülírt esetekben - offenzív választ is adhassanak. 2010 után egy újabb ugrás következik, a STUXNET felfedezésével[36]. 2016-2017-ben jelennek meg a WannaCry és a NotPetya ransomware-k[37], amelyek ismét ráirányítják a figyelmet a kiberbiztonság fontosságára. Fontos megjegyezni, hogy az ábrán nem szerepelnek az ezen idő alatt hasonló célra létrehozott polgári szervezetek.



[35] Az észt kormányzati webhelyeket megosztott szolgáltatásmegtagadási támadások (DDoS) érik, és 22 napig maradtak kompromittálva. A célpontok között szerepelt az elnöki hivatal, a parlament, a rendvédelmi tisztviselők fiókjai és Észtország két legnagyobb bankja.

[36] A Stuxnetet a világ első katonai minőségű kiberfegyvere, ez az első olyan fegyver, amely tönkretehet ipari berendezéseket, és egyben az első, amely PLC-t (programozható logikai vezérlőt) tartalmaz. Ezzel a szoftvert arra tervezték, hogy elrejtse létezését és tevékenységét.

[37] Ransomware, másnéven zsarolóvírus. A kártevők egy olyan fajtája, ami letitkosítja az általa elérhető tárhelyeken tárolt dokumentumainkat, fotóinkat, videóinkat és egyéb fájljainkat, a visszaállításhoz szükséges kulcsot pedig csak váltságdíj ellenében adják át.

9. ábra: Kiberparancsnokságok számának növekedése[17:33]

Az állam által irányított kiberműveletek nem szervezeti légüres térben zajlanak. Még akkor is széleskörű koordinációra van szükség, ha a katonai erőkön belül külön parancsnokságokat vagy részlegeket hoznak létre a kiberműveletek végzésére. Például ”nincs értelme támadó kiberművelet végrehajtásának, ha a hatás előnyei nem haladják meg a hírszerzési erőfeszítések költségeit.” [17:45] Ilyen összevonó szervezeti példaként említhető a német szövetségi kiber- és információs parancsnokság (Cyber-und-Informationsraum – CIR), amely a német hadsereg hatodik ágává vált – a szárazföldi haderővel, a haditengerészettel, a légierővel, a közös orvosi szolgálattal és a közös logisztikai, támogató szolgálattal azonos szinten. A CIR alatt helyezkednek el a híradó-, a pszichológiai műveleti, a stratégiai felderítési (beleértve a SIGINT-et, a rádióelektronikai felderítést), a földrajzi információs (katonai műholdak) és az elektronikai hadviselés egységei. Egy ehhez hasonló szervezet – és feladatintegráció – óhatatlanul együtt jár a profiltisztítással is, mégis világosan jelzi a külvilág felé a stratégiai prioritások változását.

Az akadályokat tekintve itt is fontos kiemelni a már említett útvonalfüggőséget *(path dependency*) Az path dependency olyan rendszerfolyamatot ír le, amelyben a múltbeli választások és döntések korlátozó hatással vannak a jövőbeli lehetőségekre. Más szavakkal, a szervezet múltban hozott döntései eleve korlátozzák a jövőben a szervezet számára elérhető lehetséges döntések körét, még akkor is, ha a múltbeli körülmények, amelyek ezeket a döntéseket körülvették, már nem relevánsak. Az eredmény egy olyan szervezet, amely nem tud alkalmazkodni a változó követelményekhez. Ez hatással lehet a képességfejlesztésre is, hiszen a többéves beszerzési és modernizációs ciklusok előre meghatározzák az eredményt, holott a körülmények és az elvárások közben megváltozhatnak.

Szervezeti szinten ugyancsak fontos akadály lehet a kinetikus és nem-kinetikus erők mesterséges szétválasztása, a harcoló és támogató funkciók szembe állítása.[57]. A hadsereg egy emberközpontú szervezet, amelynek elsődleges célja a szárazföldi háborúk megvívása és megnyerése. Ennek elengedhetetlen eleme a katona. Tehát a két alapvetésből kiindulva, hogy a hadsereg alapvetően kinetikusan és a terepen lévő *(boots on ground)* katonával számol, előreláthatólag szervezeti szkepticizmust kelt minden olyan technológiával vagy technológiai fejlesztéssel szemben, amely nem az egyes katonák támogatására irányul a taktikai manőver legalacsonyabb szintjén.

Ennek következménye, hogy egy hadsereg a korai szakaszban küzdeni fog a kibertér-koncepciók és képességek integrációja folyamán a területen való sikerhez szükséges technológiai szakértelem és a siker minőségi mérésének nehézségei miatt. Ahhoz, hogy ez feloldódjon, a kiberteret be kell illeszteni a hadsereg domináns manőverkultúrájába, hogy széles körű intézményi elfogadottságot élvezhessen. Fogalmilag ez az asszimiláció a doktrína fejlődésén keresztül történik meg. Gyakorlatban pedig olyan képességek fejlesztésén keresztül fog megvalósulni, amelyek taktikai szinten egyre fontosabbak. A fent leírt minta egyértelműen kirajzolódott az utolsó fejezetben az amerikai hadseregről írottakban: kiindulópont egy túlnyomórészt alacsony technológiájú szolgálat, amelynek elsődleges hangsúlya az egyes katonákon van, nem pedig az általa hordozott vagy üzemeltetett felszereléseken. A hadsereg taktikai képességét közvetlenül meghatározó, stratégiai, hírszerzési alapú vállalkozásként megjelenő kiberprobléma sikeres megoldása érdekében a hadsereg a kibertéri műveleteket az egyes műveleti egységek szintjére emelte, miközben ezzel párhuzamosan kiterjesztette a kibertűzek fogalmát (kiberhatások), hogy jobban illeszkedjenek a szolgáltatás meglévő fogalmi keretei közé. E célból a hadsereg kiberszemélyzetének egy kijelölt alcsoportja a kis egységeket érintő problémákra fordíthatná erőforrásait, így például a légi drónok elterjedésével kapcsolatos problémák, a taktikai kommunikációs hálózatok védhetősége, vagy az ellenfél kibertérhasználatának hatásai a műveletparancsnok kijelölt műveleti területét érintően. [79]

A katonai kiberszervezetet egy, a nemzeti kormány fegyveres erőin belüli parancsnokságként, szolgálatként vagy egységként definiált szervezet, amelynek felhatalmazása és feladata a kiberműveletek végrehajtása. A kiberműveletek általánosságban magukba foglalnak támadó, védekező és felderítő képességeket [80]. Ezek a szervezetek eltérőek aszerint, hogy az adott országnak milyen stratégiai célkitűzései vannak, illetve milyen jogi, szervezeti környezettel, milyen széles vagy szűk műveleti hatáskörrel rendelkeznek, mekkora létszámmal dolgoznak, milyen együttműködés van a katonai, rendvédelmi és polgári szervek között.

Max Smeets tanulmányában [81] összegezte az offenzív katonai kiberszervezetek létrehozásának előnyeit és kihívásait. A nemzeti katonai kiberparancsnokságok szervezeti felépítése igen eltérő képet mutat annak függvényében, hogy az egyes államok mennyire központosítottak, mekkora méretűek, milyen felelősségi körük van. Az államok egyik alapvető dilemmája - a szerző szerint - azon kérdés eldöntése, hogy integrálják-e (és ha igen, hogyan) a felderítési és katonai képességeiket a támadó kiberkapacitás fejlesztéséhez?

Smeets három előnyt és kockázatot azonosított [81]. Egy ilyen integráció előnye, hogy (1) biztosíthatja a hírszerzés és a katonai tevékenységek hatékonyabb együttműködését, amely fontos szerepet játszik a kiberműveleteknél mint támogató művelet, (2) a szervezeti integráció növeli a közvetlen és közvetett tudásátadást, és (3) lehetővé teszi az erőforrások hatékonyabb elosztását, továbbá csökkenti a feladatok közötti átfedéseket. A kockázatok között az első az ún. kiberbiztonsági dilemma, azaz a klasszikus biztonsági dilemma megjelenése a kibertérben: mások elrettentése céljából elindulhat egyfajta támadókapacitás-fejlesztési verseny. A második kockázatot a költségek növekedése jelenti: miután nem elégséges a kezdeti beruházás, folyamatos fejlesztésekre és újabb erőforrásokra lesz szükség ezen a területen, beleértve a humánerő fejlesztését és megtartását célzó törekvéseket is. Végül a szervezeti integráció jelentheti az eredeti küldetés kiterjesztését is (azaz a katonai kiberszervezetek „kiber-mindenessé" válhatnak, és olyan feladatokat is megkaphatnak, amelyek nem kötődnek szigorúan véve az eredeti küldetésükhöz.

Számos európai ország speciális katonai egységeket vagy ügynökségeket hozott létre a kibervédelem és a kiberműveletek feladatainak ellátására. Ezen egységeknek gyakran hasonló a feladatuk, beleértve az ország katonai és kormányzati hálózatainak védelmét, valamint mindannyian támadó kiberműveleteket hajtanak végre a nemzetbiztonsági célok érdekében.

A regionális szervezeteket tekintve Csehországban a katonai kibervédelem a Kommunikációs és Információs Rendszerek Ügynökségének (CISA) feladata, amely a Támogatási Osztály része, ez viszont a Cseh Köztársaság Fegyveres Erők Vezérkarának alárendeltje [82]. Ami az aktív kibervédelmet illeti, létrejött a Kibererők Parancsnoksága [83], amely önállóan, vagy hazai és szövetséges keretek között hajtja végre feladatait. Felelnek a műveletтervezésért és irányításért, továbbá a hadsereg STRATCOM támogatását is végzik. Biztosítják a kibertér „belföldi" védelmét, információs, pszichológiai műveleteket hajtanak végre, és szorosan együttműködnek a katonai hírszerzéssel.

Németországban a Szövetségi Védelmi Minisztériumot (Bundesministerium der Verteidigung, BMVg) a védelmi miniszter vezeti, aki békeidőben a német fegyveres erők legfőbb parancsnokaként szolgál. A közelmúlt német hadtörténelmének egyik legfigyelemreméltóbb fejleménye a Kiber- és Információs Domén Szolgálat (Cyber- und Informationsraum, CIR) elnevezésű új szervezet létrehozása 2017-ben. A CIR a Bonnban található Kiber- és Információs Domain Parancsnokság (Kommando Cyber- und

Informationsraum, KdoCIR) köré épül fel, tagjai szinte minden olyan katonai műveletben részt vesznek, amelynek a Bundeswehr részese.

A lengyel kormányban a katonai kibervédelemért felelős legmagasabb rangú tisztviselő a védelmi miniszter. A védelmi oldalon, a Honvédelmi Minisztériumon belül a lengyel katonai hálózat biztosításáért felelős egység a 2008-ban létrehozott MIL-CERT PL. Három szintre szerveződik: az első szint egy Koordinációs Központból (Centrum Koordynacyjne, CK) áll, amelyet a Katonai Elhárító Szolgálat egy alegysége működtet. A második egy Technikai Támogatási Központ (Centrum Wsparcia Technicznego, CWT), amely a CERT felelősségi körébe tartozik. A harmadik a minisztérium különböző részlegeinek rendszergazdáiból áll. A Kiberműveleti Központot (Centrum Operacji Cybernetycznych, COC) 2017-ben hozták létre, a Nemzeti Kibertér-biztonsági Központ igazgatójának közvetlenül alárendelt, a katonai műveletek és a kibertérben végzett műveletek területén illetékes szervezeti egység. A Kibervédelmi Erők (lengyelül: Wojska Obrony Cyberprzestrzeni) a Lengyel Fegyveres Erők speciális alkotóeleme, amelyet Mariusz Błaszczak honvédelmi miniszter 2022. február 8-án hozott létre Varsóban.

Szlovákia esetében a Védelmi Minisztérium stratégiai víziójába (és stratégiai dokumentumaiba) belefoglalja a kibervédelmet, a kiberbiztonságot azonban többnyire szerves képességként gyakorolja a minisztérium saját szükségleteire. A kiberműveleti erők a Különleges Műveleti Erőkbe vannak integrálva.

2.3.3 A kiképzés

A kiberműveleti képességek tekintetében a kiképzést a kibergyakorlatok adják, általában virtuális környezetben. A katonai kibergyakorlatok fő előnyei abból adódnak, hogy élőben és utólag is tudnak adatokat gyűjteni és elemezni, valamint jelzésértékű a nemzetközi környezetben (elrettentés). A kiberképesség szintjének mérése köztudottan nehéz. A katonai kibergyakorlatok azonban felhasználhatók a meglévő képesség és hajlandóság jelzésére a kiberműveletek végrehajtásában vagy ellenséges műveletekre való reagálásban.

A katonai kibergyakorlatok előtt álló kihívások abból adódnak, hogy nehéz a megfelelő környezet kialakítása, amely reális időkeretekkel és dinamikával rendelkezik. A kibergyakorlatok aligha tartanak tovább néhány napnál. Ez félrevezető elvárásokat támaszthat a kiberműveletek természetével kapcsolatban. A másik probléma, hogy a szcenáriók általában

rendkívül pusztító kibertámadások köré csoportosulnak, viszonylag rövid ideig – tipikus forgatókönyv a kritikus infrastruktúra elleni támadás egy ellenséges állam részéről. Azonban a legtöbb offenzív művelet, amit a kibertérben megfigyelünk, több éven át tartó fedett műveletsorok eredményei, amelyek gyakran összekapcsolt kiberműveletekből állnak, azzal a céllal, hogy stratégiai eredményeket érjenek el fegyveres támadás nélkül [84].

További kihívásokat jelenthetnek a szervezetek számára az erőforrás-korlátok. A kibergyakorlatok erőforrás-igényesek lehetnek, és jelentős idő- és pénzügyi ráfordítást igényelhetnek úgy a tervezéshez, mint a végrehajtáshoz. Emiatt is fontos a minőségi részvétel és elkötelezettség biztosítása a szervezők/résztvevők oldaláról. Az eredmények értékelése és mérése további nehézséget jelenthet. A pontos kiértékelésre és mérésre elengedhetetlen ahhoz, hogy meghatározzuk a kiberműveletek hatékonyságát és azonosítsuk a javítandó területeket.

2.3.4 Képzés és kiválasztás

A technológia (és a technológiai fölény) fontos alap a kibertérben és a kiberműveletekben, de a műveletek sikerét továbbra is az egyének határozzák meg.
Az amerikai hadsereg négy olyan értéket vázolt fel, amelyek a kiberkatonákat jellemzik:
1. professzionalizmus,
2. bizalom,
3. fegyelem,
4. precizitás (a járulékos károk éppen olyan súlyosak lehetnek a virtuális térben, mint bármely más harctéren).

A RAND által végzett kutatás kimutatta [85], hogy a kibermunkaerő megtartása a katonaságnál különösen nagy probléma, mivel minél több készségre és tapasztalatra tesznek szert ezek a kiberharcosok, annál piacképesebbek, és annál kevésbé valószínű, hogy a haderőn belül maradnak. A katonai kiberszakemberek világszerte elismert szabványok szerinti oktatásának és képzésének köszönhetően katonai szolgálati tapasztalataikat könnyen átültethetik a civil életbe. A lövészkatonákkal ellentétben például a kiberkatonák által az aktív szolgálat során megszerzett készségek olyan készségek, amelyek közvetlenül megfelelnek a civil munkakörnek, lehetővé téve a katonák számára, hogy könnyebben váltsanak át katonai szolgálatból jól fizető, versenyképes pályára.

Az Egyesült Államok Kiberparancsnokságának 2019-ben végzett belső felmérése szerint a három legfontosabb tényező, amely a hadsereg kiberszakembereit a hadseregben

maradásra ösztönözné, az, hogy (1) a műveletekre összpontosíthatnak az adminisztratív terhek nélkül, (2) több idő jutna a továbbképzésre, valamint (3) munkájukat jobban javadalmaznák és ismernék el. Ehhez kapcsolódott az a vágy, hogy világos és átlátható karrierpályájuk legyen. Emellett egyensúlyba kellene hozni a műveleten/gyakorlaton töltött időt az önfejlesztésre, továbbképzésre szánt idővel.

A kompenzáció és az elismerés szintén szerepet játszik: az elhagyók sok esetben jobban fizetett munkakörbe távoztak a magánszektorban. Ezenkívül a jól végzett munkát, az innovációt és a kutatást, valamint az új készségek megszerzésének elismerését általában bónuszokkal, díjakkal vagy fizetésemeléssel jutalmazzák a magánszektorban, amely opció általában nem érhető el a hadseregben az egyenlőségre törekvő humánerőforrás-korlátozások és a bónuszok korlátozott kapacitása miatt.

Végezetül, a válaszadók által körvonalazódó mögöttes aggály az autonómia. A katonai struktúra rugalmatlan, és hiába tekintenek hivatásként rá, a katonák több beleszólást szeretnének karrierjükbe és életükbe. A család stabilitása és életminősége minden katona számára fontos, de a kibermunkaerő számára ez jelentős tényezőként szerepelt a válaszadók azon döntésében, hogy elhagyják a katonaságot [86]. Ezen túl a hadsereg kulturális beállítottsága, miszerint a tiszteket elsősorban vezetőnek, másodsorban pedig műszaki szakértőnek tekinti, nehezíti az állomány megtartását. [87].

A 2022-ben megjelent könyvében Smeets [17] rávilágít egy olyan ellentmondásra, amely szerinte alapvetően kudarcra ítéli a kormányok kiberképesség-fejlesztését: ez a békeidőbeli haderő. Példaként a Holland Kiberparancsnokság esetét ismertette, amely egy korlátozott és erőforráshiányos szervezet, küldetését elsősorban háborús időkben látja el, békeidőben pedig potenciálisan elrettentő erőként működik, amely nem harcol, gyakorol nap mint nap. Emiatt a kiberparancsnokság háborúra való felkészülési képessége korlátozott.

„A szervezet nem végezhet felderítést külföldi hálózatokon, ami nemcsak megnehezíti a kellő időben történő potenciális célkiválasztást – ahogy a legtöbb fejlett művelet megköveteli –, hanem alapvető kapacitásvesztéshez is vezet. Ez az elsődleges kapacitásromlás egy formában jelentkezik: a tehetségek megtartásának és fejlesztésének képtelensége. A »polcon« heverő nukleáris robbanófejek (békeidőben) nem unatkoznak és távoznak. Amint azonban a PETIO[38]

[38] PETIO: people, exploits, toolset, infrastructure and organizational structure

keretrendszerből kiderül, a kiberkapacitás elsősorban az emberekről szól. Valószínűleg nem tartja meg a megfelelő embereket egy olyan kiberparancsnokság, amely gátolja a napi tevékenységet, és ahol a kiberszakértők nem érzik, hogy lehetőséget kapnak a folyamatos tanulásra és új készségek felhalmozására." [17:234–235]

A regionális összehasonlításokban a szlovák doktrínában találtam külön utalást erre az akadályra: „a közigazgatásban dolgozók oktatási és képzési koncepciójának kidolgozása, amelynek célja a toborzás, a fenntartás, a biztonság és a szakmai előmenetel, valamint szakmai kompetencia növelése és megtartása; valamint megfelelő motivációs és jutalmazási eszközök kialakítása a közigazgatásban dolgozó szakemberek számára a közigazgatás és a magánszféra viszonyainak egyensúlyba hozása érdekében" [77].

2.3.5 Logisztika – felszerelés (T)

A logisztika és a (köz)beszerzés egy végtelen felzárkózási játék. Ez egy időnként lassú folyamat, amelyet a költségvetés és a változó prioritások korlátoznak, illetve a jelenlegi és a várható igények vezérlik.

A hatékony hosszú távú beszerzési tervezés nehéz lehet, ha: 1) a jövőbeli fenyegetések és 2) az e veszélyek kezelésére szolgáló eszközök és készségek nagyrészt ismeretlenek. Ez a kibertérre kifejezetten igaz, ahol a technológiai fejlődés meghaladja a beszerzési ciklusokat.

A rövid távú akvizíciós stratégiákat a jelenlegi hiányosságok pótlására használják. Ennek célja az azonnali fenyegetések kezelése. A műveleti hatékonyság elérésének korábbi megközelítései nem tükrözték le a kiberhadviselés dinamizmusát vagy a lehetséges jövőbeni konfliktusok széles körét. Ez hosszabb távon is tervezési kihívásokat jelent a fenyegetések előrejelzésében, a műveletek tervezéséhez és a jövőbeli fenyegetések kezeléséhez szükséges eszközök azonosításában.

A kiberszervezetek számos beszerzési nehézséggel szembesülhetnek [88]:

- Korlátozott költségvetés: a kiberszervezetek költségvetése gyakran korlátozott, ami megnehezítheti a hálózataik hatékony védelméhez szükséges technológia és eszközök beszerzését.
- Korlátozott beszállítói lehetőségek: előfordulhat, hogy korlátozott számú szállító kínálja azt a technológiát vagy eszközt, amelyre egy kiberszervezetnek szüksége van. Ez megnehezítheti az igényeiknek legmegfelelőbb megtalálását.

- Összetett beszerzési folyamatok: a technológia és eszközök beszerzése összetett folyamat lehet, amely több lépésből és jóváhagyásból áll. Ez különösen nehéz lehet a kisebb kiberszervezetek számára, amelyek esetleg nem rendelkeznek elegendő erőforrással a beszerzési folyamatra.
- Szabványosítás hiánya: hiányozhat a szabványosítás a kiberbiztonsági ágazatban, ami megnehezítheti a szervezetek számára annak meghatározását, hogy mely termékek és szolgáltatások felelnek meg a legjobban az igényeiknek.
- Szakképzett személyzet hiánya: jelenleg hiány van képzett kiberbiztonsági szakemberekből, ami megnehezítheti a szervezetek számára a hálózataik hatékony védelméhez szükséges személyzet megtalálását és alkalmazását.
- Biztonsági aggályok: a kiberszervezeteknek biztonsági aggályai lehetnek bizonyos szállítókkal kapcsolatban a kínált technológiát és az eszközöket illetően .

2.3.6 Személyzet (P)

A kiberképességek sok esetben horizontálisak (szervezetileg), tehát egy adott területen ugyanaz a technikai szakértelem elvárható egy tiszttől, mint egy tiszthelyettestől. A rendfokozat és beosztás szétválasztása segíthetne. Ez a megkülönböztetés a legénység, az altiszt és a tisztek között akkor működik, ha a legénységtől elvárt munkakörök feladatalapúak, viszonylag alacsony képzettséget igényelnek, és rövid időn belül megtanulhatók. Akkor kezd szétesni ez a rendszer, amikor ugyanazok a munkák magas képzettséget igényelnek, és hosszú képzést vagy oktatást igényelnek.

A kibertér megkérdőjelezi a hadsereg hagyományos tiszti és legénységi megkülönböztetésének alapját képező valamennyi előfeltételt: ez egy olyan terület, amely magas szintű egyéni teljesítményt kíván meg a végrehajtás minden szintjén. A kibertér egy rendkívül technikai jellegű karrierterület is, amely évekig tartó – elsősorban tudományos jellegű – tanulást igényel az alapszintű szakértelem kialakításához. Az alap kiberszakember kiképzése legalább két év oktatást igényel, mielőtt képesítést szerezhet a metaforikus kiberfegyver elsütésére.

Ezek a strukturális gondok egy tágabb kulturális problémát tükröztek: a hadsereg intézményes idegenkedése a technikai szakértelemtől, a hierarchiához való merev ragaszkodással és a szabványos, könnyen helyettesíthető megoldások preferálásával természetesen nem kedvez a kiberrel kapcsolatos karrierterület fejlődésének. A hadsereg egyik volt tisztje és kibertisztje nyersen fogalmazott: „A hadsereg immunrendszere megöli a

kiberszakértőket.” [57:146] Az egyénre szabott megközelítés lehetővé tette a megfelelően magas színvonalú tehetségek azonosítását, de nem tette lehetővé az egységek számára, hogy ezeket a tehetségeket sokáig megtartsák, mivel a kiberfeladatok nem részei a hagyományos katonai vagy hírszerzői karriernek.

2.3.7 Infrastruktúra (I)

Számos infrastrukturális korlátot kell figyelembe venni a kiberparancsnokság felépítésénél:

- fizikai infrastruktúra: például irodaterületre, számítógépes szerverekre és hálózati berendezésekre van szükség;

- emberi erőforrások: a kiberparancsnoksághoz a küldetésének végrehajtásához szükséges készségekkel rendelkező, képzett személyzetre van szükség, beleértve a kiberbiztonsági szakértőket, elemzőket és támogató személyzetet;

- műszaki infrastruktúra: a kiberparancsnokság működésének támogatásához robusztus műszaki infrastruktúrára lesz szükség, beleértve a biztonságos hálózatokat, hardver- és szoftvereszközöket, valamint adattároló rendszereket;

- jogi és szabályozási keretek: a Kiberparancsnokságának a székhelye szerinti ország jogi és szabályozási keretein belül kell működnie, beleértve a magánélethez, adatvédelemhez és kiberbiztonsághoz kapcsolódó törvényeket és rendelkezéseket;

- finanszírozás: a kiberparancsnokság kiépítése és fenntartása költséges lehet, és a finanszírozás fontos szempont, mely magában foglalhatja a költségvetési előirányzatok állami vagy magánforrásokból történő biztosítását;

- együttműködés és partnerségek: a kiberparancsnokságnak küldetésének hatékony végrehajtása érdekében más kormányzati szervekkel, a magánszektorral és nemzetközi partnerekkel együtt kell működnie. Ezen együttműködések és partnerségek létrehozása és fenntartása bonyolult és időigényes lehet.

Doktrína	Szervezet	Vezetés	Logisztika	Oktatás	Személyzet	Létesítmények
Dinamikusan fejlődik	Meglévő egységek integrációja, kulturális különbségek	Nincs kialakított kiber karrierpálya, előmenetel	Gyorsan fejlődő technológia	Képességprioritás fontossága	Fizetés	A kialakítás költsége magas
				Folyamatos befektetés (költség)	Autonómia	
					Magas technikai tudás	
					Kiber pályamodell hiánya	

10.. ábra: összefoglaló táblázat az akadályok megszüntetését hátráltató tényezőket (saját szerkesztés).

A 8.sz. ábra foglalja össze az akadályok megszüntetése kapcsán a főbb pontokat. Doktrinálisan elmondható, hogy az dinamikusan fejlődik, egyre részletesebben ad iránymutatást. Gondot jelent, hogy a doktrinális követelményeket lekövetni idő- és forrásigényes, ugyanakkor nehéz megtalálni az egyensúlyt úgy, hogy a doktrinális háttér elég teret hagyjon a cselekvésre egy olyan környezetben, amely folyamatosan változik, és emellett maguk a részterületek, azok érdekei is átfedésben lehetnek (többek között honvédelem, rendvédelem, pénzmosás elleni küzdelem, adatvédelem, polgári kibervédelem).

A szervezeteket tekintve látható, hogy magával a kibertérrel több szervezet foglalkozik, ezen szervezeteknek a koordinációja szükséges feltétel. Katonai oldalon belül szintén szükséges a szoros együttműködés, arra vonatkozólag, hogy maguk a kiberparancsnokságok milyen funkcionális elemeket tartalmazzanak, illetve hogy maga a kiberparancsnokság hol helyezkedjen el a katonai szervezetek hierarchiájában. Erre több megoldás is van más országokban (honvédelmi miniszter alá közvetlen tartozó egység, például Lengyelország esetében, vagy a katonai hírszerzésbe integrálva). A kulturális különbségek a különböző szakterületek integrálása során tűnnek elő, és mivel egy alakulóban levő szervezetről van szó, az is sokat számíthat, hogy a kiberparancsnok maga milyen szervezeti háttérrel rendelkezik: különleges műveleti, esetleg katonai felderítő háttere van-e vagy elektronikai hadviselés területéről érkezett-e? A későbbiekben látható lesz, hogy a legtöbb részterületnek megvan a

maga szubkultúrája, azonban az is különlegessé teszi a kiberterületet katonai szempontból, hogy a kiberszakemberek sok szubkulturális elemet a civil szférából hoznak, hozhatnak.

A kiberműveletek tekintetében ennek az újdonságnak egy másik nehézsége az életpálya modell hiánya. Egyfelől jelenleg kevés lehetőség van a katonai akadémiákon "kiberszakirány"-ra menni, általában valamelyik testvér szakirányról történik a toborzás. Másfelől pedig a kiberműveletek - mint nem-kinetikus műveletek - nehezen illeszthető be a katonai előmeneteli rendszerbe: egy kiberműveleti százados saját szakterületén nem fog klasszikus értelembe vett csapatokat vezetni terepen, mint ahogyan kevés missziós feladat van kiber szakterületen. Emiatt félő, hogy az előmenetel lassul, ezáltal is erősítve az elvándorlást a privát szféra felé.

Logisztika szempontjából a beszerzések lassúsága okoz általános problémát. A technológia olyan gyorsan változik és olyan széles spektrumon kellene védekezni, hogy nehéz mindenre reagálni. Miután a kibertér egy kevéssé látványos terület, nem utolsó sorban az jelenti a sikert a védelem szempontjából, ha nincs incidens, nehezen látható a költségmegtérülés, viszont az alulfinanszírozásnak komoly kockázatai vannak. Komoly feladat biztosítani egy szervezetnek évről évre a továbbképzéseket, az új technológiák elérését olyankor, amikor a kinetikus oldalon a beszerzések sokszor egyszeriek és évekig használhatók, megfelelőek.

Ez a folyamatos befektetés jelenik meg a képzéseknél jelentkező akadályban. Ennek a kezelésére szükséges a képességek fontossági sorrendjének felállítása, annak tisztázása, hogy milyen irányba induljon el a fejlesztés, fejlődés. Ennek feltérképezéséhez szükség lehet a szervezet, terület kockázati felmérésére. A fenyegetésprofil (threat profile) létrehozása segít a szervezeteknek azonosítani a szervezetre fenyegetést jelentő a szereplőket, azok valószínű célpontjait és azt, hogy milyen típusú támadásokat fognak alkalmazni. A potenciális fenyegetések nyomon követésével a szervezetek alkalmasabbak lesznek a kockázatok kezelésére, és ez megalapozhatja a jövőbeni képességfejlesztést, illetve a szükséges költségvetést.

Az egyik általános kockázat, amely a szakirodalomban és a személyes szakmai beszélgetéseim is alátámasztanak, az a személyzet, a szakemberek felvétele és megtartása. Az anyagi különbségesen túl, amely a közszolgálat és a vállalati szféra között létezik, akadályozó tényező a korábban említett életpálya modell hiánya, illetve annak összeegyeztethetősége, hogy katonák és civilek együtt dolgozzanak. Az előremenetelnél, életpálya modellnél nehézséget jelent az is, hogy a kiber szakterületen szerepek, pozíciók vannak, speciális, általában szűk szaktudást igénylő részfeladatok. Ezen részfeladatokat megfelelő felkészítéssel és tudással elláthatja egy altiszt, tiszt vagy civil személy is, azonban a legtöbb katonai szervezetnél ezen kategóriák külön fizetési, előmeneteli besorolásban vannak. Ez a kiberszakterületre jellemző,

ún. horizontális munkavégzés (azaz minden szakértő egyenlő a maga szakterületét érintően) idegen a hierarchián alapuló katonai szervezetek számára. Ezekből az előzményekben következik az is, hogy egy kiberszakember hozzá van szokva a nagyfokú autonómiához, azaz ahhoz, hogy a saját területén belül maga járhasson el. Az előző fejezetben taglalt kibertér jellemzőkben láthattuk, hogy a kibertérben más az idő fogalma, ott gyakorlatilag azonnal keletkezhet egy incidens, és amennyiben elvárás, hogy a lehető leghamarabb reagálhasson rá egy szervezet, úgy annak meg kell lennie a megfelelő autonómiájának.

Az infrastruktúrát tekintve ismételten a költségekre szükséges utalni, hiszen akár egy létező létesítményben kerül kialakításra, akár egy új épület kerül felépítésre, mindkettő jelentős költséggel jár majd, az alap technikai feltételeken túl a célszoftverek licensz beszerzésein keresztül a rendszervédelemig mind jelentős anyagi terheket ró a védelmi költségvetésre.

Összegezve: az akadályok tekintetében láthatjuk, hogy a doktrínákban megjelenik az igény a kiberképesség-fejlesztésre, azonban számos területen akadályokkal kell megküzdeni. A következő alrészben bemutatott agilis projektmenedzsmenti elvek megoldási lehetőségek lehetnek egyfelől arra, hogy a személyzet autonómiáját és kreativitását fenntarthassa, másfelől, hogy a szervezet rugalmasan reagáljon a folyton változó kiberkönyezet kihívásaira. Ehhez természetesen idővel elengedhetetlen a finanszírozási rendszer szintén rugalmassá tétele.

2.4 Agilis módszertan – képességfejlesztés

2.4.1 Története

Az agilis menedzsment az *Agile* szoftverfejlesztés elveinek alkalmazása a különböző irányítási folyamatokban, különösen a termékfejlesztésben és a projektmenedzsmentben. Az Agilis Szoftverfejlesztési Kiáltvány 2001-es megjelenése [89] után az agilis technikák más tevékenységi területekre is kiterjedtek. Az Agilis módszertan fő értékei a következők:

- az egyének és a kölcsönhatások elsőbbsége a folyamatok és az eszközök felett;
- a működő szoftver elsőbbsége a széles körű dokumentációk felett;
- az ügyfél-együttműködés elsőbbsége a szerződés tárgyalása felett;
- rugalmas reagálás a változásra a terv vak követése helyett.

Az elsőbbség nem azt jelenti, hogy a „másik oldal” ne lenne fontos. A folyamatok és eszközök fontosak, de fontosabb a kompetens szakemberek hatékony együttműködése a siker érdekében. A dokumentáció nélkülözhetetlen, hogy érthető legyen a szoftver (termék)

működése, de a fejlesztés célja egy új termék (folyamat) létrehozása, nem a kutatás dokumentálása. A szerződés fontos, de nem válthatja ki a szoros együttműködést a „megrendelő”-vel, ami nélkülözhetetlen ahhoz, hogy megértsük, mire van pontosan szükségük. A projektterv fontos, de nem lehet túl merev, hiszen változhatnak az igények attól függően, hogy milyen megoldásokat találnak ők vagy javaslunk mi a problémára.

A Manifesztumban 12 alapelvet fogalmaztak meg [90]:

1. Ügyfél-elégedettség növelése az értékes szoftverek korai és folyamatos szállításával.
2. Üdvözöljük a követelmények megváltoztatását, még a fejlesztés késői szakaszában is.
3. Gyorsabban állítson elő és szállítson működő szoftvert (hónapok helyett heteken belül).
4. Szoros, napi együttműködés a helyi szakemberek és fejlesztők között.
5. A projektek motivált személyek köré épülnek, akikben megbíznak.
6. A személyes beszélgetés a legjobb kommunikációs forma (helyi közösség, kitelepülés).
7. A működő szoftver a fejlődés elsődleges mércéje.
8. Fenntartható fejlődés/fejlesztés követése, képes legyen állandó tempót tartani.
9. A termék műszaki kiválóságának fenntartása és a jó irányú tervezés/fejlesztés követése (design).
10. A termék lehető legegyszerűbb használatósága a sikerhez elengedhetetlen.
11. A legjobb architektúrák, követelmények és tervek önszerveződő csapatokból születnek.
12. A jó csapat rendszeresen átgondolja, hogyan válhat hatékonyabbá, és ehhez alkalmazkodva szervezi át magát és tevékenységét.

A legtöbb agilis módszer lebontja a feladatot kisebb részfeladatokra. Egy fejlesztési ciklus (sprint) általában 4 hétig tart. A sprintekben a csapattagok (ideálisan 3-9 fő) mindnyájan egy-egy szerepkört (terméktulajdonos, fejlesztő stb.) ölelnek fel, és a végén bemutatják az elkészült feladatokat a megrendelőnek. Ez teszi lehetővé, hogy a projekt gyorsan alkalmazkodjon. A módszer nagyobb hangsúlyt fektet a közvetlen kommunikációra, legyen szó jelenléti vagy online meetingekről. Minden csapatban van egy delegált a megrendelő részéről, ő a terméktulajdonos (product owner), és a fejlesztés egész ideje alatt rendelkezésre áll, hogy a felmerülő kérdéseket megválaszolja.

A fejlesztési módszerek skálája az adaptívtól a prediktívig terjed. Az agilis szoftverfejlesztési módszerek ennek a kontinuumnak az adaptív oldalán fekszenek, egyik kulcsuk az ütemezés tervezésének ún. „gördülő hullámú” megközelítése, amely azonosítja a mérföldköveket, de rugalmasságot hagy az eléréséhez vezető úton, és lehetővé teszi maguknak a mérföldköveknek a megváltoztatását is.

A módszer sikerességét három fő dimenzió határozza meg [59]: a projekt, a csapat és a kultúra. A projektet illetően fontos, hogy agilis környezetben azt célszerű kisebb, jobban kezelhető részfeladatokra bontani. Így a termék meghatározása és az ahhoz szükséges erőfeszítés becslése (28%), a gyakori változtatások (9%) és a termékelfogadás (6%) kritériumai voltak a projekttel kapcsolatos legfontosabb tényezők a sikerességhez. A csapat tekintetében az együttműködés fontos mozgatórugó, és a tanulmányok 15%-a döntő fontosságúnak találta a projekt sikere szempontjából. A csapattal kapcsolatos további sikertényező a munka elosztása (8%) és a csapat szakértelme (6%) volt. A szervezeti kultúra kapcsán a siker szempontjából a legfontosabb tényezőnek a vezetők megnyerését találták. A módszer sikerében kiemelték a munkavállalók képzését is.

2.4.2 Előnyei, hátrányai

Az adaptív módszerek a változó valósághoz való gyors alkalmazkodásra összpontosítanak. Amikor egy projekttel szembeni igények megváltoznak, a csapat is vele változik: nehezen tudja pontosan leírni, hogy mi fog történni a jövőben. Minél távolabb van egy dátum, annál homályosabb, hogy mi várható egy adott napon. Egy ilyen csapat nem tudja pontosan, hogy milyen feladatokat fog végrehajtani a jövő héten, csupán csak azt, hogy mely funkciók megvalósítását tervezi a következő hónapra. Ha egy hat hónap múlva megjelenő produktumról kérdezik, akkor csak a termék létrehozásának célját (mire lesz jó, az ún. mission statement) vagy a várható érték- és költségszámítást tudja megadni.

Ezzel szemben a prediktív módszerek a jövő részletes elemzésére és tervezésére összpontosítanak, és figyelembe veszik az ismert kockázatokat. Egy prediktív csapat pontosan tudja, hogy milyen funkciókat és feladatokat tervez a fejlesztési folyamat teljes időtartamára. A prediktív módszerek a hatékony korai fáziselemzésen alapulnak, és ha ez nem sikerül jól, akkor a projekt nehezen változtathatja meg az irányt. A prediktív csapatok gyakran változásvezérlő táblát hoznak létre annak biztosítására, hogy csak a legmeghatározóbb változtatásokat vegyék figyelembe.

Az agilis szoftverfejlesztés során a tesztelést a programozással azonos sprintben (párhuzamosan) végzik. Mivel a tesztelés minden sprintben megtörténik – ami a produktum egy kis részét fejleszti ki –, a felhasználók/fejlesztők gyakran használhatják ezeket az új produktumrészeket, és ellenőrizhetik az értékét, hasznosságát, használhatóságát. Miután a felhasználók/fejlesztők megismerik a frissített produktum valódi értékét, megalapozottabb döntéseket hozhatnak annak jövőjét illetően. Minden sprintben van egy visszatekintő értékelés és egy újra tervezés – a Scrum például általában mindössze kéthetes sprinteket szervez –, ez segít a csapatnak folyamatosan módosítani a terveit, hogy maximalizálja az általa nyújtott értéket. Ez a plan-do-check-act[39] (PDCA) ciklushoz [91] hasonló sémát követ.

2.4.3 Az agilis módszertan alkalmazása katonai szervezeteknél

Az interoperabilitás úgy definiálható, mint „a rendszerek, egységek vagy erők azon képessége, hogy szolgáltatásokat nyújtsanak más rendszereknek, egységek vagy erők számára, és szolgáltatásokat fogadjanak el azoktól, és az így kicserélt szolgáltatásokat használják annak érdekében, hogy hatékonyan működhessenek együtt” [92:1].

Az interoperabilitás létrejötte előtt álló első általános akadály az Egyesült Államok és Európa közötti szakadék a teljes védelmi beruházások, valamint a mesterséges intelligencia és a kapcsolódó technológiák civil technológiai teljesítménye tekintetében.

Az interoperabilitás másik akadálya, hogy a digitális technológiákat tekintve a gazdaság civil szektora az Atlanti-óceán mindkét partján fejlettebb, dinamikusabb, és nem is kifejezetten a katonai igények kielégítésére irányul.

Ez azzal jár, hogy a honvédelmi célra felhasználni kívánt digitális technológiák miatt a védelmi intézményekre sokkal nagyobb nyomás nehezedik arra vonatkozóan, hogy vagy alkalmazkodjanak a civil ipari termékekhez és szabványokhoz, vagy jelentős prémiumot fizessenek a beszállítóknak a katonai minőségű berendezések és szoftverek biztonságáért.

Az interoperabilitás harmadik akadálya az MI gyakorlati megvalósításában rejlik. Egy adott adatkörnyezetben testreszabott gépi tanulási algoritmus felállításához a szoftveripar legjobb gyakorlata az „agilis” fejlesztés valamilyen változata. Ez egy nagyon eltérő termékfejlesztési ciklust foglal magában, amely lényegében egy tökéletlen termék többszöri gyors iterációjával megy végbe, amelyet előzetes verziókban adtak ki, és később felülvizsgáltak – mint például a különféle „béta verziókban” kiadott szoftvertermékek – az idők során kifejlesztett frissítésekkel. Ez nagymértékben elüt a nagy katonai platformok hagyományos

[39] Tervezz-csinálj-ellenőrizd-cselekedj

gyártásával, amely minden fejlesztési lépésnél előtérbe helyezi a szigorú minőség-ellenőrzést és a követelményeknek való megfelelést – ezt a megközelítést a szoftveripar „vízesés" fejlesztésnek nevezi. Az agilis termékfejlesztés kihívások elé állíthatja az interoperabilitást. Hacsak nem alkalmaznak nagyon szigorú szabványokat, jelentős a kockázata annak, hogy a különböző nemzeti intézmények eltérő módon járnak el egy adott mesterséges intelligencia vagy adatelemzési probléma megoldásában.

A nagy hagyományos katonai platformok esetében hosszú időkeretek állnak rendelkezésre, amelyek során az államok koordinációs lépéseket tehetnek, akár ugyanazon platformok megvásárlásával, akár konszenzus kialakításával a követelmények és szabványok tekintetében. Ha azonban egy viszonylag kis csapat dinamikusan dolgozik azon, hogy hetek vagy hónapok alatt algoritmikus megoldást generáljon egy adott problémára, a meglévő konzultációs mechanizmusokon keresztül történő hagyományos koordináció kockázatot jelenthet az agilis fejlesztésben rejlő sebességelőny szempontjából. Ezzel szemben, ha egy megoldást már kidolgoztak, annak némileg eltérő környezetekben történő alkalmazása számos technikai ok miatt kihívást jelenthet.

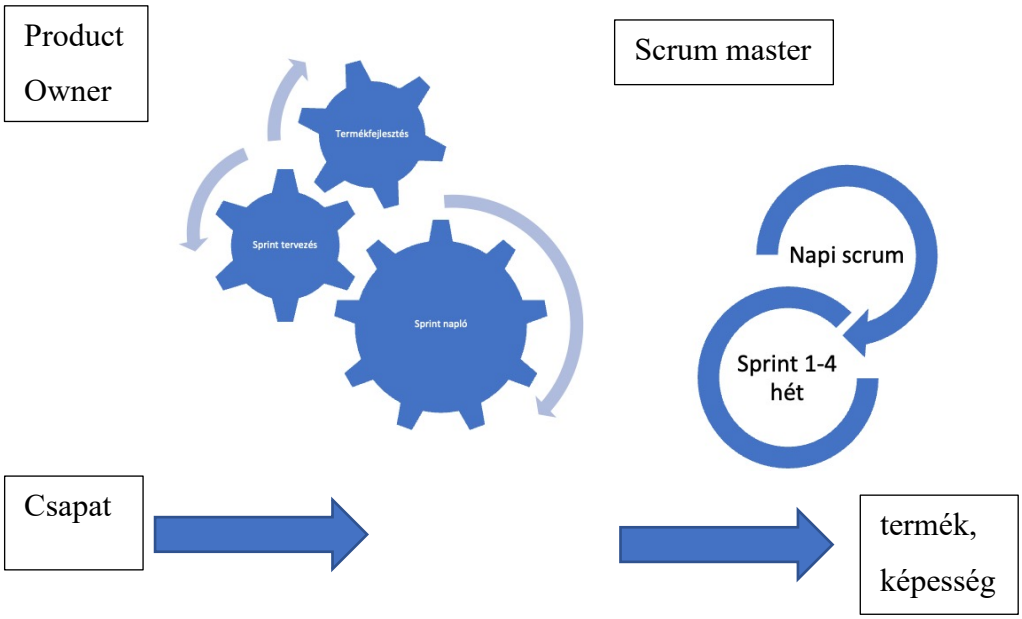
A mesterséges intelligencia esetében jellemző megfigyelés, hogy számos védelmi intézményben számos kiváló prototípus és pilotprojekt létezik, de komoly kiemelkedő kihívások is vannak a vállalati szintű megoldásokra való felskálázásban, nem beszélve a szövetségi szintű megoldásokról.

Az alábbi 9. ábra bemutatja egy agilis projektmenedzsment alapfolyamatait. A megrendelő igényei a képességfejlesztési igények. A PO (Product Owner[40]) maga a kiberparancsnokság, a Csapat áll a projektmenedzserből, a külsős értékesítési kapcsolattartóból (amennyiben külsős, piaci szereplő is jelen van), a parancsnokság által kijelölt személyből és a fejlesztőkből. A munkát 1–4 hetes sprintekre osztják szét, amelyet a Scrum Master[41] fog össze, gyakorlatilag naponta ellenőrizve az előhaladást, illetve kezeli a felmerülő problémákat. A

[40] Magyarul termékgazda a szó szerinti fordítás, de a hazai szakirodalomban is a PO az elterjedtebb. Felfogható egyfajta megrendelőnek is, hiszen a PO általában nem IT szakember, hanem a készülő rendszer legfőbb felhasználója, aki pontosan érti a majdani felhasználók igényeit, a piac jelenlegi helyzetét, a versenytársakat, illetve a jövőbeli trendeket.

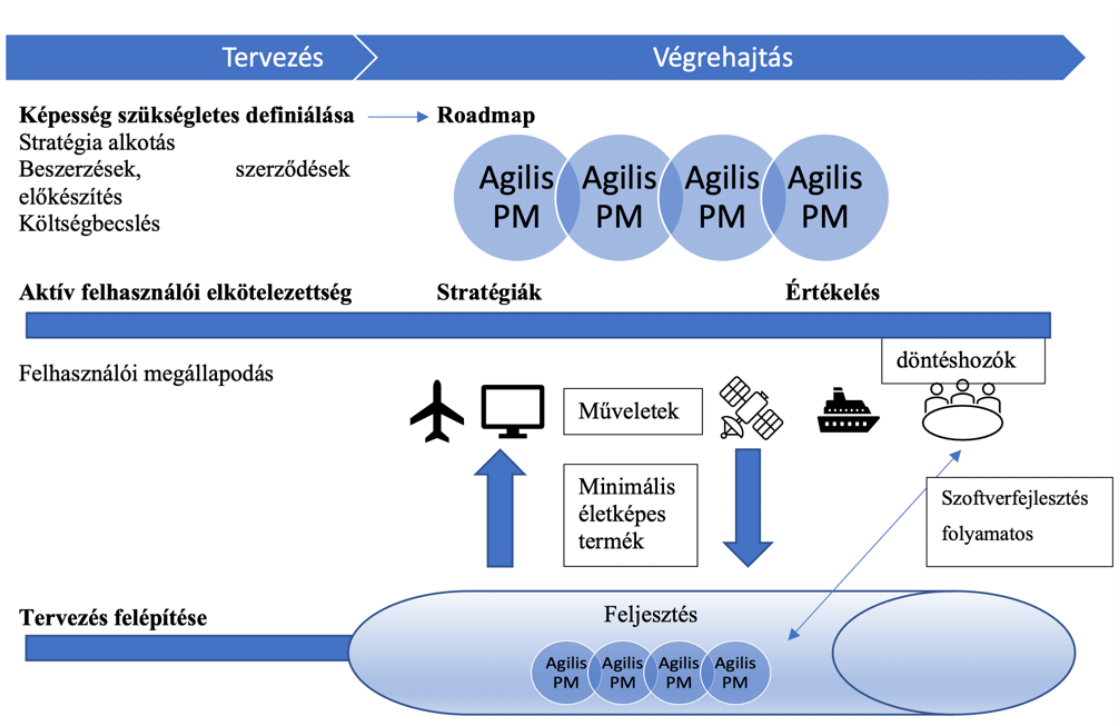
[41] Konkrét feladatai közé tartozik, hogy megszervezze és vezesse a különböző scrumos szeánszokat, motivál, segédkezik a riportálásban, monitorozza a sprint előrehaladását és cselekszik, ha valamilyen akadályt el kell hárítani. Legfőképpen ő a "ragasztó", aki összetartja a csapatot.

sprint végén van egy átbeszélés, a kész terméket értékelik, és az eredmények függvényében egy újabb sprint kezdődhet, tovább finomítva a képességet.



11. ábra: az agilis módszertan leírása [93] (fordítás)

A fentiekben felvázolt agilis módszertan a hadsereg igényeivel integrálva mutatja be a következő ábra.



12. ábra. Az agilis módszertan integrálva a haderő tervezési folyamatába [93]

A haderő tervezési folyamatba integrálva két nagy fázisra oszlik: a tervezési és kivitelezési (végrehajtás) fázis. A tervezési fázisban történik a képességigények felmérése, illetve többek között a közbeszerzések kiírása, a szerződések előkészítése és a költségbecslés. A végrehajtás fázisában több iterációs sprint megy végre a képességfejlesztésben, folyamatos visszacsatolással a műveletekről (minimum követelmények, illetve a minimumképességek tekintetében).

Az agilis módszereket úgy alakították ki, hogy rugalmasak és reagáljanak a változásokra, ami különösen hasznos lehet a hadseregben, ahol a helyzetek gyorsan változhatnak.

Az eredeti agilis módszertan manifesztója lefordítva egy katonai szervezet képességfejlesztési igényeire az alábbiak szerint módosul:

1. A szervezet céljainak elősegítése a képességfejlesztés korai és folyamatos szállításával.
2. Elfogadjuk a követelmények megváltoztatását, még a fejlesztés késői szakaszában is.
3. Gyorsabb képesség megjelenés a gyakorlatokon (hónapok helyett heteken belül).
4. Szoros, napi együttműködés a szakemberek között (alakulatok között, szervezetek között).
5. A projektek motivált személyek köré épülnek, akikben megbíznak.
6. A személyes beszélgetés a legjobb kommunikációs forma (helyi közösség, kitelepülés, projekt elkülönülés más napi feladatoktól).
7. A bevethető képesség a fejlődés elsődleges mércéje.
8. Fenntartható fejlődés/fejlesztés követése, képes legyen állandó tempót tartani.
9. A képesség műszaki kiválóságának (minőségének) fenntartása és a jó irányú tervezése/fejlesztése.
10. A felhasználható képességek olyanok legyenek, amelyek átadhatóak.
11. A legjobb architektúrák, követelmények és tervek önszerveződő csapatokból születnek.
12. A jó csapat rendszeresen átgondolja, hogyan válhat hatékonyabbá, és ehhez alkalmazkodva szervezi át magát és tevékenységét.

Úgy vélem, hogy az agilis módszertan effajta kreatív önállósága lehetővé teszi a kiberképességfejlesztés megvalósítását katonai környezetben is a megfelelő körülmények biztosításával. Javaslom, hogy egy-egy gyakorlat tapasztalatfeldolgozásából kiindulva (milyen

képesség hiányzik), a lehetőségeket felmérve (eszköz állomány, szakember állomány, leterheltség) ki lehet olyan képességeket választani, amelyben előrehaladást lehetséges elérni rövid időn belül, akár az agilis projektmenedzsment által javasolt 4-12 hetes sprintjei alatt is. Azonban ehhez szükséges egy kiszámítható munkakörnyezet biztosítása, és az egyéb feladatok alóli tehermentesítés az adott időszakra.

Az agilis módszertan katonai használatának néhány lehetséges előnye a következők lehetnek:

- továbbfejlesztett együttműködés: az agilis módszertan elősegíti a csapattagok közötti együttműködést és kommunikációt, ami fontos lehet a hadseregben, ahol a csapatoknak gyakran kihívásokkal teli körülmények között kell együtt dolgozniuk;
- fokozott alkalmazkodóképesség: az agilis módszertanok lehetővé teszik a csapatok számára, hogy gyorsan alkalmazkodjanak a változó körülményekhez, ami fontos lehet a hadseregben, ahol a helyzet gyorsan változhat;
- fokozott agilitás: az agilis módszertanok hangsúlyozzák a rugalmasság és a gyors elfordulás fontosságát, ami hasznos lehet a hadseregben, ahol a csapatoknak váratlan kihívásokra kell reagálniuk;
- fokozott elszámoltathatóság: az agilis módszertanok nagy hangsúlyt fektetnek az egyéni elszámoltathatóságra, ami fontos lehet a hadseregben, ahol a teljesítmény és az elszámoltathatóság kritikus fontosságú;
- továbbfejlesztett döntéshozatal: az agilis módszerek gyors és hatékony döntéshozatalra ösztönzik a csapatokat, ami fontos lehet a hadseregben, ahol a döntéseket nagyon stresszes, időérzékeny környezetben kell meghozni.

Összességében az agilis módszertan segítheti a katonai alakulatok hatékonyabb és eredményesebb munkáját, különösen olyan helyzetekben, amikor a környezet folyamatosan változik – például a kibertérben.

2.5 Összegzés, rész-következtetések

A második hipotézisem az volt, hogy az akadályok megszüntetése szempontjából eltérő rendszerek alakulnak ki a V4-es tagországok és Németország esetében. Ez a hipotézisem hamisnak bizonyult. Egyfelől mert az általános akadályozó tényezők a nemzetállamok tekintetében hasonlónak bizonyultak: jogi keretrendszerek (elsősorban offenzív képességek

területén), nem-kinetikus elemek integrációja, kiberszakemberek megtartásának nehézsége. A kiberképességek összemérésére a DOTMLPF-modellt alkalmaztam, amely részleges eredményt hozott. A kiberképesség-fejlesztés felmérése nyílt forrásokból korlátozott lehetőséget biztosított. Tehát egyfelől feltételezhető, hogy nincsenek jelentős eltérések a vizsgált tagállamok között (már ami a képességfejlesztés akadályait illeti), másfelől nem áll teljes kép rendelkezésre a képességfejlesztésüket tekintve. Az agilis módszertant ismertettem, és meglátásom szerint alkalmas arra, hogy a hadseregen belül alkalmazásra kerüljön.

A fejezetben a keretrendszer alapján bemutattam a főbb akadályozó tényezőket a kiberképesség-fejlesztés körül, és egy lehetséges megoldásként az agilis módszertan alkalmazásának lehetőségét.

Jelen fejezet a [94] a publikációmat dolgozta fel és egészítette ki a DOTMLP-keretrendszerrel.

3. A kiberműveletek fejlődésének összehasonlítása a légierő kialakulásával

„Mi vagyunk a történelem középső gyermekei: túl későn születünk ahhoz, hogy felfedezzük a Földet, túl korán születettünk ahhoz, hogy felfedezzük az űrt, épp időben, hogy felfedezzük a kiberteret."[42]

3.1 Bevezetés

A hadviselés története során rendszeresen jelentek meg új fegyverek és technikák. Döntő többségük fokozatosan tűnt fel, azaz több év telt el az adott fegyver vagy technika széles körű elterjedéséig, és ezek a huszadik századig a szárazföldi vagy tengeri (hadviselési) dimenziót érintették. A huszadik század hajnalán merészkedett az ember a harmadik dimenzióba, a levegőbe. Ez egy olyan, mai szóval élve diszruptív[43] folyamat volt, amely feltűnően rövid idő alatt gyökeresen megváltoztatta a hadviselést.

A légierő megjelenésével és térnyerésével egyidejűleg jelent meg a vezeték nélküli hálózatok rendszere, amelynek akkoriban elsődleges feladata a kommunikáció javítása volt, és kevésbé bolygatta fel a hadviselési alapelveket, mint a harmadik dimenzió megnyitása. Azonban a huszonegyedik századra ezek a vezeték nélküli hálózatok a kiberdomén birodalma lett – a negyedik dimenzió[44]. Ez a dimenzió minden más dimenziónál jobban átszövi a mindennapjainkat, sebessége lélegzetelállító, és a légierőhöz hasonlóan egy új, feltáratlan és diszruptív dimenziója a hadviselésnek. A kiberteret sok szempontból nem a technológiák teszik különlegessé, hanem az a több milliárd ember, aki használja, és életünk – annak társadalmi, politikai, gazdasági, katonai részei – része [95:62]. Ahogyan a huszadik század elején a légi domén egyedi képességei köré kiépült egy intézményrendszer, úgy a (katonai) kibererőknek is a kiberterület köré kell felépülniük. Azonban a légi doménnel ellentétben, a kibertérben sokkal nehezebb különválasztani a katonai és a civil entitásokat.

[42] Ismeretlen szerző, James Clear író által idézett: "We are the middle children of history. Born too late to explore earth, born too early to explore space, just in time to explore cyberspace"
[43] A szó eredeti jelentésében bomlasztó, kártékony jelentéssel bír, azonban az elmúlt évtizedben az irodalomban megjelent egy új formában is, ún. diszruptív technológiaként. Ezek a saját területükön forradalmasítják a rendszereket, gyakran egyszerűbbek, gyorsabbak vagy olcsóbbak mint a korábban alkalmazott megoldások.
[44] Az öt műveletidimenzió, domén a következő: szárazföld, tenger, légtér, kiber és űr.

Sarah P. White disszertációjában [57] feldolgozta azon kulturális különbségeket, amelyek a katonai innovációt érintik az Egyesült Államok különböző haderőnemeiben. Az ő disszertációja mentén hasonlítom össze a légierő és a kibertér fejlődéseinek párhuzamait. Először a stratégiai hátteret mutatom be, azt követően a hasonlóságokat, majd az eltéréseket a két domén között, végezetül pedig a helyzetkép adta technikai fejlődés lehetőségeit.

A harmadik fejezetben azt a kérdést jártam körbe, hogy **hogyan lehetne egy ilyen technikai, nem-kinetikus domént közelíteni a kinetikus doménhez**. Ehhez a légierő történetét vettem alapul, illetve annak helyzetképfejlesztését, amely megjelent a kibertérben is. A kiberhelyzetkép egy olyan lehetőség, amely láthatóvá tenné a kiberteret, és ezáltal – ahogyan a légierőnél is történt – elősegítené és gyorsítaná a döntéshozatalt.

A kutatáshoz a légierő-elméletet, és azok használhatóságát – illetve annak korlátait – kutattam a kibertérben. Emellett több szakmai beszélgetést folytattam a kiberhelyzetkép összetevőiről, a kiberképesség-fejlesztés akadályairól.

A fejezetet a szokásos irodalmi áttekintéssel kezdem, majd két nagyobb részre osztom: a kiberdomén és a légi domén összehasonlítása (3.3. fejezet), valamint a helyzetkép (3.4.) bemutatásával.

3.2 Kapcsolódó szakirodalmi áttekintés

3.2.1 Légierő teoretikusok használhatósága

A fejlődő haderőnemet érintően a stratégiai elméletek közül az egyik legbefolyásosabbat Giulio Douhet olasz stratéga alkotta meg, egyidőben a brit Hugh Trenchard-dal: a stratégiai bombázás fontosságára és a repülőgépre, mint alapvetően támadó fegyverre, és ezáltal a légi uralmat biztosító eszközként való definiálásra épült. Douhet meglátása szerint a győzelem a háborúban attól függ, hogy valaki képes-e elérni a légi uralmat. Ebből indultak ki a korai légierő alapvető elméleti tételei: a légierő a háború döntő eszközévé vált; hogy a légierő hatékony felhasználása légi fölényt igényelt; és hogy a légi fölény eléréséhez a légierő központosított irányítására volt szükség egy intézményesített és nagyrészt autonóm légierő révén. Az elméleti keretek meglétével a következő probléma a légi fölény elérésének meghatározása volt.

A két világháború közötti időszakban Douhet és Trenchard határozottan támogatták a repülőgépek támadó jellegű használatát a harcban. A hadsereg kötelékében rekedt légierő számára a stratégiai bombázás kínálta a legnagyobb ígéretet a teljes intézményi autonómia biztosítására. Míg a hadsereg igényt tartott a közeli légi támogatási küldetések biztosítására, valamint a hadsereg és a haditengerészet is tudta igazolni a repülőgépek hírszerzési, felderítési és kommunikációs célú felhasználását, a stratégiai bombázás logikailag nem illett bele semelyik haderőnem küldetései közé. Ez, valamint az, hogy a stratégiai bombázás doktrína kimondta, hogy a sikeres stratégiai bombázás végrehajtásához függetlenség kell a szárazföldi parancsnokoktól, tette lehetővé a függetlenedést.

Az Egyesült Államok légierejének felfogása önmagáról és a honvédelemben betöltött szerepéről nagyjából változatlan maradt a hidegháború óta, és ma ezt a küldetést a „globális csapás, globális hatókör, globális jövőkép" mottója bizonyítja. A légierőnek ez a globális csapásmérő küldetése a légi dimenzió végtelenségével kialakított egy sajátos gondolkodásmódot. Ezt a légiszemléletet úgy írják le, mint „olyan globális, stratégiai gondolkodásmódot, amely perspektívát nyújt, és amelyen keresztül a harcteret nem korlátozza a földrajzi helyzet, a távolság, a hely vagy az idő". A repülősök számára az ellenséges erők megsemmisítése és a terület irányítása – a leghagyományosabb mérési módszere a katonai sikernek – csak két lehetőséget jelent a rendelkezésre álló műveletek spektrumában. Ez a fajta gondolkodásmód nagyon hasonló ahhoz az eltérő szemléletmódhoz, amely a kiberteret jellemzi, egy olyan extra réteggel együtt, amelyet az attribúciós nehézségek adnak, amely a kiberperszónához is köthető, hiszen amíg a repülőgépek és fegyverzeteik beazonosíthatóak, addig a kibertérben lévő „fegyverek" és „végrehajtók" már nehezebben. Ezen különbségek a dimenziók közötti különbségekhez kapcsolódnak, amelyet korábban részletesen kifejtettem.

Ebből a rövid áttekintésből több következtetés is levonható a légierő kultúrájáról: először is a léte függ attól, hogy milyen technológiával rendelkezik, mennyire tud innovatív lenni és mennyire képes befogadni a technológiai változásokat. Másodszor a légierő stratégiai hatások létrehozásában gondolkodik, amit úgy érnek el, hogy olyan ellenséges súlypontokat vesznek célba, amelyek más haderőnemek hatókörén kívül esnek.

Szervezetileg az is hibának bizonyult, hogy alárendelt szervezetként létezett a szárazföldi és tengeri haderőnemek alatt, azonban a vezetés és irányítás teljes függetlenedése is tévútnak bizonyult. Végül az összhaderőnemi parancsnokságba szervezés oldotta fel a problémát. Ehhez kapcsolódó kérdéskör volt annak eldöntése, hogy egy parancsnokság

funkcionális vagy földrajz fókuszú legyen. A földrajzi parancsnokságok egyértelműen meghatározott (földrajzi) felelősségi területen működnek, és regionális fókuszúak. A funkcionális parancsnokságok földrajzi határok nélkül működnek, és egyedülálló képességeket biztosítanak küldetések és missziók támogatására. Funkcionális parancsnokság általánosságban a különleges műveleti parancsnokság, továbbá a kiberparancsnokságokat is ide szokás sorolni.

3.2.2 Munkahelyi kultúra

Egy szervezet kultúrája döntő hatással lehet az innováció folyamatára [57:2]. A hagyományos katonai innováció kutatói számos magyarázatot kínáltak az eltérő innovációs eredményekre. Ezeket nagy vonalakban fel lehet osztani a következő elméletekre. A szervezetelmélet azt állítja, hogy a hadsereg változással szembeni ellenállása olyan strukturális tényezők eredménye, amelyek az intézményi viselkedést alakítják. Egy szervezet viselkedése kevésbé a választás, mint inkább az eljárások eredménye [96:2–11]. A szervezeten belüli változás tehát külső katalizátort követel meg, amelynek három fajtáját különböztetik meg: külső nyomás, túlélési igény vagy kudarc. E katalizátorok fontossága vita tárgyát képezi a tudósok között. Barry Posen például azzal érvel, hogy ez a külső nyomás gyakran a civil vezető megjelenési formáját ölti, amely a stratégiai környezet jobb megértése alapján kívülről kényszeríti a változást [97:233]. Stephen Rosen viszont azt állítja, hogy ez a katonai vezetőkre igaz, akik belülről kényszerítik ki a változást a személyi előmeneteli lehetőségek szándékos kiigazításával [98:3]. Thomas Mahnken pedig úgy véli, hogy az ellenségről szóló hírszerzési információ a legfontosabb motiváló erő a katonai innováció mögött [99].

Szemben a szervezetelmélet strukturális magyarázatával, a folyamatvezérelt bürokratikus politikai modell szerint a katonai vezetőket alapvetően az az igény motiválja, hogy előmozdítsák szervezetük fontosságát, miközben megőrzik azt, amit Morton Halperin híresen „szervezeti lényegüknek” nevezett [100]. A belső rivalizálás és a szervezet presztízsének mérése tehát a szervezeti magatartás és döntéshozatal elsődleges befolyásolóinak tekinthetők. A bürokratikus politikai modell alapján a szervezet elutasít minden olyan új innovációt, amely megkérdőjelezi annak lényegét vagy az erőforrásokhoz való hozzáférését [57:16]. Végül a szervezeti kultúra elméletei – amelyek magukban foglalják a szervezeti lényeg, az intézményi memória és a szervezeti személyiség egymást átfedő fogalmait –, a tapasztalat, a kultúra és a tanulás közötti iteratív kapcsolatot sugallják, amely meghatározza, hogy „a szervezetek milyen hatékonyan tanulhatnak saját tapasztalataikból” [101:6]. Ezek a közös hiedelmek általában a szervezetformáló tapasztalataiból fakadnak, és az idő múlásával a sikeres gyakorlatok erősítik meg őket. A megerősítést követően a kultúra meghatározza, hogy a szervezet hogyan reagál a

kihívásokra, lehetőségekre és korlátokra azáltal, hogy egy sor heurisztikát biztosít az új információk értékeléséhez [102:16].

Terry Pierce egy további meggyőző választ ad arra a kérdésre, hogy mi különbözteti meg a tartós és múlandó innovációt. Azzal érvel, hogy az innováció tartósságának leghatékonyabb garantálási módja az, ha azt a szervezet meglévő nyelvén és kultúráján szólaltatja meg [103:31]. Ezen elv alkalmazása látható a hadsereg hagyományos manőver-terminológiájában, a kiberdoktrinális fogalmak leírásában.

3.2.3 Helyzetképismeret

A helyzetfelismerés[45] úgy definiálható, mint a környezetben lévő entitások megismerése, jelentésük megértése és állapotuk kivetítése a közeljövőbe. A légierő szemszögéből az SA arra a képességre utal, hogy előrevetíti az ellenséges és baráti repülőgépek jelenlegi és jövőbeni elhelyezkedését, valamint megjeleníti a fenyegetéseket egy képben, térben. Endsley SA-modelljét széles körben alkalmazták, amely három különböző szintből áll: észlelés, megértés és előrevetítés. Az SA különösen fontos a hadsereg és a légierő számára, a katonai vezetés és irányítás (C2) szerves része.

A kiberhelyzetkép a kibertér összefüggésében a harctér elemeinek észlelésének, kivetítésének képességét írja le. A parancsnokoknak tisztában kell lenniük a kiberhelyzetképpel, hogy megalapozott döntéseket hozzanak a kibertérben való eredményes tevékenység, a küldetés céljainak támogatása érdekében történő kiberhatások kiváltásával.

3.3 A légi domén és a kiber domén összehasonlítása

3.3.1 Történet

Ahhoz azonban, hogy ezek a törekvések megvalósuljanak, a kibertéri műveleteknek kettős függetlenséget kell nyerniük: először is a hírszerző közösségtől, amelyből sok esetben kinőtték magukat, másodsorban pedig minden olyan indokolatlan (kulturális) befolyástól, amely korlátozná a kibertérben folytatott harc egyértelmű víziójának kialakítását. A légierőnél megvalosuló szervezeti átalakítások a 2000-es években négy főbb feladatot szabtak meg a kibererőket illetően: (1) lehetővé tenni a kibertéri műveleteinek összehangoltabb alkalmazását, és teljesen integrálni őket a légi és űrműveletekkel; (2) képzett és kész erőket biztosítani „az elektromágneses spektrumon keresztül történő tartós támadó és védekező műveletek

[45] Situational Awareness, SA

végrehajtására"; (3) 24 órában működő légi műveleti központ[46] működtetése a parancsnokság által végrehajtott összes kinetikus és nem-kinetikus tevékenység irányítására, valamint a kapcsolódó taktikák kidolgozása a képességek ilyen széles spektrumának kezelésére; (4) hosszú távú terv kidolgozása a kiberparancsnokság és egy kiberkarrier-menedzsment fejlesztésére [57:218].

Fontos kulturális különbség a kockázatok különbözősége a kibertérben. A kockázat az időhöz kapcsolódik, mind a védekezésnél, mind a támadásnál van egy relevanciaablak. Ez lehet például a sebezhetőség felfedezése, a sérülékenység kihasználása és a biztonsági javítás között eltelt idő. Más szavakkal, a kiberfegyver hatékonysága jellemzően fordítottan arányos azzal az idővel, ameddig az adott fegyver használható. Az ebből eredő versenyhelyzet ellentétes a fegyverfejlesztés működésével a fizikai világban, amelyben a képesség objektív romboló képessége általában nem csökken az idő múlásával [57:230].

A legtöbb nemzeti stratégia a kiberbiztonságra összpontosít, nem az offenzív kiberműveletekre, és ez problémákat okozhat a kibererők megszervezése során. Átfogó offenzív kiberstratégia hiányában például az Egyesült Államok Légiereje egyszerűen a saját elveit alkalmazta a kibertérre. Azonban – ahogyan korábban röviden említettem – a légierő és a kibererő eltérő megközelítést igényelnek, mivel a kiberfegyverek alkalmazása eltér a többi fegyver alkalmazásától (idő, kockázat, hatás) [104:22]. Mivel nehéz felmérni egy-egy kiberművelet konkrét hatásait, a parancsnokok általában vonakodnak a használatuktól, ezért túlnyomórészt a szárazföldi, légi és tengeri kommunikációs képességek biztosítására összpontosítják a kiberképességeket, annak teljes műveleti spektruma helyett [104:23].

Ma a hadviselés egy olyan átalakuló időszakban van, amikor annak információs része felértékelődik, és a hadviselésnek háborús szint alatti, tartós nem-béke állapotára adott katonai válaszok nem tisztázottak vagy egyszerűek. Az információs hadviselés sokrétű stratégiák kombinációja, amelyek célja az ellenfél információs infrastruktúrájának rombolása.[47] A kiberműveletek (legyenek azok offenzívek vagy defenzívek) integrálása a hagyományos

[46] Air Operations Center, AOC

[47] Részletesebben: *„the integrated employment of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own."* [105:28]

(kinetikus)[48] katonai műveletekbe több szempontból nehézséget okoz, de elengedhetetlen ahhoz, hogy – akár a műveleti területen, akár a hátországban – egy adott ország megtartsa az információs fölényét.

Az információs fölény hagyományos megközelítésben „a klasszikus katonai műveletekben értelmezhető, ahol az egymással szemben álló felek között az infokommunikációs technológiai képességbeli különbségeknek komoly jelentősége van. Ebből kifolyólag e megközelítés alapvetően technológia-központú, és az információgyűjtés, -tárolás, -feldolgozás és -továbbítás hatékonyságára összpontosít" [7:162].

Az új környezethez való alkalmazkodás hiánya válság idején stratégiai meglepést okozhat és mozgásképtelenséghez vezethet, ahogyan történt az Egyesült Államok légierejével Pearl Harbornál. A számos figyelmeztetés ellenére a hadsereg és a haditengerészet figyelmen kívül hagyta vagy minimálisra értékelte a légi fenyegetés hatásait. A támadást túlélő katonák és tengerészek beszámolói hitetlenséget tükröztek afelől, hogy egy légi támadás ilyen megdöbbentő hatást tud elérni [7:33]. Az Egyesült Államok nem volt egyedül a légierő által okozott csapások alulértékelésében, sok más ország is csak azután szervezte át hadseregét, miután hasonló kudarcokkal szembesültek. A kibertérben is hasonló ráeszmélés zajlott lett a kétezres évek elején, többek között az észtországi események után.[49]

A kiberhadviselésnek nem kell célul tűznie, hogy felülmúlja a hagyományos kinetikus erőket, miután a kiberműveletek rendkívül kicsi része az, amelyik kinetikus hatás kiváltására irányul, és talán ez a legkevésbé értékes a műveletet indító ország számára. A kibertéri műveletek célkeresztjében a megtévesztés van, azonban ez a gondolkodásmód gyakran csak a célpontok eléréséig terjed, nem pedig az információs hadviselés teljességére. A kibertér kevésbé a közvetlen konfliktusról szól, de nagyban befolyásolhatja a hagyományos haderőnemek hatékonyságát. A kiberműveletek révén megzavarhatják az ellenség helyzetfelismerését és logisztikai láncait, vagy kétséget, zavart kelthetnek az ellenséges döntéshozatali folyamatokban. A korábban említett információs fölény megszerzésének és megtartásának három oldala van (hagyományos értelmezés szerint): az információszerzés a

[48] Kinetikus erők vagy hatások a mozgási energia fizikai (robbanás, lővészet) hatásaira fókuszálnak az ellenséges erők rombolásának céljából.
[49] A „kiberháborúk" első mérföldköveként a 2007-es észtországi feltételezett orosz támadást jelölik meg. Ekkor túlterheléses támadás érte például az észt kormányzati, banki és médiaszektor hálózatait [106].

parancsnoki döntést befolyásoló tényezőkről, a saját információs képességek kihasználása és védelme; valamint a másik fél információs képességeinek akadályozása" [7:163]. Ha a szemben álló hagyományos kinetikus erőket bokszolókhoz hasonlítjuk, akkor a kiberhadviselésnek nem az ütésben lesz jelentősége, hanem abban, hogy megváltoztatja a bokszolók képességeit és felfogását, vagy akár magának a boxringnek a körülményeit.

Megkérdőjelezhető, hogy a fizikai alapú kinetikus gondolkodásmód megfelelő lesz-e az információs műveletek összefüggéseinek megértéséhez a kívánt kiberhatások elérése érdekében. A „kibergondolkodás" információalapú tartományra épül, és mint ahogyan szorosan kapcsolódik a technológiai ágakhoz (híradó, elektronikai hadviselés), úgy a felderítéshez is. A kiberműveletek azonban nem elválaszthatók az összhaderőnemi gondolkodástól [95:41], ahogyan a funkcióalapú parancsnokságok többi eleme sem. A kiberdoménnek azonban van egy nehezítő körülménye: az egyben funkció és tartomány is. Egy olyan tartomány, amely keresztülszövi a többi négy tartományt is. Ezt az álláspontot támasztja alá Martin Libicki, aki szerint az elmúlt néhány évtized technológiai és szervezeti innovációi megteremtették a „nem nyilvánvaló háborúskodás" lehetőségét [95:64], mint amilyen a kiberhadviselés is. A kiberhadviselés többet jelent, mint általában a hackerek által megtámadott rendszerek összessége. A kibererők nemcsak a hadviselést befolyásolhatják a kibertérben, hanem a képességeket is a háború minden területén.

3.3.2 Hasonlóságok

Ahogyan a légi hadviselésben bizonyos jellemzők előnyt jelentenek, például a vadászrepülőgépeknél a jó manőverező képesség elengedhetetlen, vagy a nehéz rakomány szállításának képessége a bombázók fontos jellemzője. Hasonlóképpen, a kiberhadviselésben bizonyos jellemzők előnyt jelentenek, ilyenek a túlélőképesség, a feldolgozási teljesítmény és a manőverezhetőség.

Túlélőképesség

A túlélőképesség a hadviselés minden formájában értékes jellemző. A kiberterületen számos tényező határozza meg a hálózat túlélőképességét. A túlélés javításának három leggyakoribb módja a légréshálózat[50], a multiprotokollos hálózat és a redundáns rendszerek. Az

[50] Airgap network: olyan biztonsági intézkedés, amely magában foglalja a számítógép vagy a hálózat leválasztását, és annak megakadályozását, hogy külső kapcsolatot létesítsen. A légrésszámítógép fizikailag elkülönült, és nem képes vezeték nélkül vagy fizikailag csatlakozni más számítógépekhez vagy hálózati eszközökhöz.

első és legegyszerűbb a zárt hálózat vagy a „légréshálózat”. Ez a hálózat el van szigetelve az internet többi részétől, és nincs fizikai kapcsolat a hálózaton kívül, azonban továbbra is érzékenyek a fizikailag tárolt szoftverek általi támadására (például: pendrive használata által). A következő tényező, amely növelheti a túlélést, a multiprotokollos hálózat és a virtualizáció (virtuális számítógépek használata), ahol egy virtuális, szoftveralapú operációs rendszer egy másik operációs rendszerbe van beágyazva. Ezáltal például hiába éri támadás a virtuális gépet, a hatások nem terjednek át a gazdagépre. Harmadszor, a redundáns rendszerek alkalmazásának leghatékonyabb módja, ha rejtve maradnak az ellenfél elől. Ezért, még ha egy kibertámadás sikeres is, a támadó nem tudja megtalálni és megsemmisíteni a kibertér hatalmas kiterjedésében rejtőző redundáns rendszereket és biztonsági másolatokat. A redundancia nagymértékben javíthatja a vezérlő- és/vagy felügyeleti rendszer megbízhatóságát és elérhetőségét, hiszen - amennyiben bármilyen probléma felmerülne - egy másik entitás át tudja venni a feladatot.

Feldolgozási teljesítmény

A feldolgozási teljesítmény a hagyományos hadviselés tűzerőéhez hasonlítható. A nagyobb feldolgozási teljesítmény több lehetőséget kínál a kiberműveletek végrehajtására. Egy szuperszámítógép pillanatok alatt betörhet egy titkosított szerverbe, míg egy otthoni számítógépnek akár évekbe is telhet, mire elvégzi ugyanazt a feladatot. A tűzerőhöz hasonlóan néha a feldolgozási teljesítmény önmagában is elegendő ahhoz, hogy győzelmet érjünk el egy támadásban. Ezen túlmenően a feldolgozási teljesítmény természetében is folyamatosan fejlődik. Ennek érdekében használnak például botneteket[51] a nagyobb feldolgozási teljesítmény elérése érdekében.

Manőverezhetőség

A kibertérben a manőverezhetőség lehet „logikai” vagy „fizikai”. A logikai manőver szoftverek szintjén történik, míg a fizikai manőver a hardver tényleges fizikai szállítása egyik helyről a másikra. A nagyobb manőverezhetőség mindkét esetben jelentős előnyt jelent. Végső soron a manőverezőképesség előnye azt jelenti, hogy képes az ellenség előtt cselekedni, gyorsabban változtatni, mint az ellenség, és elég gyorsan mozogni ahhoz, hogy elkerülje az ellenséges támadásokat. Míg a manőverképesség elméletben viszonylag egyértelmű, addig annak alkalmazása sokkal összetettebb kérdés. A kibermanőver a manőverezési képességet használja ki egy cél elérése érdekében, ellentétben a túlélési képességgel és a feldolgozási

[51] A botnet internetre csatlakoztatott eszközök összessége, amelyek mindegyike egy vagy több botot futtat.

képességgel. A manőverezhetőség jellemzőjének korlátozott önmagában való értéke van, azt az (összhaderőnemi) célhoz kell kapcsolni.

Offenzív kiberműveletek

A kiberműveletek tervezése nehézségekbe ütközik, és alapvetően kevés nyilvános információ van az államok offenzív kiberképességeiről. Azonban azoknak az alkalmazása és alkalmazhatóságának megítélése vegyes. Egyik megítélés szerint általában nem célszerű támadó kiberműveleteket alkalmazni, mert a végrehajtásuk sebességével ellentétben ezeknek a műveleteknek a tervezése általában több időt vesz igénybe, mint a hagyományos, kinetikus műveletek megtervezése […], miközben számos kiberképességünk is lehet, hogy rendelkezésre áll „készen a polcon", használatuk sokkal több energiát igényel, mint egyszerű betöltésük és elsütésük. A kiberműveleti erőknek először meg kell ismerniük és meg kell érteniük a célhálózatot, node-okat, routereket, szervereket és switcheket, mielőtt bármilyen kiberképességet használnának ellenük. Az ilyen előkészítő munka elvégzéséhez először is parancsba kell adni az üzemeltetőknek, hogy végezzék azt el."[52] Bár, ha ezek a műveletek egyszer elindulnak, gyorsan megtörténhetnek, tervezésük rengeteg időt és erőfeszítést igényel. Az az elvárás, hogy a kibertérhatások azonnal kiválthatók legyenek, gyakran feszültség forrása a kibererők és az általuk támogatott erők művelettervezői között: a kibertérben elérhető hatások az elérhető célpontoktól függenek, ami azt jelenti, hogy a valódi hatások időhorizontja a kívánt hatás összetettségétől és a cél biztonságától függően változik. Az az elképzelés, hogy a kibertér műveletei „gyors tempójúak", csak részben igaz.

Daniel Moore könyvyében [107] két típusú offenzív kiberműveletet különböztet meg: eseményalapú és jelenléti műveleteket. Az előbbi valóban egy „fegyver elsütéséhez" hasonlítható, és általában egy kezdeti cél elérésére irányulnak. Utóbbi a felderítő műveletekhez áll közelebb, és célja inkább az adat és információ megszerzése, illetve az illetéktelen jogosultságok fenntartása vagy eszkalálása, illetve később a jelenlét fenntartása műveletek végrehajtására.

A 2022 februárja óta tartó orosz–ukrán háború kiberműveleti elemeiről több elemzés is született. A 2022. évi CyberWarCon konferencián előadott elemzések adtak elsődleges támpontokat a kiberműveletek szinergiájáról. Egyfelől elmozdulás történt a jelenlétalapú műveletekről az eseményalapú műveletek felé. Az adatbázisok által a különböző orosz érdekeltségbe tartozó kiberműveleti erők – az anyaszervezettől adódóan – inkább a jelenléti

[52] James McGhee, az amerikai különleges műveletek északi parancsnokságának jogi tanácsadója a Strategic Studies Quarterly cikkében rögzítette gondolatait a folyamatról.

típusú műveletekhez szoktak. Azonban az eseményalapú műveleteikkel a periféria infrastruktúrát célozták meg. Periféria infrastruktúrának tekinthetők a tűzfalak, routerek, e-mail-szerverek és bármely olyan infrastruktúra, amely az internet felé „néz". Ennek oka a magas műveleti tempó fenntartása, illetve az, hogy ezek az entitások nehezen védhetők és lassabban detektálhatók, könnyebben tudnak „mozogni" a hálózatban és fenntartani a jogosultságaikat. A főbb lépéseik a hozzáférés-szerzés, a hírszerzés, majd az infrastruktúra felhasználása későbbi támadásokhoz. Azonban a magas műveleti tempó több hibát is eredményez, amely elősegítheti a védekezést.[53]

A fejezetben ez idáig áttekintettük a hasonlóságokat a légierő kialakulási folyamatával, és a nehézségeket, amelyek a kiberműveletek integrációját érintik, mind kulturálisan, mind műveletileg.

A kiberműveletek hatásainak ismerete, a saját rendszerek védelme, a priorizálás és a döntések meghozatalához nélkülözhetetlen egy szintén a légierőtől származó, továbbfejlesztett koncepció: a helyzetkép.

3.3.3 Különbözőségek

Súlypont – célpont

„Általában két (ideális) típusú célpont-kiválasztási folyamatot különböztethetünk meg. Az első eszközközpontú, és általában a következő mintát követi: „Megvan ez a képességem; ki ellen használhatom, és mire?" Ez gyakran passzív, opportunista tevékenységhez vezet. A célpontkiválasztás folyamatának második típusa célközpontú: „Szeretném megcélozni ezt az entitást, hogyan tudom megtenni?" Az állami szereplőnek gyakran nincs más választása, mint a második folyamat követése." [17:46] Azonban a célpont-kiválasztási folyamat előtt még végre kell hajtania a felderítést, információgyűjtést, amely eseteként nagyon sok időt vehet igénybe..." [108:42]

„Az információgyűjtés jellemzően négy szakaszból áll. Az első szakasz a kiválasztás; a támadók nyílt forrásból dolgoznak, hogy adatok gyűjtsenek a célpontról. A második szakasz az erőforrások mélyítése; a támadók mélyebbre ásnak az információgyűjtésben. A harmadik szakasz az információ korrelációjaként határozható meg; a támadók feldolgozzák a releváns

[53] CYBER WAR ON THE EDGE: A BALANCE OF ACCESS AND ACTION Gabby Roncone and John Wolfram, saját jegyzet.

adatokat. Az utolsó és egyben a negyedik szakaszt gyakran támadásmodellezésnek nevezik; a támadók az előző fázis feldolgozott információinak felhasználásával felvázolják a támadás vázlatát." [108:47]

Clausewitz szerint a súlypontok azonosítása az első feladat a háború tervezésében. „Clausewitz a súlypontokat »minden erő és mozgás központjának nevezte«. A súlypont fogalma legjobban összefüggésként írható́ le, amelynek elvesztése pusztító hatással van az ellenség háborús képességére. Az Egyesült Államok Vezérkarának összhaderőnemi tervezésének doktrínájának értelmezése alapján a súlypontok a morális vagy fizikai erő, cselekvési szabadság vagy akarat (erő) forrásai. Ha a súlypont biztosítja az egységet, úgy annak megsemmisítése korlátozza a szereplőnek azon képességét, hogy hatékonyan fellépjen." [31] A súlypontok azonosítása lehetővé teszi a műveletek hatékonyságának fokozását, amely ugyanúgy igaz a kibertéri, mint a szárazföldi, tengeri, légi és űrbeli műveletekre.

A katonai kiberműveletek célja katonai célpontok, és a katonai célpontok a súlypontokra irányulnak, azokra, amelyek a morált vagy a fizikai erőforrásokat biztosítják az ellen-hadviselőnek, ezzel korlátozva annak cselekvési szabadságát vagy csökkentve a cselekvési akaratát. Azonban a kiberhadviselés korában a súlypont ritkán egy koncentrált egység, hanem sokkal inkább egy interdependencia, egy egymástól függő hálózat, ahol a műveleteket a kibertérben és a kibertéren keresztül vagy a kibertér által valósulnak meg. Ezért a súlypont kiberműveleti meghatározása az az erőforrás, amely összekapcsolja és lehetővé teszi a pszichológiai, morális és képességbeli/fizikai erőt, a cselekvési szabadságot és/vagy cselekvési akaratot [95].

Kovács László legújabb könyvében [108:141] az alábbi célpontokat azonosította.

	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

13. ábra: kiberműveletek lehetséges célpontjai.

A civil és a katonai kibertér összefonódása okán a célpontok azonosításakor sem lehet külön választani őket, azon felül pedig a katonai kiberképességek fejlesztésében és fenntartásában is nagyban támaszkodnak a hadseregek a civil cégek szolgáltatásaira és eszközeire. A beszállító láncok (kiber)biztonsága kiemelten fontos, sérülékeny terület biztonsági szempontból. Ezek a súlypontok azonban beleillenek a súlypont teoretikusok gondolkodásába is:

A 14. ábra foglalja össze a főbb légi teoretikusok súlypont elméleteinek célpontját. Egyből feltűnik, hogy egyre komplexebb rendszereket tekintettek célpontnak a légierő fejlődésének előrehaladásával, míg Wardennel elértük gyakorlatilag a kritikus infrastruktúrák támadásáig[54].

Teoretikusok	Célpontok/CoG
Douhet	Lakosság (városok)
Trenchard	Hadianyagok, szállítás, kommunikáció
Mitchell	Létfontosságú központok
de Seversky	Az ipari infrastruktúra minden vonatkozása
ACTS	Kulcsfontosságú gazdasági entitások (háborús anyagok, szállítás, áram, olaj)
Warden	Öt gyűrű-elmélet (vezetés, kulcsfontosságú folyamatok, infrastruktúra, lakosság, haderő)

14. ábra: súlypont elméletek összevetése [saját szerkesztés]

John Warden kiemelkedő elképzelése volt, hogy minden szereplőt rendszernek kell tekinteni. Ezen a nagyobb rendszeren belül öt alrendszer (gyűrű) létezik: a vezetés, az erőforrások (utólag pontosította elméletét, és kulcsfontosságú folyamatokra módosította), az infrastruktúra, a lakosság és a haderő. Minden alrendszer középpontjában számos súlypont található, amelyek sebezhetők, és Warden szerint fontos a párhuzamos támadás használata. E rendszerszintű és párhuzamos támadás a kibertérben nagyfokú hatékonyságot jelenthet [31].

[54] Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek egy ország működése szempontjából létfontosságúak.

A kibertérrel összefüggésben a súlypont olyan fogalom, amely egy hálózat vagy rendszer működéséhez vagy hatékonyságához elengedhetetlen kritikus csomópontra, rendszerre vagy képességre utal. Ez egy kulcsfontosságú tényező vagy elem, amely meghatározza a rendszer általános erősségét vagy gyengeségét, és a kívánt eredmény elérése érdekében sebezhetőségi pontként vagy tőkeáttételként célozható meg.

A kibertér súlypontjai különféle típusú rendszereket foglalhatnak magukban, mint például a kritikus infrastruktúra, katonai hálózatok, pénzügyi rendszerek, kommunikációs rendszerek vagy akár közösségimédia-platformok. Ezeket a rendszereket támadók célba vehetik, hogy megzavarják, tönkretegyék, vagy rosszindulatú célokra kihasználják őket, például károkozásra, adatlopásra vagy a közvélemény manipulálására.

Fontos, hogy a szervezetek és a kormányok azonosítsák és megvédjék súlypontjaikat a kibertérben, mivel ezek gyakran kulcsfontosságúak a rendszer általános biztonsága és ellenálló képessége szempontjából. Ez számos intézkedést foglalhat magában, ideértve a robusztus biztonsági protokollok végrehajtását, a rendszeres kockázatértékelések elvégzését és a vészhelyzeti tervek végrehajtását.

A légtérben és a kibertérben való célzás egyaránt kritikus eleme a modern hadviselésnek, de van néhány lényeges különbség a kettő között. A légtér a földfelszín feletti területet, míg a kibertér a számítógépes hálózatok és az internet által létrehozott virtuális környezetet jelenti. Ez két nagyon különböző környezet, eltérő fizikai tulajdonságokkal és korlátokkal. A légtérben fizikai fegyverekkel, például rakétákkal vagy repülőgépekkel indítható támadás, míg a kibertérben jellemzően digitális eszközökkel, például rosszindulatú szoftverekkel vagy hálózati sebezhetőségekkel indítanak támadást. A légtérben végrehajtott támadások gyakran egy adott helyre vagy régióra korlátozódnak, míg a kibertérben végrehajtott támadásnak potenciálisan globális hatásai lehetnek, mivel bármely csatlakoztatott eszközt vagy hálózatot érinthet. Amint korábban említettük, a kibertérben az attribució/azonosítás kihívást jelenthet az anonimitás és az ebben a környezetben fennálló technikai akadályok miatt. Ezzel szemben sokszor könnyebb a légtérben elkövetett támadásokat nyomon követni, mivel a fizikai fegyverek gyakran származási helyükre vezethetők vissza.

Számos oka lehet annak, hogy miért lehet nehéz eseményeket azonosítani a kibertérben:

- anonimitás: a kibertérben egy egyén vagy csoport viszonylag könnyen névtelen marad, és eltitkolja valódi kilétét. Ez megnehezíti egy cselekvés vagy esemény forrásának egy adott személyre vagy csoportra való visszakövetését.
- technológiai akadályok: a különféle technológiák és titkosítási módszerek alkalmazása megnehezítheti egy cselekvés vagy esemény eredetének nyomon követését. Például egy kibertámadás több kiszolgálót vagy eszközt is felhasználhat a valódi eredete elfedésére.
- false flag: egyes esetekben egy egyén vagy csoport szándékosan félrevezethet másokat olyan taktikákkal, mint például hamis online identitás létrehozása vagy egy másik csoport eszközeinek és technikáinak használata, hogy úgy tűnjön, mintha a támadás más forrásból származna.
- korlátozott digitális nyomrögzítési képességek: előfordulhat, hogy a kibertérben történt eseményeket vizsgáló nyomozók korlátozott kriminalisztikai képességekkel rendelkeznek. Például előfordulhat, hogy bizonyos típusú adatokat nem őriznek meg, vagy nehéz hozzáférni, ami megnehezíti egy művelet vagy esemény forrásának azonosítását.

Összességében az attribúció a kibertérben kihívást jelenthet a környezet összetettsége és az egyének és csoportok tetteik elrejtésének különféle módjai miatt.

Cyber Kill Chain

A Cyber Kill Chain-t már bemutattam az 1. fejezet információs műveletekről szóló alfejezetében (39.oldal, 8. ábra). A modell azért fontos, mert keretet biztosít a támadások előrehaladásának megértéséhez, és segíthet a szervezeteknek a támadások azonosításában és megelőzésében a különböző szakaszokban [109]. Például végrehajthatnak olyan intézkedéseket, amelyek megakadályozzák a felderítést, például elrejthetik az alkalmazottak és hálózatok nevét, vagy víruskereső szoftvert használhatnak a rosszindulatú rakományok kézbesítésének észlelésére és megakadályozására. Ezenkívül a szervezetek hálózati megfigyelőeszközöket használhatnak a kihasználás és telepítés észlelésére, és biztonsági intézkedéseket hajthatnak végre a támadó parancs- és irányítási csatornáinak megzavarására.

A Kill Chain hét szakaszból áll:

- felderítés: ez a támadás kezdeti szakasza, ahol a támadó információkat gyűjt a célpontról. Ez magában foglalhatja a célpont hálózatainak, rendszereinek és alkalmazottainak kutatását.
- fegyverkezés: ebben a szakaszban a támadó előkészíti azokat az eszközöket és rakományokat, amelyeket a célpont kompromittálására használnak fel. Ide tartozhat rosszindulatú programok, adathalász e-mailek vagy kihasználó készletek létrehozása.
- kézbesítés: a támadó eljuttatja a fegyveres rakományt a célponthoz, gyakran e-mailben, rosszindulatú webhelyen vagy feltört hálózaton keresztül.
- kihasználás: a támadó kihasználja a célpont rendszereinek biztonsági rését a hasznos terhelés végrehajtásához és a hozzáféréshez.
- telepítés: a támadó rosszindulatú programokat vagy más eszközöket telepít, hogy fenntartsa a hozzáférést a célpont rendszereihez.
- parancs és vezérlés: a támadó kommunikációs eszközt hoz létre a feltört rendszerekkel, lehetővé téve számukra, hogy távolról irányítsák azokat.
- célok elérése érdekében végrehajtott műveletek: a támadó a feltört rendszereket céljai elérése érdekében használja, beleértve az érzékeny adatok ellopását, a műveletek megzavarását vagy károk okozását.

Online Műveleti Cyber Kill Chain

És hogy mi ellen kellene a TOC/SOC/JSOC-nak védekezniük? Az egyik alapmodell a Lockheed Martin vállalat által leírt „Cyber Kill Chain”. A hét lépcsőből álló lánc három jól elkülöníthető részre oszlik: a kompromittálás előtti szakaszra (felderítés, fegyverkezés, szállítás), a kompromittálási szakaszra (sérülékenység kihasználása, káros elem telepítése) és maga a káros tevékenység (vezetési és irányítási rendszerek, végrehajtás). Ez a megközelítés a kiberműveletekre igaz lehet, azonban az információs műveletekre már kevésbé. Ezért a META vállalat két mérnöke, Ben Nimmo és Eric Hutchins javaslatot tettek egy online műveleti kill chainre. Az elmúlt 18 hónap tapasztalatai alapján egyfajta kombinált, kiber- és információs műveletekre lettek figyelmesek. Ennek jellegzetessége, hogy a művelet mindkét oldalán fizikai személyek állnak, és a befolyásolás sémája mindig egy adott fiók feletti irányítás átvételével kezdődik, majd a befolyásolási művelet indul, utána pedig elkezdődik a dezinformáció terjesztése. Példa erre a Ghostwriter kampány, ahol a webhelyek feltörését vagy e-mail-fiókok hamisítását hamis tartalom terjesztésére használták fel, ideértve a hamisított híreket, idézeteket,

levelezést és más olyan dokumentumokat, amelyekről úgy tűnik, mintha katonai tisztviselőktől és politikai személyiségektől származnának. A Ghostwriter kampány elsődlegesen a Balti-államokat célozta NATO-ellenes üzenetekkel.

„Remek példa erre a fajta műveletre a Ghostwriter kampány, amely fiókok átvételét és kompromisszumokat egyaránt alkalmaz. De ha ezek a fiókok már nyitottak, akkor befolyásolási művelet végrehajtására is használja őket." A Ghostwriter egy olyan befolyásolási kampány volt, amely Litvániát, Lettországot és Lengyelországot célozta meg, és népszerűsítette az Észak-atlanti Szerződés Szervezetének (NATO) kelet európai jelenlétét kritizáló narratívákat.

Az online műveleti kill chain modellt úgy tervezték, hogy áthidalja a kárt okozó információs műveletek és az egyéb online rosszindulatú műveletek közötti szakadékot. A modell alapvetően azon az elven alapszik, hogy ha online műveletet folytatunk, akkor mindegy, hogy mit tervezünk vele, bizonyos közös vonások érvényesülni fognak: csatlakozni kell az internethez, ha a közösségi médiában fogják a művelet végrehajtani, akkor szükség lesz közösségimédia-fiókokra.

A következőkben röviden leírom ennek a kill chain[55] 10 lépését, fontos azonban hangsúlyozni, hogy ez a lánc moduláris, nem minden online művelet fogja az összes lépést tartalmazni:

1. eszközbeszerzés: ezek lehetnek például IP-címek, e-mail-címek, telefonszámok, kripto-pénztárcák, vagy bármi, amire az ellenfélnek szüksége van a működéshez;
2. eszközök álcázása: ezáltal hitelesítik az eszközeiket, miután a művelet majd látszódni fog az interneten;
3. információgyűjtés: célja a környezet vagy a célszemély feltérképezése;
4. koordináció és tervezés;
5. védelem tesztelése: célja felmérni a rendszerek védelmét;
6. észlelés elkerülése: légierő-hasonlattal élve ez nem azt jelenti, hogy más felségjeleket használ, más színekre festi magát vagy más lajstromszámot kap, hanem hogy a radarok alatt repül, például azáltal, hogy Unicode karaktereket használnak az ál-weboldalhoz;
7. válogatás nélküli támadás: ilyen a legtöbb spamkampány és az online műveletek spektrumának kevésbé kifinomult vége;
8. célszemély elleni támadás: ez hasonló a valós célszemély kiválasztásához;

55

9. eszközök kompromittálása: ekkor történik a tényleges támadás, a célszemély által használt eszközök átvétele,
10. persistence (kitartás) elősegítése: általában ebben a fázisban találkoznak először a kibervédelmi szakértők az incidenssel.

Az online műveleti kill chain annyiban különbözik a Lockheed Martint által elterjesztett cyber kill chaintől, hogy az előkészületi fázis (beszerzés, álcázás) illetve a humán oldalát jobban előtérbe helyezi (célszemélyek kiválasztása), ezáltal a technikai oldalon túl számol az emberi oldallal is. Ez megnehezíti a támadók dolgát, mert az ő szemszögükből költséghatékonyabb egy phishing e-maillel (megtévesztő email) vagy social engineeringgel[56] eljutni rendszerekbe, és ebből következik, hogy minden szervezetnek fontos odafigyelnie, hogy munkavállalóik kellően fel legyenek készülve ilyen támadásokra, megtévesztésekre.

A kill chain-ek jelentősége abban van, hogy segítenek azokat a folyamatokat átlátni, amelyekkel a szervezetek szembe kerülhetnek, és amelyeket minél korábban észlelni szükséges ahhoz, hogy időben beavatkozhassanak az illetékes szakemberek. Ehhez (is) szükségessé válik a helyzetkép megjelenítése a kibertérben.

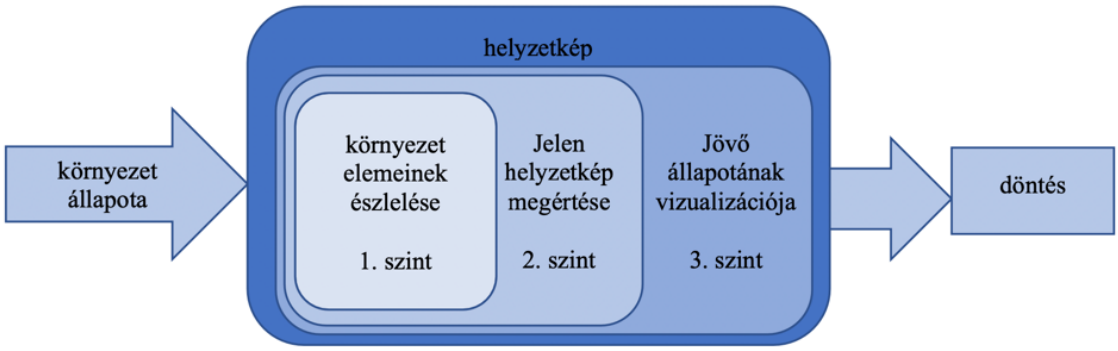
3.4 Helyzetkép

3.4.1 Hagyományos helyzetkép

A helyzetfelismerést (SA, situational awareness) először Endsley mutatta be átfogó munkájában. Endsley definíciója alapján az SA-rendszer három fő összetevőből áll, ezek az észlelés, a megértés és a vizualizáció. Ezt a munkát az SA-kutatás fő referenciamodelljének tekintik, és széles körben alkalmazzák számos kutatási kontextusban, többek között a légierőnél. A 80-as évekre az automatizált rendszerek már az emberi operátorra voltak optimalizálva az aktuális helyzet nyomon követéséhez. Ekkor vált ketté az ember által felfogott és a tényleges rendszerállapot, és vált az SA központi elemévé, növelve az optimális döntések valószínűségét összetett valós idejű helyzetekben. Azóta az SA-koncepció alkalmazása gyorsan elterjedt a repülésen kívül más területekre is. Ennek az elterjedésének legjelentősebb mozgatórugója a technológia fejlődése volt.

[56] Olyan támadási módszert jelent, ahol nem valamilyen technológiai sebezhetőséget használnak ki, hanem a számítógépet használó személyt tévesztik meg.

Endsley a háromszintű modelldefiníciót javasolta: „A helyzettudatosság (1) a környezet elemeinek észlelése egy térben és időben, (2) jelentésük megértése és (3) állapotuk vizualizációja a közeljövőben”. Endsley az SA-t tudásállapotként fogja fel, és megkülönbözteti az állapot eléréséhez használt folyamatoktól [110].

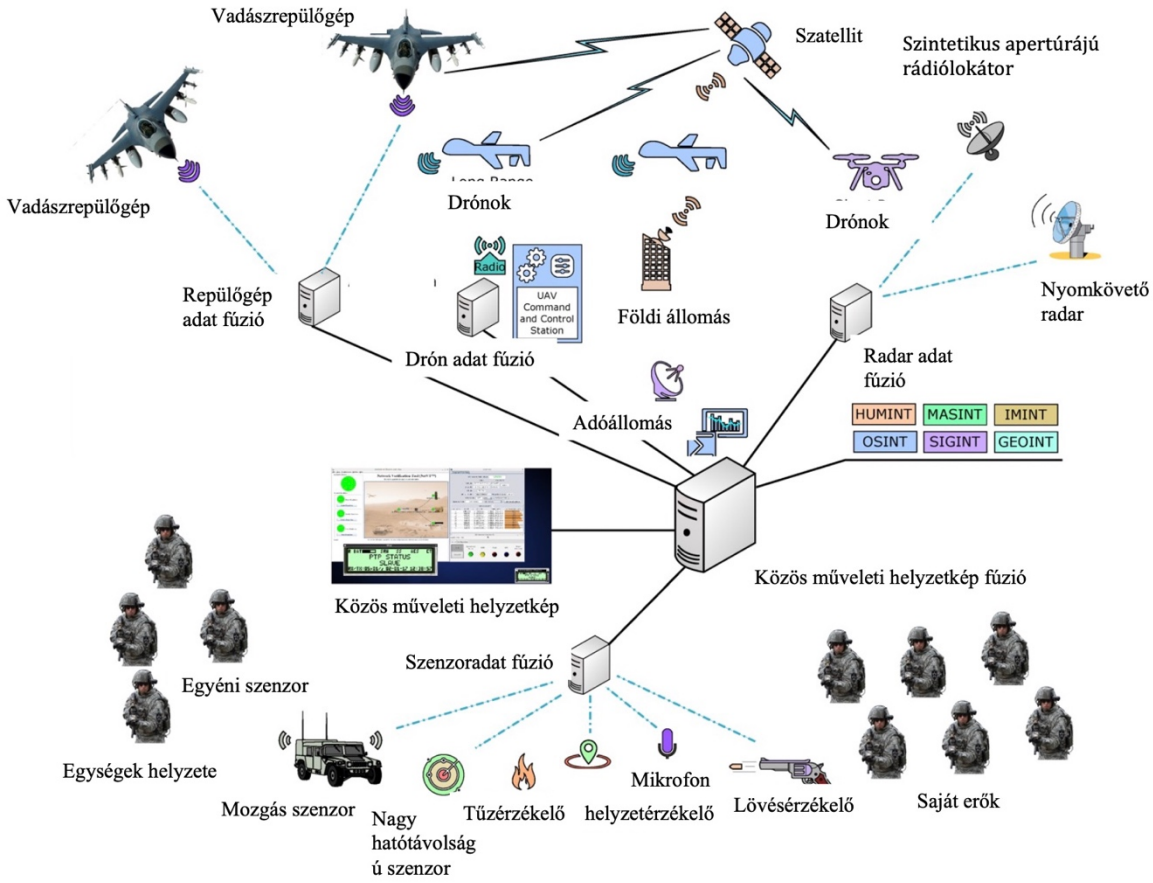


15. ábra. Az SA egymásra épülő elemeiről (saját készítés). Forrás: [111]

Az első szint a környezet elemeinek észlelési szintje, a környezet állapotjellemzői és a releváns attribútumok dinamikája érzékelhetők. A második szint az információ nyers formában történő kezdeti fogadását jelenti. Az adatrögzítés, valamint az adatmegértés és adatértelmezés szétválasztása lehetővé teszi az eltérések beazonosítását. A cél nemcsak a helyzet észlelése, hanem a valós helyzet megértése is. Az elemek kombinálása, értelmezése, adott célokhoz kapcsolódó kontextus hozzárendelése, az elemző-értékelő személy ismereteivel és tapasztalatával kombinálva holisztikus környezetképet alkotnak. A jövőbeli állapot előrejelzése az SA harmadik és legmagasabb szintje. A legtöbb területen, ahol az SA fontos, a tapasztalt kezelők nagymértékben támaszkodnak a jövőbeli előrejelzésekre. A jelenlegi eseményeken és dinamikán alapuló jövő előre vetítése lehetővé teszi számukra, hogy ideje korán jelezzék a jövőbeli eseményeket és azok következményeit, ezzel lehetővé téve a megfelelő időbeli döntés meghozatalát.

A 16. sz. ábra mutatja be az SA összetettségét a jelenben. Az ábra bal felső területén látjuk a repülőgépeket, amelyek kommunikálnak a műholdakkal, valamint a légierő központtal is (aircraft data fusion), mely adatközpont azután továbbítja az adatokat a COP (common operational picture, a közös hadműveleti helyzetkép) feldolgozó számára. A COP feldolgozóba érkeznek be adatok a szenzorokból, a különböző felderítési adatok (OSINT, SIGINT) is.

Maga a COP a releváns (műveleti) információk integrált megjelenítése (pl. saját csapatok és ellenséges csapatok helyzete, fontos infrastruktúrák, helyzete és állapota), amelyet több parancsnokság is megoszt. Ez nagyban elősegíti az összhaderőnemi művelet tervezést és vezetést.



16. ábra: a helyzetképkomplexitásának bemutatása [112]

3.4.2 OSINT

Az OSINT (nyíltforrású hírszerzés – OSINT, open-source intelligence) a hírszerzés egyik ága. Definíciói között létezik eltérés, ahogyan Solti István tanulmányában [113:5–7] rámutat, az angolszász megfogalmazásban nyilvánosan elérhető forrásokról beszélünk (azaz bárki által fellelhető, megvásárolható), míg Lévay és Vida értelmezésében fontos, hogy nyílt is legyen a forrás (azaz nem minősített) [143:6]. További megkülönböztetésre ad lehetőséget,

hogy klasszikus vagy elektronikus forrásról van-e szó. Klasszikusnak (vagy első generációs) forrásnak tekinthető a könyvtár, irattár, sajtótermék, rádió és tv-adások, konferenciák, interjúk, folyóiratok, tudományos publikációk, míg elektronikus (vagy második generációs) forrásnak például az interneten fellelhető adatbázisok, a közösségi média vagy a keresőrendszerek [115:88]. Az OSINT mindkét oldalról fontos: a támadók oldaláról OSINT-tal kezdik meg a feltérképezést, információgyűjtést, célszemélyek azonosítását. Védekező oldalról az OSINT segítségével képesek a helyzetképet legszélesebben kiszolgálni.

A hírszerzési ciklus a hírszerzés folyamatának sematikus leírása, amelynek általánosságban öt fázisát szokás megkülönböztetni : (1) az információigények fogadása, (2) az adatszerzés, (3) az információk feldolgozása és rendszerezése, (4) az információk elemzése-értékelése, valamint (5) a tájékoztatás [115:115]. A ciklust összekapcsolva az OSINT-tal, Vida Csaba megfogalmazásában „a nyílt forrású adatszerzés speciális módszertan alapján, folyamatosan végzendő adatszerző tevékenység, amely elsődleges (nyers) és másodlagos (már feldolgozott vagy átvett) nyílt információk megszerzésére és feldolgozására irányul a felhasználók (kormányzat, haderő, rendőrség, cégek, vállalatok stb.) információigényeinek kielégítése érdekében” [115:134].

Az OSINT tipizálásának egyik módja a generációkra való osztása, ahogyan a RAND is tette [106]. Az ő meglátásuk szerint az OSINT-nak – kiváltképp a második generációs, nyílt forrású felderítésnek – számtalan előnye van: a gyorsasága (elsősorban az információ terjedésének gyorsasága), a mennyisége (sokkal több blogger, újságíró, riporter és kutató van, mint elemző-értékelő egy adott szervezetnél), a minőség (megfelelő szűrés és ellenőrzés után), az átláthatóság (forrás), a tájékoztatás egyszerűsége (az információ továbbítása egyszerűbb, mint minősített adatok esetében) és a költséghatékonyság (technikai, előfizetések) [116].

Az alábbiakban összefoglalom az OSINT-generációinak egy lehetséges fogalmi és tartalmi meghatározását.

Az első generáció az OSINT hagyományos megközelítésére utal, amely nyilvánosan elérhető forrásokból, például újságokból, könyvekből és kormányzati jelentésekből származó információk kézi gyűjtésén és elemzésén alapult. Ezt a generációt az információkhoz való korlátozott hozzáférés, valamint azok feldolgozásának és megosztásának korlátozott lehetőségei jellemezték.

A második generáció a számítástechnika bevezetését jelenti az OSINT folyamatba. Ezt a generációt az internetről, közösségi médiából és más digitális forrásokból származó nagy mennyiségű adat összegyűjtésére, szűrésére és elemzésére szolgáló automatizált eszközök használata jellemezte. A hangsúly az adatbányászaton és a mintafelismerésen volt.

E folyamat következménye az értékelő-elemzők információs túltelítődése. Az információs túltelítődés fogalmát Alvin Toffler népszerűsítette Jövősokk című könyvében, a definíciója: „az információ össz-tömegének disszonáns, egészségtelen növekedése. Mivel az információk áttekintésének, keresésének, kezelésének és felhasználásának módszerei lassabban fejlődnek, mint az elérhető információ mennyisége, a túlzott információtermelés okozta feldolgozási problémák alapvető rendszerfunkciókat veszélyeztetnek” [117].

A harmadik generáció a humán hírszerzés (HUMINT) és az OSINT integrálását jelenti. Ezt a generációt az a felismerés hozta létre, hogy az automatizált eszközök önmagukban nem tudják biztosítani a döntéshozatalhoz szükséges mélységű elemzést és megértést. A hangsúly a humán elemzők és az automatizált eszközök közötti együttműködésen volt, az előbbiek az a begyűjtött és feldolgozott információkhoz a kontextust, a megítélést és szakértelmet adják.

A növekvő adattömeg és az elemzők véges teljesítőképessége közötti szakadék áthidalására a fő segítség a mesterséges intelligencia alkalmazása a folyamatok automatizálásában, az elemző-értékelők képességeinek kiterjesztésében, az adatok gyűjtésében, szűrésében, összekapcsolásában. A mesterséges intelligencia használata egyben az OSINT esetében több kihívást is jelent, mert:

- a releváns információk mind hihetetlenül sokrétűek, és erősen összefüggenek a kontextussal,
- a nagy mennyiségű adatelemzés képes ugyan trendeket kimutatni, azonban ehhez gyakran minden rendelkezésre álló, releváns adatra szükség lenne,
- meg kell vizsgálni minden dokumentum hitelességét, megbízhatóságát, valamint a szerző motivációját is [118:3].

A negyedik generáció jelenleg még nem egészen különíthető el a harmadik generációtól. Ebben - az OSINT folyamat javítására - a mesterséges intelligencia és a gépi tanulás használatának egyre növekvő trendje jelenik meg. Ezt a generációt fejlett algoritmusok és modellek használata jellemzi az adatok elemzéséhez, előrejelzéséhez és megjelenítéséhez. A

hangsúly azon van, hogy kifinomultabb és pontosabb eszközöket fejlesszenek ki, melyek segítségével igen összetett és gyorsan változó körülmények között is jó döntéseket lehet hozni. Ezek azok a folyamatok, amelyek a kiber helyzetképben is megjelennek.

3.4.3 Kiberhelyzetkép

A kiberhelyzetkép-ismeret (CSA, cyber situational awareness) az általános helyzetismeret (SA) alkalmazása a kiberterületre. A kiberkörnyezet érzékelése, a jelenlegi biztonsági helyzet megértése, valamint a jövőbeni helyzet alakulásának előrejelzése a kiberműveletek elengedhetetlen része. Tekintettel az SA és CSA definícióival és fogalmaival foglalkozó számos kutatási munkára, meglepően kevés taxonómia található az összetevőiről. Ha a kibertérvédelmi tartományról van szó, a CSA úgy definiálható, mint egy adott rendszerrel kapcsolatos adatok előkészítése, egyesítése, feldolgozása és kiértékelése, hogy megértsék a rendszer környezetét, hogy képes legyen előre jelezni a rendszert vagy hálózatot fenyegető potenciális kiberfenyegetéseket, és reagálni tudjon azokra [119:5].

A kiber helyzetfelismerés javítása segíti a döntéshozókat a küldetésközpontú képességek fejlesztése révén, ezzel egyben erősíti a szervezet kibertér műveleti képességeit is. Cél egy interoperábilis, valós idejű védelmi célú CSA létrehozása. Az „EU katonai víziója és stratégiája a kibertérről, mint műveleti területről”[70] dokumentum szerint: a kibertér magában foglalja a különálló, de egymással összefüggő fizikai réteget, logikai réteget és kognitív réteget, amely nem tekinthető önállóan, hanem a triád kibertér, az elektromágneses környezet és a kognitív környezet egyik oldala. A kibertér műveletek mindig tartalmazzák a logikai réteget, és opcionálisan tartalmazhat tevékenységeket vagy elemeket a másik két rétegből is.

A kibertérben végzett katonai tevékenységek két átfogó küldetést foglalhatnak magukban: saját kiberterük védelmét (nemzeti szint, uniós szint, koalíciós szint stb.), valamint offenzív műveletek végrehajtását. Ebben az összefüggésben a CSA azt a képességet írja le, amely képes érzékelni, értelmezni és kivetíteni a jól megalapozott döntések meghozatalához szükséges csatatér elemeit, hangsúlyt fektetve a kiberhelyzetekre és azok hatásaira a tervezett küldetésekre vonatkozóan. Ehhez a helyzet elemeinek holisztikus és emberileg érthető ábrázolására van szükség, hiszen a parancsnokoknak tudniuk kell értelmezniük és döntést hozniuk a CSA alapján.

A kibertérben végzett katonai műveletek összetettsége összefügg azzal a kihívással, hogy:

1. valós időben a különböző adatfeldolgozási síkok állapotát, amelyekben a különböző szereplők - szövetségesek, ellenségek, ismeretlen és semleges entitások - egymás mellett léteznek,
2. valamint a küldetések erőfeszítési irányaihoz, feladataihoz és célkitűzéseihez való viszonyt is megjelenítse és értelmezze.

Ezek a katonai műveletek kiterjesztik a kiberfizikai rendszerekben (CPS, cyber-physical system) fennálló helyzetek hagyományos megértésének hatókörét a kiberműveletekre, beleértve a kibersúlypontok, a kibertérben vagy azon keresztül végrehajtott küldetéseket, valamint a kinetikus csatához kapcsolódó hatások és dimenziók területére (levegő, szárazföld, űr, tenger) vagy nem-kinetikus hatásokra (információs, politikai, gazdasági, társadalmi, környezeti stb.).

Kihívásnak számít az emberi döntéshozókat segítő, a parancsnoki szándék megőrzése mellett a küldetésközpontú CSA képességek fejlesztése, amelyet felerősít a kibertér különböző alrétegeinek egyetlen környezetként való megértésének nehézsége, valamint a kiberhatásokból fakadó hibrid hatások figyelembevétele.

Az ideális CSA-nak rendelkeznie kellene teljes spektrumú kiberhelyzeti helyzetfelismeréssel, amely a kibertér egészének megértésének elősegítését jelentené a döntéshozók számára, beleértve a fizikai (hardver, földrajzi, elektromágneses spektrum stb.), a logikai (szoftver, hálózatok stb.) és a kiberszemélyiség (ember-gép interfész, kognitív, pszichológiai, társadalmi) eszközeit és hatásait. Támogatnia kellene a döntéshoztatalt kreatív és rugalmas döntési pontokkal és lehetőségekkel, valamint a kibertérben vagy azon keresztül történő küldetések teljesítése lehetőségeinek azonosítását és értékelését. Fontos a képességek összehangolása és az interoperabilitás, amely lehetővé teszi a bevethetőséget a taktikai, műveleti és stratégiai egységek esetében is. Ez magában foglalja az olyan együttműködési környezetekhez való alkalmazkodást, mint a nemzeti, európai és NATO szintű közös és/vagy kombinált műveletek.

Mindezek biztosításával érhető el a kibertér helyzetfelismerés és helyzetmegértés, amely valamennyi környezeti elem és esemény észlelésének és megértésének szintje az idő vagy tér vonatkozásában, valamint állapotuk előrevetítése valamely változó megváltozását követően, amely lehetővé teszi a racionális döntések és tettek meghozatalát a kibertérben [70].

A kiberhelyzet-tudatosság a szervezet azon képességére vonatkozik, hogy megértse kiberkörnyezete jelenlegi állapotát, beleértve a potenciális fenyegetéseket és sebezhetőségeket, amelyekkel szembe kell néznie, valamint azokat az erőforrásokat és képességeket, amelyekkel ezekre a fenyegetésekre reagálnia kell. Ez magában foglalja a szervezet hálózataira, rendszereire és adataira vonatkozó információk gyűjtését és elemzését, valamint a potenciális kibertámadások vagy más biztonsági incidensek mutatóinak figyelését.

A hatékony kiberhelyzet-felismerés elengedhetetlen ahhoz, hogy a szervezetek megvédjék magukat a kiberfenyegetésekkel szemben, és reagáljanak az incidensekre bekövetkezésükkor. Ez megköveteli a technikai és elemző készségek kombinációját, valamint a helyzet gyors és pontos felmérésének és a megfelelő intézkedések megtételének képességét.

A kiberhelyzeti helyzetfelismerésnek számos kulcsfontosságú összetevője van, többek között:

- a hálózat feltérképezése: egy szervezet hálózatai és rendszerei elrendezésének és konfigurációjának megértése, beleértve azok függőségeit és összekapcsolódásait;
- az eszközkezelés: a szervezet kritikus eszközeinek, például szerverek, munkaállomások és adattárolók azonosítása és nyomon követése;
- a fenyegetések felderítése (cyber threat intelligence, CTI): információgyűjtés és elemzés a lehetséges kiberfenyegetésekről és sebezhetőségekről, beleértve a rosszindulatú programokat, az adathalász-támadásokat és a kiberbűnözők által használt egyéb taktikákat;
- a sebezhetőségkezelés: a szervezet rendszereinek és hálózatainak sebezhetőségeinek azonosítása és kezelése;
- az incidensreagálás: a kiberincidensekre adott választerv kidolgozása és fenntartása, beleértve a támadások észlelésére, megfékezésére és hatásainak mérséklésére szolgáló eljárásokat.

Mindamellett, hogy az SA általános definíciója alkalmazható a CSA-ra is, katonai szempontból a kiberkörnyezetnek számos sajátossága van, amelyeket figyelembe kell venni: ilyen a (1) kiberkörnyezet maga, az (2) érzékelés, a (3) teljesítmény és az (4) ellenfél előnye.

A kiberkörnyezetben szinte korlátlan lehetőségek rejlenek, hiszen nincsenek határai. Egy ilyen környezet dinamikája és határtalansága kihívást jelent a helyzetfelmérés szempontjából a hagyományos katonai konfliktusok fizikai világához képest, ahol a környezet állandó és a fizika törvényei szerint irányítható. A kiberkörnyezet térbeli tulajdonságai globálisak, ami problémássá teszi az SA-határok meghatározását, ha nem akarjuk a „minden/mindenhol" specifikációt használni. Ezért a hálózat vagy a rendszer fizikai helyét általában a CSA térbeli határaként használják.

Érzékelés: a hadsereg számára az információk specifikus hardveres érzékelőkkel és fizikai megfigyeléssel is rögzíthetők. A hardveres érzékelők és jelfeldolgozási technikák fontos, de nem alapvető szerepet játszanak; fizikai megfigyelés használható olyan esetekben, amikor hardveres érzékelők nem állnak rendelkezésre. A CSA-ban az információt kizárólag érzékelők nyerik ki, az információ közvetlen megfigyelése nem lehetséges. Az információhoz hasonlóan az ellenfeleket sem lehet közvetlenül megfigyelni. Csak az érzékelők által rögzített információk elemzésével észlelhetők, ez teszi lehetővé, hogy az ellenfelek rejtve maradjanak a hálózatokban.

Teljesítmény: a számítógépes környezetben történő támadás indításához szükséges erőforrások viszonylag kicsik. Egy hagyományos konfliktushoz képest a kiberkonfliktus elindításához szükséges erőforrások néhány előfeltételt figyelembe véve egy személyre is korlátozódhatnak. Egy másik tényező, amelyet figyelembe kell venni a teljesítménnyel kapcsolatban, az az események sebessége. Az események sebessége nagyságrendekkel gyorsabb kehet, mint a fizikai konfliktusok esetén. Az ilyen nagy mennyiségű információ feldolgozásához szükséges erőforrások lényegesen költségesebbek a CSA esetében.

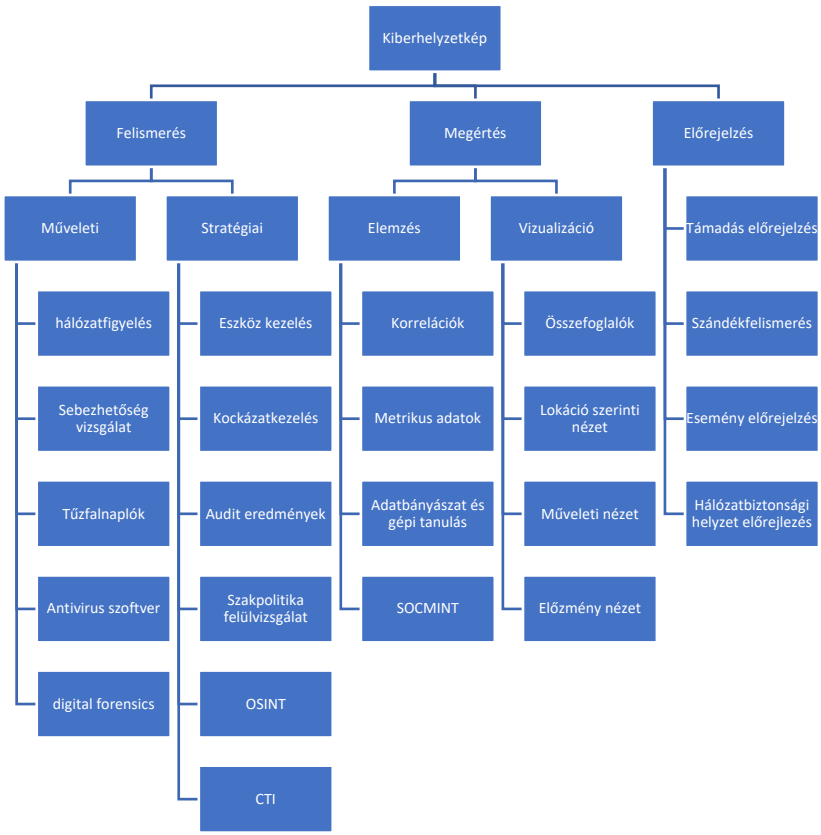
A támadó előnye kiberkörnyezetben: a hagyományos katonai doktrína szerint a védekezőnek számos előnye van, például védett létesítmény adta fizikai védelem, vagy az információs aszimmetriából eredő jobb döntéshozatali képesség. A kibertámadó a kiberkonfliktusok esetén minden előnyt átvesz: többek között az anonimitást, a sérülékenységek felderítését bárhonnan a világból, az emberi gyengeségek kihasználását social engineering révén, valamint az idő, hely és eszközök kiválasztásának lehetőségét.

Ezeket figyelembe véve szükséges egy kiberhelyzetkép megalkotása, amely képes valós időben, több helyszínen érzékelni és értelmezni az eseményeket. Ennek a szakirodalom szerint három összetevője van [120:1]:

(i) a helyzetkép-felismerés a támadás előfordulásának azonosításával, valamint a támadás típusával, forrásával és céljával foglalkozik. Ez a szempont magában foglalja az összegyűjtött adatok és információk minőségét, valóságtartalmát, teljességét és frissességét.

(ii) a helyzetkép-megértés, beleértve a kibertámadási hatásvizsgálatát mind a jelenlegi, mind a jövőbeli hatásokra vonatkozóan. Ez magában foglalja a támadó viselkedésének, szándékainak vizsgálatát is, annak felderítését, hogy megismerje a jelenlegi helyzet kialakulásának okát.

(iii) a helyzetkép-előrejelzés, beleértve a helyzet alakulásának és további hatásainak bemutatását.



17. ábra: Kiber SA lehetséges összevetőinek ábrázolása (saját készítés)

Az SA-technikák jelenlegi megközelítésének többségében az első és a második szintre összpontosítanak, így a sebezhetőségelemzésekre, azonban a vizualizáció szintje, a magasabb SA-szint még mindig hiányzik. Azonban a 13.sz. ábra alapján a különböző javasolt rendszerelemeket szétbontva megvalósítható egy integrált CSA taktikai szinten a műveleti területre kiküldhető TOC-okkal (tactical operations center), a hátországban maradó (műveleti)

SOC-kal (security operations center) és stratégiai szinten megjelenő JSOC-kal (joint security operations center).

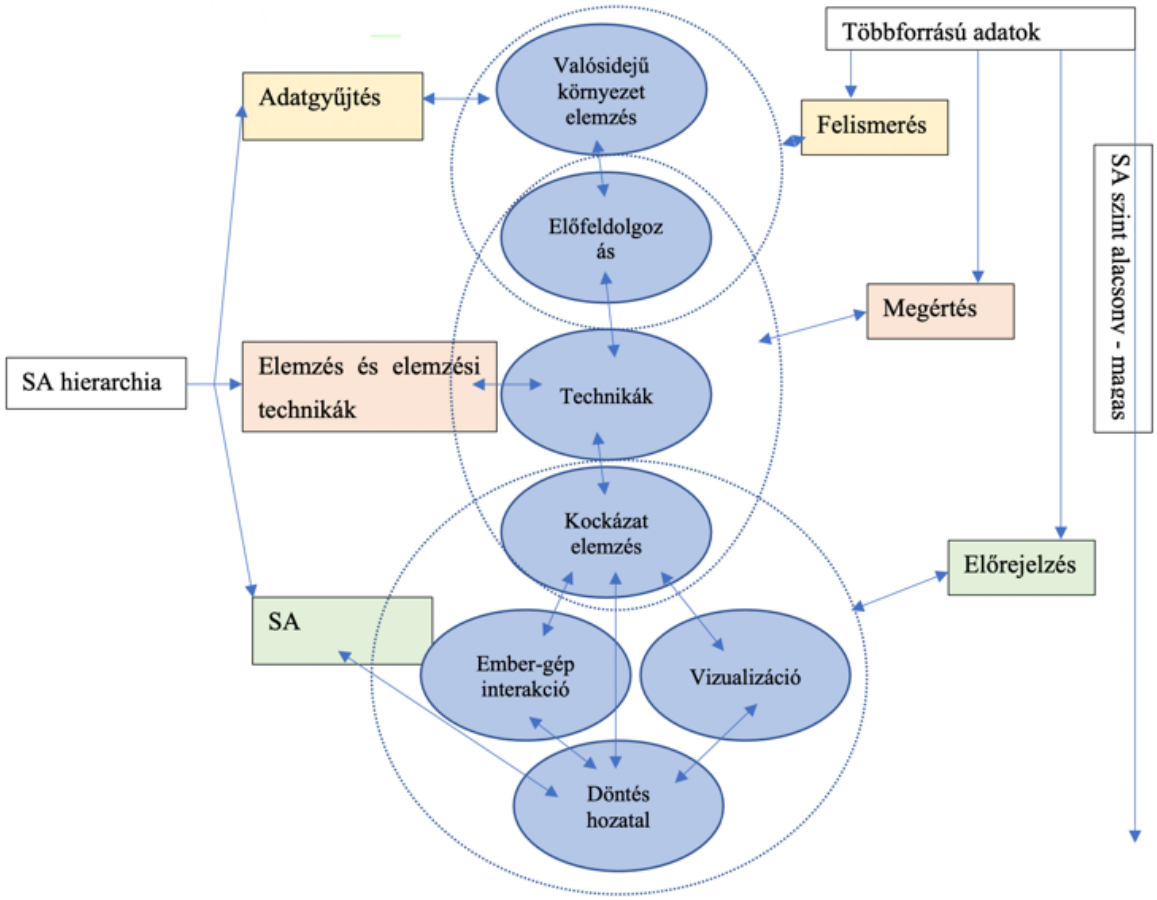
3.4.4 Műveleti SOC

A taktikai műveleti központ (TOC) olyan parancsnoki és irányítási létesítmény, amelyet katonai vagy bűnüldöző szervezetek használnak a személyzet és az erőforrások tevékenységének koordinálására és irányítására a művelet során. Általában kisebb léptékű műveletek támogatására szolgál, mint például razzia vagy kutató-mentő küldetés, nem pedig nagyobb konfliktusok esetén.

A TOC jellemzően a műveleti terület közelében található, és számos kommunikációs és információgyűjtő berendezéssel van felszerelve, amelyek lehetővé teszik a parancsnoki csapat számára, hogy tájékozott maradjon a helyszíni helyzetről, és megalapozott döntéseket hozhasson. A TOC felszerelhető kijelzőkkel vagy térképekkel is, amelyek segítik az aktuális helyzet megjelenítését, valamint a személyzet és az eszközök mozgásának nyomon követését.

A TOC-ban dolgozó személyzet felelős a művelet nyomon követéséért, a terepi egységekkel való kommunikációért és a magasabb szintű parancsnokok frissítéséért. Felelősek lehetnek a logisztikai és egyéb támogató funkciók irányításáért is, mint például a sérültek egészségügyi ellátásának koordinálásáért vagy a személyzet és a felszerelés szállításának megszervezéséért.

A TOC-knak interoperábilisnak kell lennie és közös műveleti képet kell nyújtania a döntéshozó számára [121]. Hogy a műveleti területen lévő hálózatokat és kommunikációt biztosítani tudja, szükséges műveleti szintű érzékelést végeznie (többek között hálózatfigyelés, tűzfalellenőrzés stb.), valamint egy elsődleges elemzést kell végeznie arról, hogy mit észlel. Ez megegyezik a 14. sz. ábra adatgyűjtés-halmazával. Azonban ez nemcsak a terepen lévő TOC-nak a feladata, hanem a hátországban levő SOC-nak is. A SOC-nak általában szélesebb mandátuma van, mint egy műveletre vagy misszióra specializált TOC-nak, azonban ennek köszönhetően nagyobb kapacitással is rendelkezik. A SOC-ban megtörténik az észlelt adatok és anomáliák kielemzése, majd megkezdődik az értékelési fázis.



18. ábra Kiber SA folyamatai [120]

A 18. ábra mutatja be a 17. ábra továbbfejlesztett változatát, amely magába foglalja a folyamatokat is. Ez alapján három szinte osztható az SA: a felismerés, megértés és előrejelzés szintjére.

A felismerés szintje az adatok gyűjtését és azok elemzésre való előkészítését foglalja magában. Adatforrások lehetnek a szenzorok adatai, a tevékenységi naplók, vagy a tűzfalnaplók. A megértés szintjéhez tartoznak a különböző technikai elemzési technikák: anomália felismerés, összefüggés-kutatás, illetve a kockázatelemzés is. Végül az SA-hoz tartozik a vizualizáció, az ember-gép interakciók (a számítástechnika tervezésével és használatával kapcsolatos kutatás, amely a felhasználók és a számítógépek közötti interfészekre összpontosít), és a döntéshozatal is.

A katonai szervezetek a kibertér eszközeit (információs technológiát, IT) beágyazták műveleti folyamataikba, hogy növeljék hatékonyságukat, javítsák a döntéshozatal minőségét. Ez az IT-műveleti függőség a szervezet küldetését veszélybe sodorhatja, ha valamilyen incidens (például egy kritikus információforrás elvesztése vagy manipulálása) történik a kibertérben. A

katonai műveletek jellemzően dinamikusan változó, időérzékeny, összetett, összehangolt műveleteket és feladatokat foglalnak magukban, több szervezeti egység bevonásával.

Valamikor elfogadott volt, hogy a kiberbiztonságot egy szervezeten belül csak úgy lehet elérni, ha minden sebezhetőséget megszüntetnek. Mostanra azonban ez lehetetlenné vált, nem lehetséges mindent megvédeni. Ezért jelent meg a szakirodalomban a küldetésbiztosítás[57] fogalma. Elismerve ezeket a kihívásokat, valamint a kockázatkezelés nehézségeit a kiberhelyzet-felismerés által, a következő küldetésbiztosítási stratégiát és folyamatokat kell alkalmazni [122]:

(1) Elfogadható szintre csökkenteni a működési kockázatot.

(1a) Csökkenteni a működési kockázatot a folyamatok tervezése során.

(1b) A működési kockázat folyamatos kezelése a műveletek során.

(2) Megoldani a felmerülő problémákat.

(2a) A műveletek során felmerülő problémák megoldása.

Ezek azok a feladatokat, amelyek ellátására egy műveletben résztvevő TOC-nak képesnek kell lennie.

A holisztikus SA-megközelítés révén a különböző területekről származó információk – például a HUMINT, a GEOINT és az OSINT[58] – kombinálódnak a kibertér információival (többek között a TOC- információval, de akár a kereskedelmi vállalatok információival) a JSOC-ban. Ez a 14. ábra stratégiai észlelés része, amelyben a CTI[59] ugyanúgy helyet kap, mint a kockázatmenedzsment. A JSOC-nak képesnek kell lennie a CSA kérdéseire választ adni:

1 – Mi történik: van-e folyamatban lévő támadás a rendszer környezetében, vagy milyen erőforrások kerültek veszélybe? Mik az észlelt támadás hatásai? Ez a szakasz többnyire automatizált adatgyűjtő eszközöket és hatalmas mennyiségű összegyűjtött adat

[57] Mission assurance.
[58] Humán hírszerzés, geoinformációs hírszerzés, nyílt forrású hírszerzés.
[59] Cyber threat intelligence, kiberfenyegetettség felderítése.

előfeldolgozását foglalja magában. Az összegyűjtött adatok mennyisége és minősége meghatározza, hogy mennyire hatékonyan tud válaszolni erre a kérdésre.

2 – Miért történik: a rendszer környezetének megfigyelése a sebezhetőségek, biztonsági rések, biztonsági riasztások segítségével, hogy tisztában legyenek a lehetséges fenyegetésekkel és támadásokkal. Ezenkívül ez az elem a helyzet alakulásának mikéntjére is vonatkozik, beleértve a támadások nyomon követését, a támadási viselkedés és a stratégiák elemzését. Ebben a szakaszban több elemzési és értékelési technikát kell párhuzamosan alkalmazni.

3 – Mi történhet a jövőben: a lehetséges jövők előrejelzésének képességét jelzi, a valószínűségekkel és a kárpotenciál, a hatások előrejelzésével együtt. Tartalmazza az aktuális helyzetismeretet és annak alakulásának lehetőségét, valamint az ellenfelek viselkedésére vonatkozó ismereteket. Ez a kérdés az előrejelzés – vizualizáció része, amely olyan kérdésekre ad választ, mint hogy milyen helyzetek lehetségesek a jelenlegi rendszerkomponensek, biztonsági helyzet és fenyegetések alapján. Ezen túlmenően milyen lehetséges módokon alakulhat tovább a jelenlegi helyzet? [120:2]

„Amikor az információs előnyökről beszélünk, térjünk vissza ehhez a három dologhoz: lássuk magunkat, lássuk az ellenfelet, és lássuk az összes többi lényeges dolgot, ami történik” – mondta Stephen Fogarty altábornagy, a Hadsereg Kiberparancsnokságának parancsnoka. „Mert ha csak a kék [barátságos erők] és a vörös [ellenséges erők] mellett ragadunk, akkor lemaradunk minden másról, ami történik, ami óriási hatással lehet küldetésünk teljesítésének eredményére.” [123]

Ezek azok az információk, amelyeket egy döntéshozó parancsnok elé kell tárni művelet vagy misszió közben. Az adat- és információmennyiség túlterhelést okozhat, illetve a hatások pontos ismerete nélkül a döntéshozatal is akadozhat, ahogyan korábban írtam, sokszor visszaszorítva a kiberműveleteket a kommunikáció biztosítására. Érthetően nehéz integrálni a kinetikus műveletekbe a kiberműveleteket, és több projekt is fut annak érdekében, hogy közérthetőbbé váljanak a kibertér által nyújtott képességek és lehetőségek. Az egyik ilyen a jelenleg is fejlesztés alatt álló kiberhelyzetkép megértését[60] elősegítő vizualizációs eszköz.

A Cyber Situational Understanding program keretében 2019 óta fejlesztenek egy olyan, kifejezetten parancsnokok számára készült felületet, amely révén jobb betekintést kapnak a

[60] Cyber Situational Understanding

kiber- és elektromágneses környezetbe. A fejlesztés első szakaszának célja a baráti hálózat és az azt fenyegető veszélyek helyzetfelismerésének javítása. Szervezetileg a hadosztály és a hadtest az elsőbbséget élvező csoportok. A Cyber SU által kapott információk egy része egyébként is jellemzően magasabb (stratégiai) szintűek, így számukra az a kihívás, hogy azokat megfelelő szinten gyűjtsék össze, majd a lehető legalacsonyabb szinteken osszák meg [124]. A Cyber SU az első olyan program, amely kifejezetten egy webkompatibilis rendszerre fejlesztettek le, és célja a jelenlegi műveleti rendszereket és programokat egyetlen felhasználói felületben egyesíteni.

3.5 Nehézségek

Adatgyűjtési nehézségek [120:9]

- Az SA-rendszer tervezésének leglényegesebb részeként elmondható, hogy az adatgyűjtési folyamat még mindig túl sok nyersadattal dolgozik. Meg kell vizsgálni a költséghatékonyabb adatgyűjtést/szűrést és az adatok előfeldolgozását.
    - A különböző adattípusok más-más forrásból nyerhetők, ami bonyolultabbá teszi az adatgyűjtést, egyben nehezíti a valós idejű monitorozási képességeket.
    - A különböző források eltérő adatábrázolási formátumokat igényelnek, melyek együttes megjelenítése növeli az előfeldolgozás költségeit.
    - Az összegyűjtött és a további elemzéshez tárolt adatmennyiség folyamatos növekedése a rendszer túlterheléséhez vezethet.

A CSA-ként megjelenő irodalmak jelenleg csak részeredményeket adnak: a rendszerről és a fenyegetésekről gyűjtött nagy mennyiségű adat önmagában nem minősül SA-nak, ahogyan a felderítés és az adatmegosztás sem, hiszen azok még mindig csak adatforrások, ahogyan minden további/egyéb nyers vagy feldolgozott adat. Ahhoz, hogy egy adathalmaz valós CSA legyen, az elemzési és értékelési fázisokon is keresztül kell mennie [120:18].

3.6 Összegzés, rész-következtetések

Ebben a fejezetben bemutattam és elemeztem a légierő és a kiberműveletek kialakulásának hasonlóságait és különbözőségeit. A légierő gondolkodásmódja – a végtelen lehetőségről – hasonlít a kiberműveleti gondolkodáshoz, azonban nagyban eltérnek a kinetikus-nemkinetikus mivoltukban, legfőképp a hatások tekintetében. Ahogyan eleinte nehézséget okozott a hadsereg és a tengerészet parancsnokainak integrálni a légierő adta lehetőségeket, úgy

jelenleg a kiberműveletek is küzdenek azért, hogy megtalálják a helyüket az összhaderőnemi műveletekben. Amíg a légierő számára a stratégiai bombázás volt a függetlenségének megváltása, addig a kiberműveletek terén még várjuk az áttörést.

A kiberműveletek jobb megértését azonban több modell is elősegíti. Az egyik ilyen a kiberhelyzetkép modellje, amelynek alapja az ugyancsak a légierőtől származó helyzetkép modell. Azonban a légierő háromszintű modelljének eddig leginkább csak az első kettő szintjét sikerült a kiberteret illetően megvalósítani: az adatok gyűjtését és értelmezését. A harmadik szintet, a vizualizációt tekintve vannak kezdeményezések, azonban nehéz úgy prezentálni egy jelenlegi helyzetet (és jövőben várható eseményeket) akár térképen, akár diagramokon, hogy azok ne okozzanak információ túlterhelést. A kibertér mindenhol-levősége miatt ezért annak egyfajta leszűkítése zajlik az adott műveletet érintő fizikai entitásokra, elsősorban ezek (kiber) védelmére. Ennek megvalósítása szervezetileg – maradva a hármas felosztásnál – a következőképpen képzelhető el: egy stacioner blue team (SOC) megléte, egy műveleti területre kiküldhető TOC-csapat, és a legfelsőbb szinten egy JSOC/CSA-csapat, ezzel biztosítva a képességek túlélését.

Az elmúlt időszak megmutatta, hogy a hagyományosnak mondható cyber kill chain már nem teljesen fedi le az információs műveletekbe is belenövő kiberműveleteket. Emiatt tettek javaslatot az online műveletek kill chainjére, amely hibrid megközelítés. Figyelembe véve ezeket a tapasztalatokat, elképzelhető, hogy a kiber-helyzetképbe a jövőben az ún. brandmonitoringot is bele kell szerkeszteni, nyomon követve a döntéshozó személyek online jelenlétét bizonyítékul, hogy nem estek áldozatul online műveleteknek.

Az új technológiák és az ezeket felölelő katonai innovációs folyamatok mindig tartalmaznak bizonytalansági elemet. A kibertérnek azonban számos olyan tulajdonsága van, amely egyedivé teszi a történelmi katonai újítások között. Ezek közül ötöt emelek ki itt.

Először is, a kibertér nem szigorúan katonai technológia, és nem is létezik szigorúan katonai térben. A kibertér inkább globális, összekapcsolt rendszer és különféle kormányzati és nem kormányzati szereplők használják különféle célokra.

Másodszor, a kibertér lehetővé teszi olyan katonai hatások létrehozását, amelyek sem nem erőszakosak, sem nem tartósak. E hatások tolakodó, de nem erőszakos természete elkerüli a hagyományos jogi kategorizálást, és ezért megnehezíti a megfelelő súlyú válasz/ellencsapás adásának mérlegelését. A globálisan összefüggő terep ilyen kombinációja - az erőszakmentes hatások elérésének képességével - a kibertér harmadik egyedi jellemzőjéhez vezet: az állandó cselekvés feltételezése határozza meg. Más szóval, mind a kormányzati, mind a nem kormányzati szereplők állandó versengés-szerű kapcsolatban állnak egymással, és

folyamatosan próbálnak előnyt szerezni. A támadás és a védelem, illetve a háború és a nem háború közötti hagyományos katonai megkülönböztetés, bár fogalmilag még mindig hasznos, ilyen körülmények között a gyakorlatban pontatlan, sőt félrevezető leírást ad az ilyen típusú kibertevékenységről.

Negyedszer, az a tény, hogy a kibertér magából az információból – úgy az elektronikus rendszereket tápláló bitekből és bájtokból, mint pedig az ilyen rendszerek által előállított érthető tartalomból - álló tartomány, egyedülálló módon képessé teszi a kiberteret arra, hogy a hadviselés történetében példátlan léptékű narratívamanipulációt tegyen lehetővé.

Ötödikként, a új kommunikációs technológiák fejlődése és elterjedése az információtermelésnek és fogyasztásnak a decentralizálódásához vezetett. Ez a folyamat a fölötte gyakorolt hatalom megosztását eredményezte: a hagyományos, állami határokon és intézményeken túl magánszereplők is részesei lettek, és képessé váltak globális szintű hatást kiváltani, ami jelentős következményekkel jár a háborúk megvívására nézve. Az így létrejövő – tájékoztató forrásokban,/célpontokban gazdag - információs környezet lehetővé teszi a valós ismeretekért folyó küzdelem olyan új típusát, amelyben nehéz megkülönböztetni az igazat a hamistól – ezt a körülményt bizonyos hadseregek kimutathatóan jobban hajlandók/képesek előnyükre kihasználni, mint mások [54:8–9].

Jelen fejezet a [31] publikációmat dolgozta fel és egészítette ki.

4. Magyarország kiberképességei

4.1 Bevezetés

Az elmúlt fejezetek bemutatása után a hazai katonai kiberképesség helyzetét mutatom be. A kiberképességek olyan új gondolkodásmódot igényelnek, amelyek minden katonai szervezetet próbára tesznek. Az eljárásrendek és a hatások merőben mások, mint amelyek a katonaságról alkotott képben élnek. Azonban ez a megújulás – modernizáció, digitalizáció, „kiberesedés" – lehetőségeket is jelenthet: az, hogy másként gondolkodunk a haderőről, nem feltétletlenül jelenti azt, hogy rosszabbul.

Azonban a domén adta körülmények tekintetében egy sokkal szorosabb együttműködés szükséges mind a polgári oldallal, mind a piaci szereplőkkel. Ez az együttműködés azonban sokkal láthatóbbá, „kézzelfoghatóbbá" teheti a haderőt a civil szféra számára.

Hipotézisem az volt, hogy **a magyar katonai kiberképességek állapota megfelel a környező országok kiberképességei fejlettségének** azonban szükségesek a szövetségi gyakorlatok és jó-gyakorlatok a műveleti területen történő alkalmazáshoz.

Ahhoz, hogy ezt felmérjem, megnéztem a hazai doktrinális környezetet, megvizsgáltam a szervezeti átalakulásokat, és SWOT-analízist[61] végeztem el. Ennek célja az volt, hogy bemutassam a hazai kiberképességek fejlődési lehetőségeit.

A kutatáshoz a SWOT-elemzés módszertanát[62] használtam, és annak keretrendszerét vetítem le a hazai katonai kiberképességekről.

---

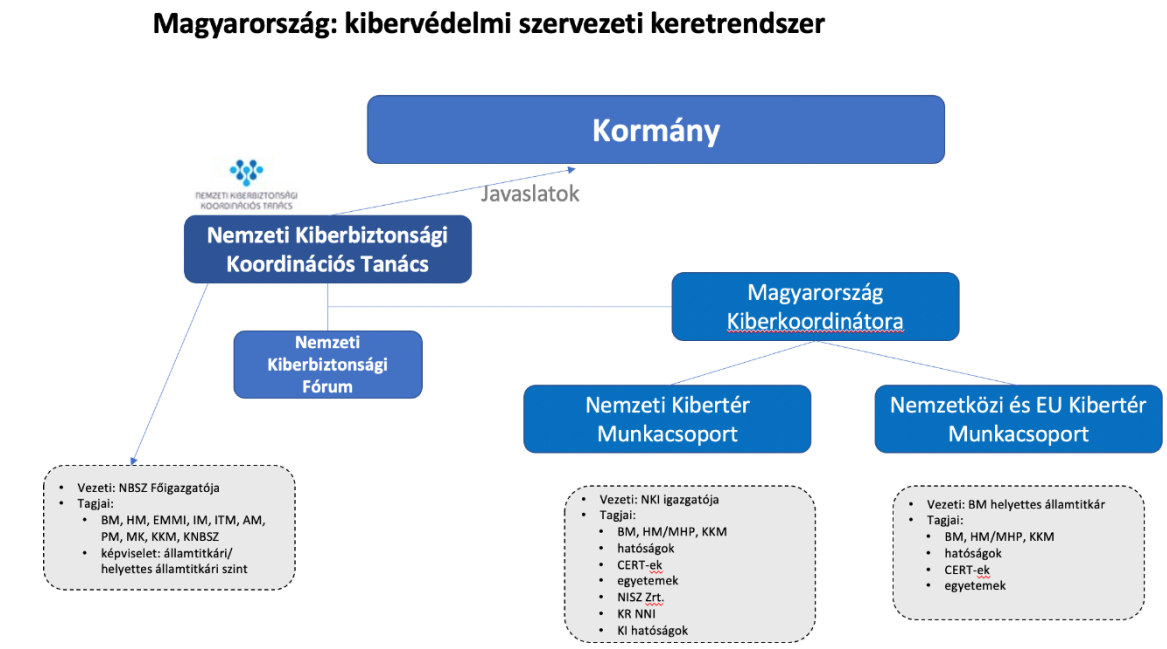
[61] SWOT-analízis: egy adott entitás erősségeinek (strength), gyengeségeinek (weakness), lehetőségeinek (opportunity) és kockázatainak (threat) megbecsülése, feltárása.

[62] Az erősségek, gyengeségek, lehetőségek és veszélyek (SWOT) elemzése alapvető eszközzé vált a szervezetek számára, hogy értékeljék piaci pozíciójukat, és széles körben használják a szervezetek belső és külső környezetének elemzésére. Az erősségek a szervezet azon belső elemeire utalnak, amelyek elősegítik céljainak elérését, míg a gyengeségek azokat a belső elemeket, amelyek megzavarják a szervezet sikerét. A lehetőségek – olyan külső szempontok, amelyek segítik a szervezetet céljai elérésében – nemcsak pozitív környezeti szempontok, hanem lehetőségek a hiányosságok kezelésére és új tevékenységek kezdeményezésére. Másrészt a fenyegetések a szervezet külső környezetének olyan aspektusai, amelyek akadályok vagy potenciális akadályok a céljai elérésében.
A SWOT elemzés egyik legfontosabb képessége, hogy a belső és külső tényezőket párosítja, ezáltal egy könnyen értelmezhető stratégiai mátrixot biztosít. Fontos megjegyezni, hogy a belső tényezők a szervezet ellenőrzése alatt állnak, például a pénzügy vagy a szervezeti kultúra, míg a külső tényezők, mint a gazdasági tényezők, az új technológiák, versenytársa kívül esnek a szervezet hatáskörén. A SWOT elemzés elsődleges célja a döntéshozatal elősegítése, azonban a módszernek vannak korlátai, mint a priorizálás lehetőségének hiánya, az általános megfogalmazás, súlyozás hiánya, és az ezekből eredő szubjektivítás. Mindezen korlátok mellett

A fejezetet a szokásos irodalmi áttekintéssel kezdem, majd bemutatom a SWOT-analízis módszertanát (4.2. fejezet), valamint a keretrendszert (4.3.). A fejezet végén levonom a részkövetkeztetéseket, és bemutatom a részeredményeket.

4.2 Szakpolitikai és jogi keretrendszer

A szakpolitikai keretrendszer felépítése szintekre tagozódik, mely ezen a szakterületen a Nemzeti Biztonsági Stratégia (NBS). Ez határozza meg a nemzeti értékeket, érdekeket, írja le a nemzetközi biztonsági környezetet, az abból fakadó kihívások és veszélyeket és fogalmazza meg a célokat. Ebből eredeztetődnek le a szakpolitikai stratégiák, mint amilyen a Nemzeti Katonai Stratégia és a Nemzeti Kibervédelmi Stratégia. Ezek lefordítják az NBS-ben megfogalmazott kihívásokat, veszélyeket, célok ágazati szintre, valamint azokat az ágazati szervezetrendszerhez allokálják. Ezek után jelennek meg ezek a törekvések a jogszabályokat, rendeletekben, szabályzókban, a gyakorlatban.



19. ábra Magyarországi kibervédelmi szervezetek, koordináció [125]

népszerű módszer maradt, és egy szervezet *pillanatképének* bemutatására egyszerűség és átfogósága okán alkalmas.

A magyarországi kibervédelmi szervezetek és azok koordinációja igen sokrétű, 2013-ban, majd 2015-benkomoly átszervezés ment végbe ezen a téren. Számos kérdésre megadták a választ egy új törvénnyel, mint például hogyan valósul meg a kibervédelemmel kapcsolatos feladatok tárcaközi koordinációja a kormányzaton belül, vagy mely testület látja el a feladatot és milyen jogkörök gyakorlásán keresztül. Mindezek legfontosabb forrása a 1139/2013. (III. 21.) Korm. Határozat, 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. [126]

A legtisztább tárcaközi koordináció a Nemzeti Kiberbiztonsági Koordinációs Tanács keretében valósul meg. Ennek a szervezetnek a kialakításért a Kormány 2013-ban a Miniszterelnökséget vezető államtitkárt bízta meg a Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat 2. pontjában [2]. A Nemzeti Kiberbiztonsági Koordinációs Tanács (továbbiakban: Tanács) létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatásköréről a 484/2013. (XII. 17.) Korm. rendelet foglalkozik részletesen. Ezen rendelet 1. § (2) bekezdése tételesen meghatározza a Tanács tagjait, amely lefedi az adott kormányciklus összes minisztériumát. Ezen minisztériumok 239/2022 (VI.30.) Korm. Rendelet által módosított felsorolása a következő:

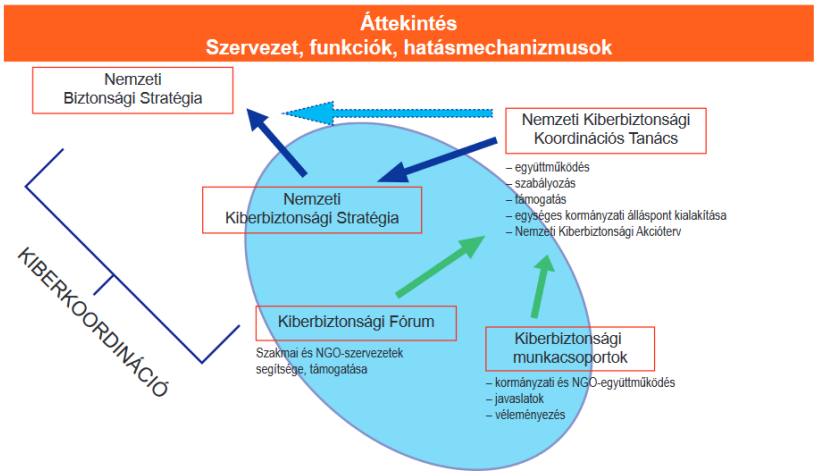
A belügyminiszter által delegált 1 fő, az építési és beruházási miniszter által delegált 1 fő, a honvédelmi miniszter által delegált 1 fő, az igazságügyi miniszter által delegált 1 fő, a külgazdasági és külügyminiszter által delegált 1 fő, a kultúráért és innovációért felelős miniszter által delegált 1 fő, a pénzügyminiszter által delegált 1 fő, az agrárminiszter által delegált 1 fő, a Miniszterelnökséget vezető miniszter által delegált 1 fő, a technológiai és ipari miniszter által delegált 1 fő, a gazdaságfejlesztési miniszter által delegált 1 fő, a területfejlesztési miniszter által delegált 1 fő, a Miniszterelnöki Kabinetirodát vezető miniszter által delegált 2 fő.

A Tanács feladata a Magyarország Nemzeti Kiberbiztonsági Stratégiájában meghatározott cselekvési területeken a kormányzati tevékenység koordinációjának elősegítése és a végrehajtás figyelemmel kísérése. A szervezeti ezt különböző munkacsoportok megalakításával kezeli, ezek a következők: eseménykezelő, belbiztonsági, e-közigazgatási, energetikai és gyermekvédelmi munkacsoport.

A 2013. évi L. törvény, mely az állami és önkormányzati szervek elektronikus információbiztonságáról szól, szintén nevesít bizonyos minisztereket, de csak az ellátott feladatkör alapján. A nevezett miniszterek között szerepel a honvédelmi miniszter, az e-közigazgatásért felelős miniszter, az informatikáért felelős miniszter, a minősített adat védelmének szakmai felügyeletéért felelős miniszter, a katasztrófák elleni védekezésért felelős

miniszter, a polgári nemzetbiztonsági szolgálatok irányításáért felelős miniszter, a közigazgatás-fejlesztésért felelős miniszter, az adópolitikáért felelős miniszter, valamint a központi szolgáltatók felett felügyeletet gyakorló miniszter.

Ez a felsorolás a 2023-as kormányalakításnak megfelelően a Honvédelmi Minisztériumot, a Miniszterelnöki Kabinetirodát, a Miniszterelnökséget, a Belügyminisztériumot és a Pénzügyminisztériumot fedi le. A felsorolt minisztériumok alapján látható, hogy ez egy szűkebb körű koordináció, és inkább az elektronikus információs rendszerek védelmével kapcsolatban hozott normatív utasítások körét hivatott rendezni. -[126]



20. ábra: A magyarországi kibervédelmi struktúra szervezeti, funkcionális és hatásmechanizmusai. Forrás [127]

Mely minisztériumhoz tartozik a kibervédelmi feladatok kormányzati koordináció irányítása? A 484/2013. (XII.17.) Korm. rendelet alapján a Nemzeti Kiberbiztonsági Koordinációs Tanács elnöke a Nemzetbiztonsági Szakszolgálat vezetője, a Nemzetbiztonsági Szakszolgálat irányítása pedig a 182/2022. (V. 24.) Korm. rendelet 1. mellékletének B) pontjában található táblázat szerint a Miniszterelnöki Kabinetirodát vezető miniszter feladatai közé tartozik. Ez alapján kijelenthetjük, hogy a kormányzati koordinációt jelenleg a Miniszterelnöki Kabinetirodát vezető miniszter irányítja - ez egyébként abban is megnyilvánul, hogy, amennyiben Tanács elnökét valami akadályozza feladata ellátásban, úgy a Miniszterelnöki Kabinetirodát vezető miniszter által megbízott kiberkoordinátor (a továbbiakban: kiberkoordinátor) helyettesíti. (484/2013. (XII.17.) Korm. rendelet 1. § (1))

A kibervédelem egyik legfontosabb szerve a Nemzeti Kibervédelmi Intézet (továbbiakban: NKI), ami egyben lát el hatósági és incidenskezelési feladatokat. Közigazgatási hatósági hatáskörét az 2013. évi L. törvény és 2001. évi CVIII. törvény határozza meg. Az NKI

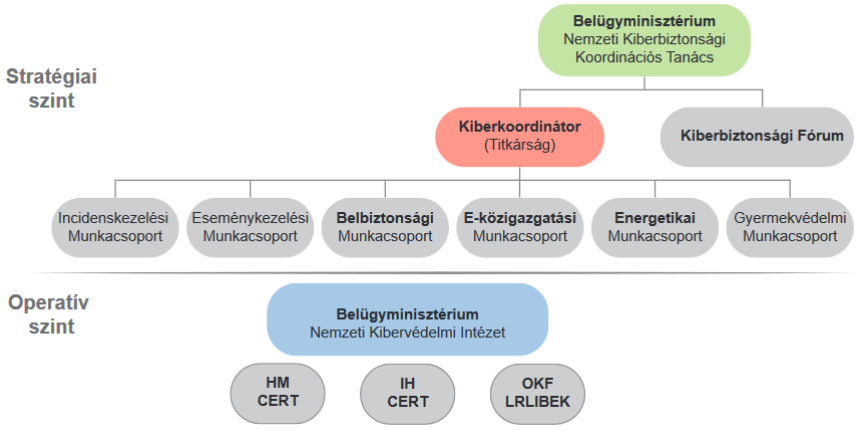
hatósági feladatai mellett az információs rendszerek informatikai támogatását (országosan) és sérülékenységmenedzsment feladatait látja el.

Az NKI a Nemzetbiztonsági Szakszolgálat szervezetén belül helyezkedik el, mely Szakszolgálat jelenleg a Miniszterelnöki Kabinetirodát vezető miniszter irányítása alatt áll. A Nemzetbiztonsági Szakszolgálat egyben az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóságként is működik. Feladatait részletesen a 187/2015. (VII. 13.) Korm. rendelet a 6. § - 10. § terjedően sorolja fel.

Hatóságként jelenik meg az NKI mellett a Szabályozott Tevékenységek Felügyeleti Hatósága is, melynek feladata a kiberbiztonság felügyelete. A Kormány évente elfogadja a Nemzeti Kiberbiztonsági Koordinációs Tanács által előkésztett Nemzeti Kiberbiztonsági Akciótervet. Meg kell említeni a Honvédelmi miniszter és a Kormány irányítása alatt álló Magyar Honvédség Kiber- és Információs Műveleti központját is, ami kiberhadviselés során kap fontos szerepet.

A kibertámadások elhárításának kérdésköre jellemzően utólagos reakciókra és értékelésekre épül. Az Ibtv. által felépített ciklus, ami a megelőzés, korai figyelmeztetés, észlelés, reagálás és biztonsági esemény kezelés, majd visszacsatolás lépésekre épít, szintén ezt próbálja szemléltetni. A tény, hogy a Nemzeti Kiberbiztonsági Koordinációs Tanács évente terjeszt elő akciótervet a Kormány számára, mindenképp hatékonyságra utal - nevezhetjük ezt akár gyakorinak is egy adott elektronikus információs rendszer felülvizsgálatára vonatkozóan, azonban ezek még mindig csak a stratégiák és tervezés szintjén mozog. [128]

Első körben maga a kibervédelem, mint tevékenység a Nemzeti Kibervédelmi Intézetre hárul, amely azonban csak utólagos bejelentésekre reagálva tud cselekedni. Saját kutatási munkája és sajtófigyelése alapján ad ki ugyan figyelmeztetéseket, hatóságként kérelemre különböző eljárásokat is tud folytatni törvény által kijelölt hatáskörében, ezek a tevékenységek azonban ritkán vezetnek megelőzéshez, vagy akár korai figyelmeztetéshez. A leghatékonyabb szabály talán az, hogy bizonyos szolgáltatásokat ért kibertámadás esetén az érintett szolgáltató köteles bejelentést tenni az NKI számára (felhőszolgáltatás, keresőmotorok, online piactér). [129]



21. ábra: A hazai kibervédelmi struktúra 2015 után. Forrás: [127]

Másik oldalról minden központi és államigazgatási szervnek/szervezetnek megvan a saját elektronikus információs rendszere, ezt kell figyelnie és karban tartania. Mivel a legújabb szabályozások megszüntették a 2015 előtti intézményi széttagoltságot, nem feltétlenül tudunk összehangolt reakcióról beszélni. A Nemzeti Kibervédelmi Intézeten kívül a Magyar Honvédség Kiber- és Információs Műveleti Központja képes még reagálni, de ezt a tevékenységet már kiberhadviselésként kategorizáljuk. A fentieket figyelembe véve, közigazgatási szinten nem tudunk összehangolt reakcióról beszélni, de ez nem a szabályozások hibájából ered, hanem az elektronikus információs rendszerek és a kibertámadások természetéből.

Fontos szereplő még a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), amely Magyarország adatvédelmi és információszabadságért felelős szervezete. Feladata az adatvédelemmel kapcsolatos jogszabályok betartatása, valamint az adatvédelmi incidensek kezelése és a kibervédelemmel kapcsolatos tanácsadás. Természetesen a Rendőrség Kibervédelmi Osztálya is fontos szerepet tölt be a kibertér védelmében.

2021. december 31-ig a 32/2021 (július 23 -i) HM utasítással összhangban az MH (Magyar Honvédség) Polgári -katonai Együttműködési és Pszichológiai Műveleti Központot mint költségvetési szervet megszüntetik az MH katonai kibertér operatív képességeinek javítása érdekében. Utódszervezetként új szervezet jön létre az MH Tiszthelyettesi Akadémia szervezeti elemeinek összevonásával, amely a továbbiakkal kapcsolatos döntés-előkészítést végzi. Az MH PK 2022. január 1-jével új költségvetési szervet hozott létre Szentendrén, amely MH Kiber- és Információs Műveleti Központ néven működik majd, és közvetlenül alárendeltje lesz.

Magyarországon - véleményem szerint - a kibervédelem és az információs műveletek irányításának integrált megközelítése nagy előnyökkel járhat. Ez a megközelítés proaktív jellegű, célja a kiberbiztonsági intézkedések és technológiák fejlesztése annak érdekében, hogy

a potenciális fenyegetéseket még azok bekövetkezése előtt felismerjék és kezeljék. A fő cél a létfontosságúnak ítélt rendszerek védelme a támadások ellen és ellenálló képességük megerősítése.

A kiberbiztonság megerősítése érdekében a szervezeteknek és a magánszemélyeknek növelniük kell tudatosságukat, fel kell készülniük a potenciális fenyegetésekkel szembeni fellépésre. A személyzet és a felhasználók oktatása, valamint a szervezeten belüli kiberbiztonsági kultúra meghonosítása kulcsfontosságú lépések az integrált megközelítés kialakításában. Emellett elengedhetetlen a nemzetközi együttműködés is; a kibervédelmi szervezeteknek és a különböző iparágaknak együtt kell működniük, és gyorsan információt kell cserélniük a felmerülő fenyegetésekről. Ezekben a feladatokban játszik igen fontos szerepet többek között az NKI és társszervezetei.

A biztonságos információs rendszerek kiépítése és fenntartása érdekében a Nemzeti Kibervédelmi Intézet a kiberbiztonság szervezeti, szabályozási és jogszabályi szempontú erősítésén dolgozik. Az NKI céljai közé tartozik az alapvető kiberbiztonsági stratégiák és szakpolitikák kidolgozásának elősegítése, a kibervédelmi műveletek hatékony keretének megteremtése, valamint a kiberfenyegetések elleni védekezéssel foglalkozó különböző szervezetek közötti optimális koordináció és együttműködés biztosítása. [129]

A Nemzeti Kiberbiztonsági Intézet (NKI) a legújabb kiberfenyegetések felderítésére, elemzésére és az azokra való reagálásra törekszik a potenciális kiberincidensek szoros figyelemmel kísérésével és értékelésével, hogy a sebezhetőség fő forrásait feltárja és a szükséges biztonsági intézkedéseket bevezetesse. Az NKI több nemzeti és nemzetközi szervvel is együttműködik a kibervédelemmel kapcsolatos információk, tapasztalatok és erőforrások megosztása érdekében.

22. ábra: NKI szervezeti felépítése. Forrás:[129]

A Nemzeti Kiberbiztonsági Intézet a kiberbiztonsági iparág hazai szintű védelmén és fejlődésének előmozdításán dolgozik. Ezt úgy éri el, hogy támogatást nyújt a területen működő start-up vállalkozásoknak és vállalatoknak, segíti a hazai kiberbiztonsági szolgáltatások

körének bővítését és új termékek gyártását, valamint növeli nemzetközi versenyképességüket. Ezzel az NKI nemcsak a biztonsági fenyegetésekkel szemben védekezik, hanem a gazdaságot is ösztönzi.

Nagy jelentőséget tulajdonít a kritikus infrastruktúrák biztonságának is. Ennek elősegítése érdekében a kiberbiztonság kritériumainak megteremtésén és a hatékony védelmi eljárások meghatározásán dolgoznak. Az NKI emellett elkötelezett amellett, hogy támogatást nyújtson a létfontosságú infrastruktúrákkal rendelkező szervezeteknek a kiberbiztonsági gyakorlatok bevezetésében és a kibertámadásokkal szembeni védekező készségek kialakításában.

Itt látható az a csoportos felosztás, ami szerint a magyar kibervédelmi szervezetek dolgoznak, az NKI nemzetközi partnerei:

ENISA: European Network and Information Security Agency,5
FIRST: Forum of Incident Response and Security Teams,6
TI: Trusted Introducer,7
IWWN: International Watch and Warning Network,
CECSP: Central European Cyber Security Platform (a visegrádi négyek és Ausztria kiberbiztonsági szervezeteit tömörítő platform).

Az Ibtv (és az elektronikus információbiztonságra vonatkozó rendelkezéseket tartalmazó egyéb vonatkozó jogszabályok) alapján ellenőrzik , hogy a szervezetek megfelelnek-e a szükséges követelményeknek. Ezen túlmenően döntő szerepet játszik annak biztosításában, hogy a központilag vagy uniós forrásokból finanszírozott IKT - projektek fejlesztése során az elektronikus információs rendszerek teljes életciklusa során teljes mértékben és következetesen betartsák ezeket a rendelkezéseket. [127]

A Nemzeti Elektronikus Információs Hatóság (NEKH) feladat - és hatáskörét az Ibtv. és a 187/2015 (VII. 13.) Korm. rendelet állapítja meg és határozza meg, amely meghatározza az elektronikus információs rendszerek biztonsági felügyeletéért felelős hatóságok, valamint az információbiztonsági felügyelő feladatait, és meghatározza a zárt elektronikus információs rendszerek fogalmát.

Az OKF Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központról is érdemes szólni. Az Országos Katasztrófavédelmi Főigazgatóságon (OKF) működik a Kritikus Rendszerek és Létesítmények Informatikai

Biztonsági Eszközkezelő Központja (LRLIBEK), amely a nemzeti kritikus rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági intézkedésekért felelős, kivéve az Ibtv. hatálya alá tartozó szervezetek által üzemeltetett rendszereket és létesítményeket.

Az elektronikus információs rendszerek biztonsági felügyeletéért felelős hatóságok feladat- és hatásköréről, valamint a zárt elektronikus információs rendszerek meghatározásáról szóló 185 /2015 (VII. 13) és 187/2015 (VII. 13) Kormányrendelet alapján az LRLIBEK főbb feladatai meghatározásra kerültek. Az eseménykezelés a 185/2015. (VII. 13.) Korm. rendelet alapján történik. A biztonsági eseményekkel kapcsolatos feladatok között szerepel a nyilvántartás vezetése, az érintettek azonnali értesítése, szakmai támogatás nyújtása, együttműködés a hatóságokkal és az érintett szervezetekkel, valamint a kezelésükre vonatkozó tájékoztatók készítése.

A szervezet folyamatosan elérhető, 24 órás ügyeletet működtet. Tájékoztatást nyújt a sérülékenységekről és a fenyegető kockázatokról. Rendszeresen elvégzi a magyar kibertér biztonsági helyzetértékelését. A szervezet részt vesz a hazai és nemzetközi információbiztonsági és kibervédelmi gyakorlatok tervezésében és szervezésében. Szakértői-oktatói és tudatosító tevékenységet végez. Az információtechnológiai, hálózatbiztonsági és biztonságiesemény-kezelési együttműködési fórum működtetése is a feladatai közé tartozik.

Végezetül röviden visszatérnék a már említett A hazai kibervédelem rendvédelmi szervezetére, a Készenléti Rendőrség Nemzeti Nyomozó Iroda (KR NNI) Kiberbűnözés Elleni Főosztályra. [130]

A rendőrség az alaptörvények, például a rendőrségről szóló 1994. évi XXXIV. törvény és az említett törvényt támogató egyéb kapcsolódó jogszabályok keretein belül gyakorolhatja a velejáró bűnügyi nyomozati hatásköröket, megelőzheti, megakadályozhatja és felderítheti a bűncselekményeket, valamint visszaszerezheti a bűncselekmények következtében elvett vagyontárgyakat. A rendőrség aktívan küzd a számítógépes bűnözés minden formája ellen, különösen a számítógépes rendszerek elleni támadások, a rosszindulatú szoftverek, az adathalászat, az online csalások, az elektronikus banki csalások , a hitelkártyacsalások és a kiskorúak internetes kizsákmányolása ellen.

Összefoglalva, a különböző intézmények közötti együttműködés elengedhetetlen a kiberbiztonság biztosításához és növeléséhez, amit az információs és kiber műveletek hatékony felügyeletének szükségessége is bizonyít. Az együttműködés tehát elengedhetetlen a modern társadalmakban ezen erőforrások megfelelő kezelése érdekében. A biztonságos kiberkörnyezet biztosítása a magyarországi polgárok és vállalkozások számára a képzés és a tudatosság folyamatos fejlesztését, valamint a hatékony incidenskezelést igényli. A változó

kiberfenyegetésekhez való alkalmazkodás és az új technológiák kihasználása fontos tényezők a sikeres védelmi stratégiák kialakításához. Ezáltal biztosítható, hogy a magyar kibertér biztonságos és ellenálló maradjon.

4.2.1 Hazai kibertörténelem stratégiai szinten

A hazai stratégiai dokumentumokban 2012-ben fogalmazódott meg a kibertér fenyegetéseivel szembeni védelem fontossága, és megjelent a kibertér hadszíntérként való meghatározása is [51]. A 2011. évi CXIII. tv. módosításával [131] [132] a (katonai) kibertér törvényi szinten is megjelent a jogrendben. A magyar katonai kiberképességek kialakításának fő hazai kereteit a Nemzeti Biztonsági Stratégia [2], a Nemzeti Katonai Stratégia [133], a Nemzeti Kibervédelmi Stratégia [51], a Honvédség Kibervédelmi Szakmai Koncepciója [134] és a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program [135] jelölik ki, míg NATO-szövetségi szinten a 2016-os Varsói Csúcstalálkozón elfogadott kibervédelmi vállalások adják. A 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről kijelöli a Honvédség kiberképességeinek és műveleteinek alkalmazási, illetve fejlesztési területeit [131]. A 2012. évi Nemzeti Biztonsági Stratégiában [2] jelenik meg a kiberbiztonság, mint Magyarország biztonságát meghatározó tényező [135:233], ebből eredően az e térből fakadó fenyegetések és kockázatok kezelése az állam feladata. A 2020. évi új Nemzeti Biztonság Stratégiának a kiberbiztonságot érintően legfigyelemreméltóbb eleme a 101. pont, amely kijelenti, hogy *„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”* [2:2110].

A 2012. évi Nemzeti Katonai Stratégiában is megjelenik a kibertér, kiberbiztonság fogalma, azonban egy lépéssel tovább menve utal a kiberhadviselésre is: „a kiberfenyegetésnek a hagyományos fenyegetésektől eltérő jellemzői szükségessé teszik a háborúval kapcsolatos fogalmaink átfogó felülvizsgálatát és adott esetben módosítását” [137:234]. Konkrét feladatként fogalmazza meg a dokumentum az MH tekintetében a Honvédség kibervédelmének erősítését, a rendszabályok kidolgozását, a megfelelő eszközök beszerzését és az állomány felkészítését [136:236], azonban ennek keretei csak később valósulnak meg.

A 2013. évi Nemzeti Kibervédelmi Stratégia utal elsőként a magyar kibertérre, mint fogalomra: „Magyarország kibertere a globális kibertér elektronikus információs rendszereinek

azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett" [51:3. pont]. A feladatokat tekintve kijelenti, hogy „a meglévő és potenciálisan jelentkező kihívásokkal szemben ki kell alakítani egy hatékony megelőző-, észlelési, reagálási képességet, amelybe a kibertámadások esetleges bekövetkezése esetén a helyreállítási képességek is bele kell, hogy tartozzanak" [16:9.pont]. Ez utóbbihoz kapcsolódóan konkrétabb feladatszabásként jelenik meg a kiberbiztonságot illetően a kormányzati koordináció és együttműködés erősítése, a megfelelő szakintézmények kialakítása, aktív részvétel a nemzetközi együttműködésekben, a kiberbiztonság jobb megjelenítése az oktatásban.

A kibertér védelmével kapcsolatos katonai érdekek azonosítása és szervezeti válaszok keresése a kormányzati stratégiák megjelenése előtt, 2011-ben kezdődött. 2011-ben miniszteri utasítás [137] került kiadásra a feladatokról, majd 2013-ban adták ki a Magyar Honvédség Kibervédelmi Szakmai Koncepciót [138]. Ugyanebben az évben határozták meg a honvédelmi ágazati eseménykezelési és hatósági struktúráját [139]. 2016-ban kerültek az ágazati elektronikus információbiztonsági hatósági felügyeleti feladatok [140] a KNBSZ[63] alá. 2017-ben a jogszabályok szerinti eseménykezelésre, sérülékenységvizsgálatra és hatósági feladatokra vonatkozó ágazati követelmények részletes meghatározása érdekében HM utasítást adtak ki [131]. A Hvt. 2018-as módosításában megjelent a Honvédség feladatai között a kibertér védelme, illetve ezzel kapcsolatban a szövetségesi, nemzetközi együttműködési kötelezettség [131]. Ez a változás a szövetségi keretrendszernek megfelelően kijelentette, hogy a kibertér műveleti területként kezelendő. Új feladatként jelent meg a „honvédelmi veszélyhelyzet" fogalom, amikor a Kormány elrendelheti a honvédségi szervezetek kibertérműveleti erők tevékenységeinek fokozását. 2019-ben megjelentek a katonai kibertérműveletekre vonatkozó különös szabályok (eljárásrend, a kibervédelmi ügyeletes parancsnok feladatköre) [131: 37. §. (5) d. pont, 62/A (1–8).].

2019-ben Szentendrén indult útjára a Kiberakadémia, amelynek fő profilja a tudatossági és szakmai képzések, valamint 2021-től elkezdte munkáját a Kiberműveleti Központ Előkészítő Osztály [141]. 2021-ben szintén megjelent az új Nemzeti Katonai Stratégia [142], és megújult a Nemzeti Kiberbiztonsági Koordinációs Tanács [143] is. 2022. január 1-jével megalakult a

[63] Katonai Nemzetbiztonsági Szakszolgálat

Magyar Honvédség Kiber- és Információs Műveleti Központ [144], valamint 2022. november 1-jével, a Magyar Honvédség átalakítása nyomán, megalakult a Magyar Honvédség Kiberműveleti Parancsnoksága [145].

4.2.2 Doktrinális háttér

Az új, 2020. évi Nemzeti Biztonsági Stratégia (NBS) [2] kiemeli, hogy Magyarország és a magyar állampolgárok mindenoldalú […] információs és kibertérbeli – biztonsága *alapvető érték.* Kiemeli a honvédelmi és rendvédelmi erők szoros *együttműködés*ének fontosságát egymással és a releváns polgári infrastruktúrával, és hogy az új biztonsági kihívások miatt *folyamatosan szükséges fejleszteni* a [...] kiberhadviselés elleni védekezés rendszerét. Az információbiztonság *tudatosság*ának alacsony szintjére is felhívja a figyelmet, és megállapítja, hogy a kibertér ma már […] *külön műveleti tér*nek számít.

Az egyik legfontosabb eleme az NBS-nek, hogy „Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes *kiberképesség*eket fegyvernek, alkalmazásukat fegyveres agressziónak tekinti, amelyre a fizikai térben megvalósuló válaszadás is lehetséges” [2], mindazonáltal kitér a kiberműveletek (támadások) attribúciós nehézségeire is.

A honvédelemmel kapcsolatosan ismételten kiemeli a kiberteret, mint műveleti területet, és a „katonai kibervédelmet növekvő mértékben alkalmassá kell tenni a haderő kinetikus műveleteinek kibertérbeli támogatására, ki kell alakítani a kiberműveletekben alkalmazható *offenzív képesség*eket. Ennek érdekében fejleszteni kell a Magyar Honvédség kibervédelmi és kiberműveleti erőit” [2], pontos irányvonalat kijelölve ez által. Nagy lépés, hogy megjelenik az offenzív képességek fontossága. Továbbá elsődleges feladatként tekint többek között (...) a *kormányzati koordináció* erősítésére, a kibertér *jogi szabályozás*ának fejlesztésére, (…) valamint a kiberbiztonsággal kapcsolatos *nemzetközi együttműködés* bővítésére [2].

Kovács László összefoglalója alapján elmondható, hogy a stratégiában markánsan megjelenik a Magyar Honvédség kibertéri szerepe és annak feladatai is, meghatározza, hogy a fejlesztések kibervédelmi (defenzív) és kiberműveleti (offenzív) erőinek alkalmasnak kell lenniük a kinetikus erők műveleteinek támogatására is. Ezen főbb irányvonalak megadása után szükséges a végrehajtást elősegítő ágazati stratégiák átalakítása, létrehozása, amelyek tükrözik ezeket a fejleményeket. Ilyen a 2021. évi Nemzeti Katonai Stratégia, illetve az előkészület alatt

álló Nemzeti Kiberbiztonsági Stratégia, amelyekben megjelenik a katonai kiberműveleti képességek helye és szerepe [145:4]. A katonai stratégia a katonai végcélok, a katonai módszerek és a végrehajtásra biztosított katonai eszközök együttese.

A 2021. évi Nemzeti Katonai Stratégia [133] (NKS) meghatározza, hogy a hagyományos (katonai, gazdasági, politikai, társadalmi és környezeti) biztonsági elemek mellett azt a kiber- és az információs dimenziók is alkotják [142]. Ahogyan az NBS-ben, úgy itt is megjelenik az a fajta szemlélet, hogy a hazánk „fizikai biztonságát veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat pedig akár *fegyveres támadásnak tekinti*, amelyre adott esetben katonai válaszadás is lehetséges" [142], amelyhez szükséges többek között a kibertér eszközrendszereinek fejlesztése. A *katonai kibertérműveleti erők* a kibertérben végrehajtott (offenzív vagy defenzív) műveleteikkel támogatják a haderőnemeket, és aktívan közreműködnek a nemzeti kibervédelmi feladatokban.

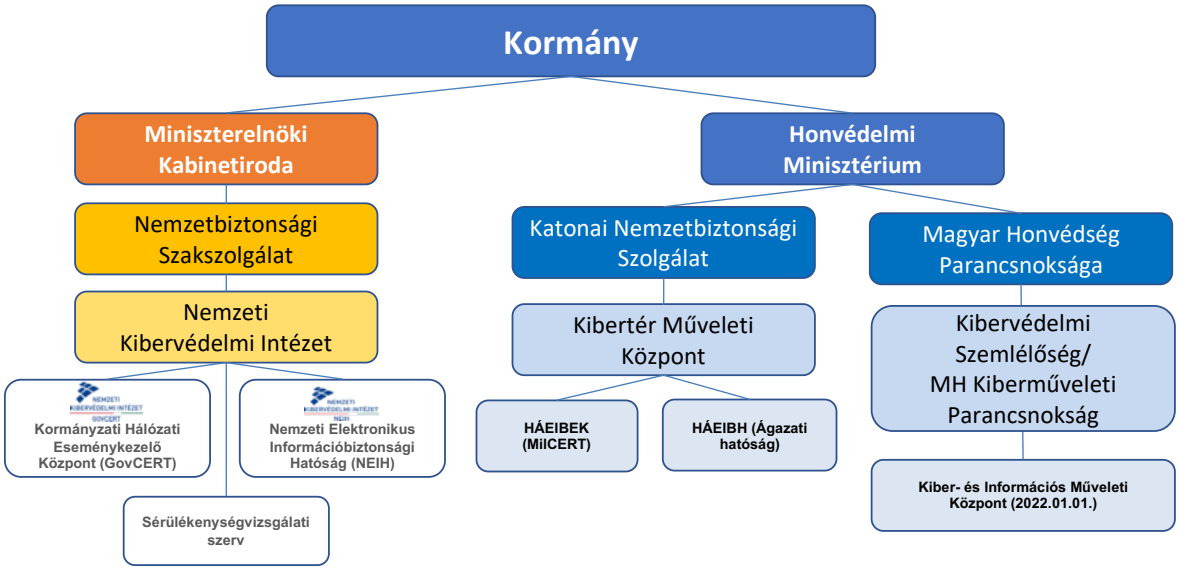
4.2.3 Szakpolitikai keretrendszer

Mindamellett, hogy a NATO mindig is védte az információs és kommunikációs rendszereit, a 2002. évi prágai csúcstalálkozón került először napirendre a kibervédelem ügye, miszerint a Szövetségnek *meg kell erősítenie a kibertámadások elleni védekezési képességeit.* A 2014. szeptemberi walesi csúcstalálkozón jóváhagyták az új kibervédelmi szakpolitika irányvonalait és az ahhoz kapcsolódó cselekvési tervet. Ezek mellett a kibervédelmet a NATO alapvető kollektív védelmi feladatának részeként ismerték el, amelyre a nemzetközi jog alkalmazandó. A 2016-os varsói csúcson a kiberteret műveleti területként ismerték el, kiemelve a szövetség védelmi jellegét, és hangsúlyozva, hogy a kibertérben ugyanolyan hatékonyan kell tudnia megvédenie magát a Szövetségnek, mint a többi műveleti térben. Ezen a csúcstalálkozón fogadták el az úgynevezett Kibervédelmi Vállalások csomagot is, amelyben a tagállamok vállalták, hogy nemzeti kibervédelmüket, beleértve a hálózatokat, infrastruktúrákat, erőforrásokat, együttműködéseiket, oktatást és képzést, erőteljesen fejlesztik.

2017-ben a szövetséges védelmi miniszterek jóváhagytak egy frissített kibervédelmi cselekvési tervet a kibertér műveleti területté való fejlesztéséről. 2018-ban a brüsszeli csúcstalálkozón döntöttek arról, hogy az európai műveleti parancsnokságon belül (NATO SHAPE) létrehozzák a kiberműveleti központot (*Cyber Operational Center* – CyOC), amelynek feladata a NATO kiberműveleteinek koordinálása. Jens Stoltenberg NATO-fő- titkár

egy 2019-es cikkben pontosította, hogy „egy súlyos kibertámadás kiválthatja az 5. cikkelyt a kollektív védelemről (amely értelmezés szerint egy szövetséges tagállam elleni támadást a teljes szövetség elleni támadásként értelmez) – ez egyben ellenlépéseket is feltételez”.[64]

Az elmúlt években kialakult a hazai kiberbiztonságért felelős szervezeti rendszer, amely alapvetően két szintre bontható: stratégiaira és operatívra. A stratégiai szinten a Kiberbiztonsági Fórum, a kiberkoordinátor, valamint az általa vezetett munkacsoportok találhatók, míg az operatív szintet – több esetben hatósági funkciókkal is kiegészülve – a Nemzetbiztonsági Szakszolgálat keretein belül működő Nemzeti Kibervédelmi Intézet (NKI), az Országos Katasztrófavédelmi Főigazgatóság szervezetében található Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (LRLIBEK), a Honvédelmi Minisztérium és az Információs Hivatal saját hálózatbiztonsági vészhelyzeteket elhárító csoportjai (Computer Emergency Response Team, a továbbiakban: CERT) alkotják [127]. A katonai oldalról látható, hogy két nagyobb szervezet felel a Honvédelmi Minisztérium felügyelet alatt a katonai kibervédelemért: a KNBSZ, mint hatósági ágazati szereplő, és a Magyar Honvédség Parancsnoksága (MHP) irányítása alatt a Kiberműveleti Parancsnokság.



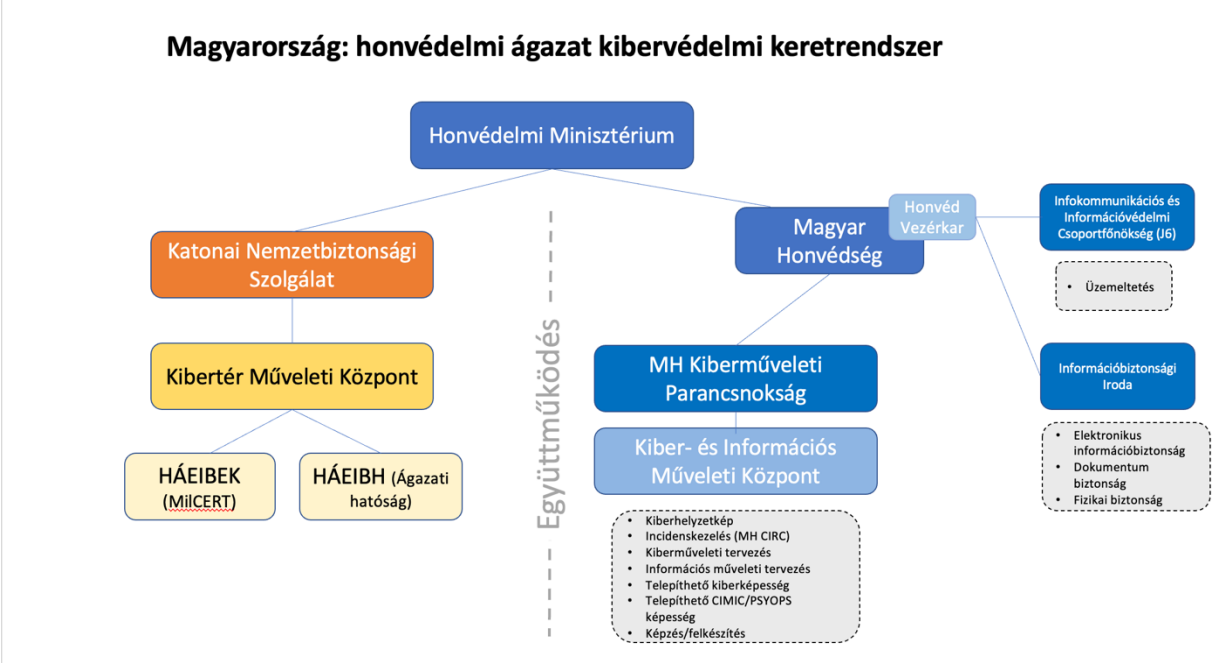
24. ábra: A hazai kibervédelem háttere. Forrás: dr. Kovács László előadása [125]

4.2.4 Honvédelmi szervezetek

A kiberképességek szervezeti kialakítása 2019-ben indult meg, melynek állomásaként megnyitott a Magyar Honvédség Kiberakadémiája. Általánosságban elmondható, hogy a nemzeti képességfejlesztésekről kevés információ kerül nyilvánosságra, azonban valószínűsíthetően a legtöbb állam végez kiberfejlesztéseket. A kiberképességek körében megkülönböztethetőek passzív és aktív védelmi képességek. A passzív védelmi képességek esetében saját hálózaton belüli hatókörű, főként megelőző, incidenskezelő, adat- és rendszer-helyreállító jellegű tevékenységeket értünk [146:11], míg aktív védelmi képességek alatt egy fenyegetés megelőzésére vagy megakadályozására irányuló, saját hálózaton kívüli hatókörrel is rendelkező, támadó jellegű műveleti képességeket [147:109]. Ez a szervezet végzi az oktatási, képzési és kiképzési feladatokat, beleértve a honvédség felhasználóinak kibertudatossági képzését, illetve a jövőbeli kiberműveleti erők felkészítését [148].

Az egyik ilyen feladat az oktatás, képzés és kiképzés rendszerének és akár intézményrendszerének a megteremtése. Ez nemcsak a saját állomány felkészítését jelenti, hanem a Magyar Honvédség egészére vonatkozó, elsősorban kibervédelmi képzéseket is. Ezekkel a képzésekkel lehetséges emelni a kiberbiztonsági tudatosság és elkötelezettség szintjén. Nyilvánvalóan ezek a képzések és kiképzések az eltérő szinteken eltérő célokkal is párosulnak, hiszen amíg az említett kiberbiztonsági tudatossági képzéseket minden szinten folytatni kell, addig a kiberműveletek stratégiai kérdéseit a katonai felsővezetés szintjén, de a konkrét technikai végrehajtást műveleti és harcászati szinten szükséges oktatni.

Benkő Tibor honvédelmi miniszter 2020. évi honvédelmi bizottsági ülésén elmondta, hogy a tárgyév decemberéig a kiberakadémián 19 tanfolyam került lebonyolításra, és 3000 fő vett részt a biztonságtudatosítási tanfolyamon [149:29].



25. ábra: a hazai honvédelmi ágazat kibervédelmi keretrendszere. [125]

A hazai katonai kiberképességeket tekintve két szervezetet kell kiemelni: a Katonai Nemzetbiztonsági Szolgálatot (KNBSZ) és a Kiberműveleti Parancsnokságot (és alárendelt szervezeté, a Kiber- és Információs Műveleti Központot). Előbbi feladatait a 2019. évi CV. tv. 12. §3 (3) állapította meg, így új feladatként jelentkezett, hogy a KNBSZ „információkat gyűjt a honvédelmi érdeket veszélyeztető kibertevékenységekről és -szervezetekről, jogszabály keretei között ellátja a honvédelmi ágazat elektronikus információbiztonsági feladatait, biztosítja a honvédelemért felelős miniszter által vezetett minisztérium, valamint a Magyar Honvédség Parancsnoksága információvédelmi tervező munkájához szükséges információkat, továbbá kibertérműveleti képességeivel ellátja a honvédelmi érdekek nemzetbiztonsági jellegű védelmét és a Magyar Honvédség kibervédelmének és műveleteinek támogatását” [150]. A kibervédelmi képesség ennek tükrében jelent egy figyelő és információjelentő tevékenységet (defenzív képességet), valamint egy beavatkozó tevékenységet (reagáló képességet) [151:85].

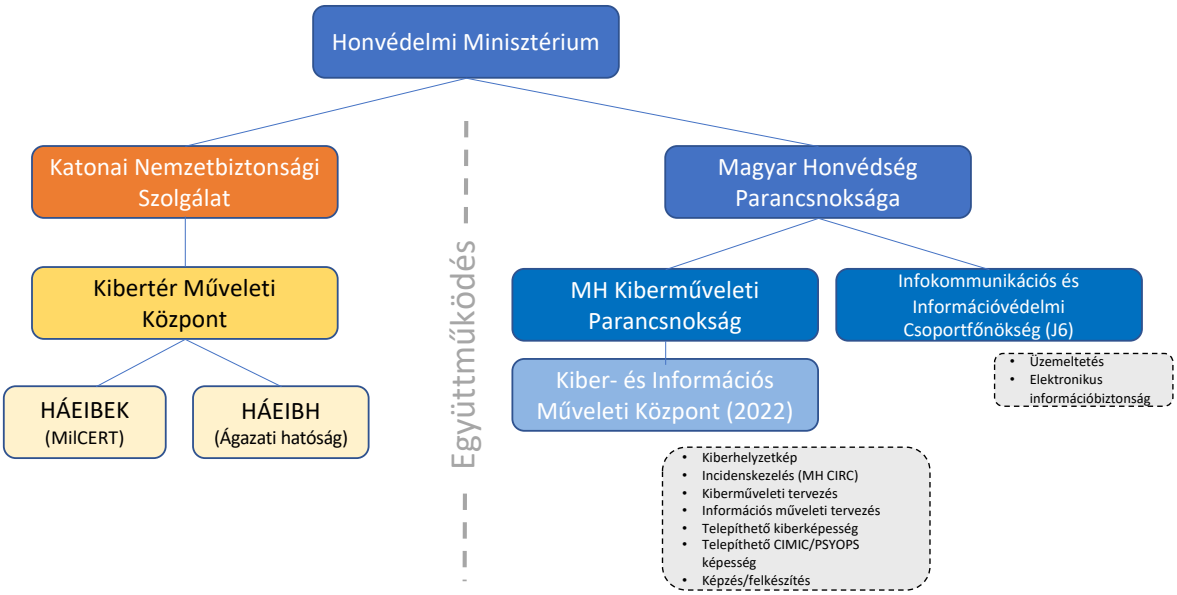
A honvédelmi miniszter 3/2019. (I. 31.) HM-utasításban, a honvédelmi szervezetek 2019. évi feladatainak, valamint a 2020–2021. évi tevékenységek fő irányairól meghatározásáról megjelenik „a jóváhagyott fejlesztési programok megvalósításának folytatása, figyelemmel a technikai adatszerző eszközpark korszerűsítésére, a honvédelmi szervezetek minősített összeköttetéseinek biztosítására, *a honvédelmi ágazati szintű kibervédelmi képességfejlesztésre”*. A 2019. évi éves beszámolóban [152] egyfelől megjelenik, hogy az MH fő feladatai Magyarország szuverenitásának, határainak – ezen belül területe,

légtere és *kibertere* – védelméhez, valamint a szövetségi rendszerekben vállalt kötelezettségek ellátásához szükséges katonai képességek kialakítása és fenntartása, továbbá az ezekhez szükséges feltételrendszer biztosítása. Ennek biztosítása érdekében a KNBSZ „információkat gyűjt (...) a honvédelmi érdeket sértő kibertevékenységről, továbbá a műveleti területén lévő alakulatok és azok állománya ellen irányuló törekvésekről és tevékenységekről".

A másik szervezet az MHP-n belüli, korábban kibervédelmi szemlélőségnek nevezett, Kiberműveleti Parancsnokság. Az MHP-nak az MH kibervédelmének és kiberműveleti képességeinek stratégiai szintű képességkialakító, az MH kibervédelmi szakterülete fejlesztését irányító és felügyeletét ellátó önálló szervezeti egysége.

A Kiberműveleti Parancsnokság munkáját a parancsnok - korábban szemlélő - vezeti és irányította az MHP, valamint az MH hadrendjébe tartozó katonai szervezetek kibervédelmi és kiberműveleti tevékenységét. Meghatározza a szakterülete vezetéséhez szükséges szervezeti kialakítás alappilléreit, struktúráját. Az MHP Infokommunikációs és Információvédelmi Csoportfőnökséggel együttműködve koordinálja a kibervédelmi képességfejlesztést, valamint harmonizálja ezen képességek kialakítását [153].

Az MH Kiber- és Információs Műveleti Központot (MH KIMK) öt funkcióra építették fel. Az első funkció az adat- és információgyűjtés, elemzés és értékelés. A másik a művelettervező, a harmadik a műveleti. Az utóbbi szerves részét képezi a nem kinetikus terület is, vagyis a jogelőd szervezettől megörökölt CIMIC-PSYOPS tevékenység. A műveleti résznek vannak statikus és telepíthető, tehát mobil elemei is. A negyedik-ötödik funkciók pedig a művelettámogatás és nem utolsósorban az oktatási tevékenység. Az MH KIMK-en belül jelenik meg a kiberhelyzetkép (SA) előállításának képessége, továbbá a kiberműveleti tervezés.



26. ábra. A honvédelem ágazat kibervédelmi szervezetei. Forrás: dr. Kovács László előadása. [125]

Erősen kapcsolódnak a katonai kiberképességek fejlesztéséhez az oktatási intézmények. Elsősorban a Nemzeti Közszolgálati Egyetem szakjai révén (Kiberbiztonsági mesterszak, Katonai vezető Bsc szak – híradó/elektronikai hadviselés/üzemeltetés szakirány), másfelől az Altiszti Akadémián keresztül.

4.3 SWOT-analízis

Magyarország tekintetében az 1. szint a 2020. évi Nemzeti Biztonsági Stratégiában jelenik meg, ahol hangsúlyozzák a kiberképességek fejlesztésének fontosságát. A 2. szint, a fejlesztés indítása 2019-ben kezdődött el, a Magyar Honvédség Parancsnoksága (MHP) Kibervédelmi Szemlélőség, majd a Kibervédelmi Akadémia létrehozásával. Jelenleg a 3. szinten tartunk, elértük a kezdeti kapacitási szintet (IOC). Ahhoz, hogy a növekedési stádiumból a 4., kiterjesztési stádiumba érjen egy szervezet, a hatékonyság növeléséhez szükséges az integráció és az áramvonalasítás.

Szint	Leírás
1. Ötletelés	A kormány elismeri az offenzív kiberberuházások fontosságát, és beszél a szervezet létrehozásának szükségességéről
2. Fejlesztés indítása	Politikai felhatalmazás van a szervezet létrehozására
3. Növekedés	A szervezet a tényleges működési kapacitás felé mozdult el
4. Kiterjesztés	A szervezet többször is offenzív kiberműveleteket hajtott végre, és felméri a további fejlesztési lehetőségeket
5. Érettség	A szervezet képes teljes spektrumú műveleteket végezni

27. sz. ábra. Forrás: Ambrus Éva, kiberszervezetek képességei, [154: 271]

A kiberműveleti képességek fejlesztési lehetőségeinek feltérképezéséhez egy jelenlegi pillanatképből kiindulva lehetséges eljutni. Ehhez az ún. SWOT-elemzést veszem alapul, amely, ahogyan korábban bemutattam egy stratégiai tervezési technika, amely segít a szervezeteknek azonosítani a projekttervezéssel kapcsolatos erősségeket, gyengeségeket, lehetőségeket és veszélyeket [155].

Erősségek	Gyengeségek
új biztonsági és katonai stratégia erősödő kiberszemlélete (doktrínális háttér) szervezeti megújulás (szervezet) képzés és oktatás (kiberakadémia, MA) felszerelés (Zrínyi Haderő-fejlesztési Program)	civil és katonai „kibertér" összetettsége koordináció szakemberek vonzása és megtartása (személyzet) haderőfejlesztés
Lehetőségek	**Kihívások**
rugalmas reagálás (alkalmazkodóképesség) intézményközi és nemzetközi együttműködések	gyorsan változó technológia, lekövetési nehézség adaptábilitás lassúsága (információ)

28. ábra: SWOT-analízis a hazai kiberképesség fejlesztésről [saját szerkesztés]

4.3.1 Erősségek

A hagyományosan államközpontú nemzetközi rendszerben az államok saját maguk biztonságáról, annak alkotóelemeiről, területeiről és az azt fenyegető tényezőkről alkotott képe jelenti a kiindulási pontot, melynek megtestesülése a Nemzeti Biztonsági Stratégia (NBS). A nemzeti katonai stratégia (NKS) mindig része a nemzeti stratégiának, azt támogatja, azaz megfelel a nemzeti politikának. Az NKS a nemzeti biztonsági erőforrások, valamint a fegyveres erők fejlesztésével kapcsolatos komplex nézet- és tevékenységrendszer. Az NKS már nem ismétli meg az NBS általános megállapításait [156:34–35].

Az elmúlt évek doktrinális háttérében egyértelműen erősödik a kiberfókusz, amelynek oka és okozata a szervezeti háttér kiépülése. A Kiber Szemlélőség, majd Kiberműveleti

Parancsnokság, illetve a műveleti szinten az MH KIMK megjelenése hozzájárult ahhoz, hogy az NBS-ben és az NKS-ben megjelenő feladatok leképeződjenek szervezeti elemekben. Ahhoz, hogy ez az új képesség kifejlődhessen, szükség volt beruházásra úgy a felszerelés, mint a képzések tekintetében, ezt foglalta keretbe az általános haderőfejlesztési program (Zrínyi Honvédelmi és Haderőfejlesztési Program).

A 2021. évi honvédelmi költségvetés 778 milliárd forint volt, a 2022. évi 1003 milliárd forint, amely 28,9%-os nominális emelést jelent. A nemzeti összтermékhez viszonyítva is jelentős a bővülés, az idei 1,66 százalék után jövőre meghaladja az 1,7 százalékot a honvédelmi kiadások GDP-hez viszonyított aránya, így egyre közeledünk a NATO által elvárt kétszázalékos mértékhez, amit a vállalások alapján 2024-re kell elérni [144]. Ezt 2023-ban sikerült teljesíteni, a 842 milliárd forintos Honvédelmi Alap megteremtette a honvédelmi fejlesztések forrásait, így a honvédelemre fordított kiadások 2023-ban meghaladják a GDP 2%-át. A Honvédelmi Alap 2024 évi kerete 1310 milliárt forint lesz, ezzel 2024-ben is teljesülni fog a 2%-os vállalás. Ennek a költségvetési növekedésnek központi eleme a Zrínyi Honvédelmi és Haderőfejlesztési Program, amely egyszerre jelent hadiipari és haderőfejlesztést. Ez a két elem egymást támogatva, hosszabb távon képes biztosítani a honvédség ütőképességét, hogy a befektetések ne egyszeriek legyenek, hanem folyamatosan fenntartsák és igazítsák képességeiket a kor követelményeihez. [154]

Kiberbiztonsági szempontból elmondható, hogy Magyarországon a kiberbiztonság jó állapotban van és egy nagyon jól szabályozott terület. A jogszabályi háttér is rendelkezésre áll, hiszen 2013-tól az illetékes szervezetek java egyrészt a Belügyminisztérium fennhatósága alatt felel a 2013. évi L. törvény (az állami és önkormányzati szervek elektronikus információbiztonságáról) betartásáért. Mindemellett a honvédelmi ágazatban a kiberbiztonságért és kiberműveletekért felelős szervezetek is közreműködnek, ezen szervezetek együtt felelősek a területért. Az egyetemi képzések nagyon fontosak, az, hogy a Nemzeti Közszolgálati Egyetemen van kiberbiztonsági mesterképzés unikumnak számít az Európai Unióban. Más egyetemeken is folyik hasonló, mint például az Óbudai Egyetemen is előremutató oktatás- és kutatásfejlesztés zajlik, másfél évtizede működnek kutatóintézetek, műhelyek, és ezek világszínvonalúak. Az egyik motorja a közigazgatás, a tudományos élet és a vállalati szféra együttműködésének a nemzeti kiberbiztonsági koordinációs tanács, illetve a kiberkoordinátor. [157:1333-1334]

Mindazonáltal vannak itt is fejlődési lehetőségek. A Nemzeti Kibervédelmi Intézet által publikált kézikönyve, mely elsősorban a villamosenergia területét érintő kibertámadásokat érinti, olyan javaslatokat fogalmaz meg a kiberstratégiát érintően, amely általánosságban is előremutatók lennének. Ilyen javaslat, hogy a magyar stratégiát is meghatározott időtartamra (3 vagy 5 év) alkossák meg, illetve azon belül jelenjenek meg elérendő célok, a megvalósítás módjai és eszközei- valamint határidejét, illetve a felelősöket, továbbá a visszaellenőrzés eszközrendszere. [158:183]

4.3.2 Gyengeségek

Az erős kiberképességek kiépítése összetett és folyamatos folyamat lehet, és számos lehetséges kihívással és gyengeséggel szembesülhetnek a szervezetek. A kiberképesség-építés fő gyengeségei közé tartozik az erőforrások hiánya. A kiberképességek kiépítése erőforrás-igényes lehet, és előfordulhat, hogy a szervezetek nem rendelkeznek a szükséges költségvetéssel, személyzettel vagy szakértelemmel ahhoz, hogy hatékonyan kiépítsék és fenntartsák képességeiket. Gyengeség (és kihívása) az összetettsége, a kiberbiztonság összetett terület, és a szervezeteknek nehézséget okozhat, hogy lépést tudjanak tartani a fenyegetések és technológiák folyamatosan fejlődő környezetével. Ez részben koordinációt igényel a különböző szervezetek között, részben pedig - miután erőforrás igényes terület - folyamatos befektetést igényel.

Nehézséget jelenthet a hatékonyság mérése, miután nehéz számszerűsíteni a kibertámadások vagy incidensek lehetséges következményeit, és így a befektetések megtérülését. A kiber, mint terület, összetettsége azt is jelenti, hogy nehéz (a kiberbiztonság) értékét, a kibertér veszélyeit kommunikálni.

A haderőfejlesztés mind az erősség, mind a gyengeség oldalán megjelenik az elemzésnek. Erősség (belső faktor), hogy Magyarország többet költ haderőreformra, mint korábban. Gyengeség (külső faktor), hogy szövetségi szinten továbbra sem érjük el a 2% GDP összegét. A NATO szövetség 30 tagjából csak hét költötte GDP-jének legalább 2 százalékát védelemre 2022-ben. Azt a 21 EU-tagállamot, amelyek egyben NATO-tagok is, a 2014-es walesi csúcstalálkozó óta a GDP 2%-át kitevő NATO védelmi kiadási kötelezettsége vezérli. 2021-ben azonban a NATO-tag 21 tagállam közül csak hét (Litvánia, Lettország, Észtország, Horvátország, Lengyelország, Portugália és Görögország) költötte a GDP 2%-át védelemre. Az állandó strukturált együttműködésben (PESCO) részt vevő EU-tagállamok (így Magyarország is) szintén megállapodtak abban, hogy „rendszeres reálértéken növelik védelmi költségvetésüket” PESCO-kötelezettségeik értelmében. [159]

	2014	2015	2016	2017	2018	2019	2020	2021	2022*
Greece	2.22	2.31	2.40	2.38	2.54	2.45	2.91	3.70	3.54
U.S.	3.72	3.52	3.52	3.31	3.29	3.51	3.64	3.48	3.46
Lithuania**	0.88	1.14	1.48	1.71	1.97	2.00	2.07	1.97	2.47
Poland**	1.87	2.22	2.00	1.89	2.01	1.98	2.23	2.22	2.42
U.K.	2.14	2.03	2.08	2.07	2.10	2.08	2.35	2.30	2.16
Estonia	1.93	2.03	2.07	2.01	2.01	2.05	2.30	2.02	2.12
Latvia**	0.94	1.03	1.44	1.59	2.06	2.02	2.15	2.07	2.07
Croatia	1.82	1.76	1.60	1.64	1.55	1.61	1.71	1.98	1.91
France	1.82	1.78	1.79	1.78	1.81	1.81	2.00	1.91	1.89
Slovakia	0.98	1.11	1.12	1.10	1.22	1.70	1.92	1.77	1.76
Romania**	1.35	1.45	1.43	1.73	1.79	1.84	2.01	1.86	1.75
Netherlands	1.15	1.13	1.16	1.15	1.22	1.32	1.41	1.38	1.64
North Macedonia	1.09	1.05	0.97	0.89	0.94	1.16	1.27	1.47	1.61
Norway	1.55	1.59	1.74	1.72	1.73	1.86	2.00	1.75	1.57
Albania	1.35	1.16	1.10	1.11	1.16	1.28	1.30	1.22	1.57
Bulgaria	1.31	1.25	1.24	1.22	1.45	3.13	1.59	1.52	1.54
Italy	1.14	1.07	1.18	1.20	1.23	1.17	1.59	1.57	1.51
Germany	1.19	1.19	1.20	1.23	1.25	1.35	1.51	1.46	1.49
Hungary	0.86	0.90	1.00	1.19	1.01	1.34	1.76	1.68	1.44
Denmark	1.15	1.11	1.15	1.14	1.28	1.30	1.38	1.32	1.38
Portugal	1.31	1.33	1.27	1.24	1.34	1.37	1.43	1.54	1.38
Turkey	1.45	1.38	1.45	1.51	1.82	1.86	1.86	1.61	1.37
Montenegro	1.50	1.40	1.42	1.34	1.37	1.33	1.73	1.55	1.35
Czech Rep.	0.94	1.02	0.95	1.03	1.10	1.18	1.30	1.39	1.34
Canada	1.01	1.20	1.16	1.44	1.30	1.30	1.42	1.28	1.29
Slovenia	0.97	0.93	1.00	0.98	1.01	1.05	1.06	1.24	1.26
Belgium	0.97	0.91	0.89	0.88	0.89	0.89	1.01	1.05	1.18
Spain	0.92	0.93	0.81	0.91	0.93	0.91	1.01	1.04	1.09
Luxembourg	0.37	0.42	0.38	0.50	0.50	0.55	0.58	0.47	0.62

29. ábra: GDP arányos védelmi kiadások 2022-ben [159]

4.3.3. Lehetőségek

Az alkalmazkodóképesség a kiberszervezet fejlesztésének lehetőségének tekinthető, hiszen az a szervezet azon képességére utal, hogy reagálni és alkalmazkodni tud a belső vagy külső környezet változásaihoz. Egy kiberszervezet esetében az alkalmazkodóképesség jelentős előnyt jelenthet, hiszen a technológiai és kiberbiztonsági környezet folyamatosan fejlődik és változik. A SWOT-elemzésben a lehetőségek olyan külső tényezők, amelyek kihasználhatók a szervezet javára. Az alkalmazkodóképességével a szervezet olyan stratégiák és taktikák kidolgozására összpontosíthat, amelyek javítják a kiberbiztonsági környezet változásaihoz való alkalmazkodási képességét, ami végső soron a túlélőképesség növekedéséhez vezethet.

A nemzeti és nemzetközi együttműködés több lehetőséget is rejt. A fokozott kiberfenyegetések elleni védelemben a szervezetek megoszthatják egymással a legújabb fenyegetésekkel kapcsolatos információkat. A kiberbiztonság költséges és erőforrás-igényes lehet, az együttműködés révén a szervezetek egyesíthetik erőforrásaikat és szakértelmüket egy robusztusabb kiberbiztonsági infrastruktúra létrehozása érdekében. Mivel a különböző iparágak különböző típusú kiberfenyegetésekkel néznek szembe, együttműködésük révén a szervezetek betekintést nyerhetnek az adott iparágakban érvényesülő legújabb trendekbe és legjobb gyakorlatokba.

Az egyik ilyen nemzetközi lehetőség Magyarország számára az EU PESCO Projekt keretében megvalósuló Kiber-és Információs Domén Koordinációs Központ projekt.

A kiber- és információs domén az Európai Unió közös biztonság- és védelempolitikája szempontjából is egyre fontosabbá válik. Ezért a projektpartnerek közösen egy Kiber- és Információs Domén Koordinációs Központot (CIDCC) kívánnak az EU rendelkezésére bocsátani. Ehhez a PESCO keretrendszerben[65] (CIDCC PESCO) kezdeti koordinációs elemként az EU által vezetett katonai műveleteket és missziókat kívánja támogatni.

A CIDCC PESCO kezdeti képességének három fő funkciója lenne:

- Olyan **információsközpont** szerep betöltését, amely összeköti az érintett uniós érdekelt feleket, adatokat és információkat cserél a kiber- és információs terület közös helyzetképéhez (CONNECT);
- **Elemzőközpont**ként működni az adatok összegyűjtésére, egyesítésére és vizsgálatára a helyzetfelismerés növelése, továbbá a holisztikus elemzések és szervezetre szabott ajánlások biztosítása érdekében (COMPOUND);
- **Tanácsadó elem**ként a CIDCC a kiber- és információs területtel kapcsolatos szakértelmet biztosít az EU katonai missziók és műveletek tervezéséhez és végrehajtásához (CONTRIBUTE).

Magyarország 2018 óta partner tagállam a CIDCC PESCO Projektben. A Projekt vezetőnemzete Németország, partner tagállam még Franciaország és Hollandia. Jelenleg tizenegy megfigyelő tagállam van jelen a projektben[66]. A négy partnerország megállapodott abban, hogy biztosítják a kezdeti finanszírozást a CIDCC-képesség elindításához, az összes uniós tagállam javára.

[65] A PESCO az Európai Unió egyik állandó együttműködési keretrendszere, aminek részeként alapvetően védelmi típusú projekteket, kezdeményezéseket támogatnak.

[66] Belgium, Észtország, Görögország, Olaszország, Ausztria, Lengyelország, Portugália, Szlovákia, Spanyolország, a Cseh Köztársaság és Ciprus.

A kezdeti CIDCC-képesség az EU katonai képességeinek egyik jelentős hiányát orvosolja, mivel az EU a stratégiai verseny és az összetett biztonsági fenyegetések korszakával néz szembe, és – katonai célokra vonatkozóan – nincs átfogó képessége a kiber- és információs terület helyzetképének kialakítására, elemzésére és értékelésére. Az a következtetés, hogy a képességhiányt ad hoc megoldásként CIDCC PESCO biztosításával kell orvosolni, a jelenlegi geopolitikai helyzetből és három naprakész uniós politikai, stratégiai és operatív szintű dokumentumból lett levezetve:

- A „Biztonsági és Védelmi Stratégiai Iránytű” – amelyet az EU Tanácsa 2022. márciusban tett közzé – egyértelmű iránymutatást ad az EU közös biztonság- és védelempolitikája közösen finanszírozott biztonsági architektúrájának javításához. Kiemeli a katonai fellépés és a 21. századi környezetben való működés képességének megerősítésére irányuló szándékot, amelyben többek között a hibrid konfliktusok veszélyeztetik a biztonságot.
- A 2021 szeptemberében jóváhagyott „EU katonai víziója és stratégiája a kibertérről, mint műveleti területről”, az EU tagállamai kijelentették, hogy a kiber- és információs tartomány a kibertér, az elektromágneses környezet és a kognitív környezet hármasából áll.
- Végül az EU-tagállamok az „EU Kibervédelmi Koncepció” 2022. májusi kiadásával deklarálták a Kiber- és Információs Domén Koordinációs Központ – követelményét.

Az ez és ehhez hasonlo együttműködések elősegítik az ellenállóképesség növekedését, növelik az államok közötti bizalmat és elősegítik a tudás-transzfert, amely ezen a területen kiemelten fontos.

Ez a nemzetek közötti együttműködés azért is fontos, mert jelenleg létezik egy stratégiai vákuum, egy új stratégia környezet, amelyre az EU-ban még egyetlen tagállam sem tudott reagálni. A háború szintje alatti kiberkonfliktus egy olyan, állandósulni látszó stratégiai környezet, amelyben a katonai, hírszerző, rendvédelmi szerveknek együtt kell navigálniuk és koordinálniuk. [160] A legtöbb katonai kiberdoktrínák kezdeti stratégiai útmutatást adnak a fegyveres konfliktusokhoz, de továbbra sem részletezik, hogy a háború szintje alatt zajló folyamatos kiberkonfliktus hogyan befolyásolja az országok stratégiai helyzetét. Az azzal kapcsolatos kérdések, hogy mikor, hogyan, kik és milyen mértékben alkalmaznak kiberellenintézkedéseket továbbra is kétértelműek és titkosak. [160] A háború szintje alatti

konfliktus Magyarország számára is állandó, szoros együttműködést igényel a kibervédelem, kiberbiztonság területén résztvevő szervezetektől és vállalatoktól.

4.3.4 Kihívások

Számos potenciális fenyegetéssel szembesülhetnek a szervezetek a kiberképességeik kiépítése során. Ezek közül kettő, amelyet azonosítottam a gyorsan változó környezet és az ahhoz való alkalmazkodás lassúsága. Ennek okai többek között a koordináció, hiszen a kiberparancsnokságok jellemzően nagyobb katonai szervezetek részét képezik, és a bürokratikus folyamatok lelassíthatják a döntéshozatalt és a végrehajtást. Másodszor a korábban említett erőforrások hiánya. A kiberbiztonság folyamatosan fejlődő terület, és a legújabb technológiával és technikákkal való lépéstartás jelentős erőforrásokat igényel. Gondot jelenthetnek még az összetett szabályozások, hiszen a kiberműveletek gyakran bonyolult jogi és szabályozási kereteket foglalnak magukban, amelyekben nehéz lehet eligazodni. Ez lelassíthatja a döntéshozatalt és a végrehajtást, mivel a kiberparancsnokságoknak biztosítaniuk kell a törvényi keretek közötti működést.

Általánosságban elmondható, hogy az egyik legsürgetőbb probléma, amellyel meg kell küzdeni az elkövetkező években, hogy hogyan lehet megtalálni a megfelelő egyensúlyt a kibertérben történő rosszindulatú tevékenységekre való gyors reagálás és a megfelelő koordináció egyidejű biztosítása között.

Ehhez a gyorsreagáláshoz és rezilienciához szükséges a megfelelő keretrendszer biztosítása. Spitzer Jenő és Vikman László tanulmányukban kiemelik, "hogy védelmi és biztonsági tervezés mind a stratégiai dokumentumok kialakításakor, mind a jogalkotáskor magában kell, hogy rejtse a perspektivikusságot, fenntartva a kihívások változásának hirtelenségét, biztosítva az erre is kiterjedő rezílienciát;" valamint " a változó környezetre reagálás nem lehet időleges, a jogalkotás következetessége mellett legalább fontos innovációt és hatékonyságnövelést hozó intézményrendszeri reformokat eszközölni, ami csak akképpen lehetséges, hogy a hatáskörök hagyományos helyéhez és az „ágazati buborékhoz” ragaszkodást szellemiségében az államigazgatás maga mögött tudja hagyni és a szükséges kihívásokban koordinatív együttműködésben képes a feladatait ellátni". [161:25]

Tovább bontva ezeket az NKI konkrét javaslatokat fogalmaz meg:

- Pontosan azonosítani kellene, hogy mi az elvárás a NATO-val történő együttműködés, vagy a PPP[67] kapcsán, és ehhez határidőket és felelősöket rendelni, illetve a megvalósulást érintő ellenőrzési rendszert. A megvalósulás hiányának vagy nem megfelelőségének kellene generálnia a stratégia felülvizsgálata utáni módosítását.
- A kiberkoordinátornak rendkívül fontos szerepe lenne a stratégiában megfogalmazott intézkedések végrehajtásában. A Nemzeti Kiberbiztonsági Koordinációs Tanáccsal együtt lehetne egy supervisori feladatkörrel ellátott szereplő, illetve a villamosenergia alágazati szereplők döntéshozóival és/vagy szakembereivel együttesen.
- A kiberfenyegetések folyamatosan fejlődnek, ahogy a támadások számai is világszerte. A szabályozás, illetve az elvileg alapját képező stratégia kiadásának hiánya egy olyan idő szakadékot eredményez, amely a megfelelő védelem kialakítását nagy mértékben hátráltatja. [162:185]

A hagyományosabb tartományoktól eltérően a kiberteret az állandó kontaktus jellemzi, emiatt szükséges a gyors reakció és az állandó koordináció. A kibertérben gyakorlatilag állandóan összhaderőnemi műveletekre kell készülni. A koordináció - békeidőben is - azért szükséges, mert egy egyoldalú művelet során – akaratlanul is - veszélyeztethet folyamatban lévő hírszerzési műveleteket.

4.4 Összegzés, rész-következtetések

A kibertér, mint negyedik dimenzió a hadviselésben, régebben megjelent elméletben, mint a gyakorlatban. A kiberképességek integrálása a hagyományos katonai szervezetben több kérdést vet fel egyfelől a támadóképességek fejlesztésének fontosságáról, másfelől a konkrét szervezeti átalakításról, hiszen jelenleg a kiberműveletek támogató funkciót látnak el. Ahogyan a kiberképességek fejlődnek és e terület fontossága növekszik, ezt felismerve elképzelhető egy tényleges összhaderőnemi integrálódás. Magyarország e tekintetben nincs elmaradva. Az új Nemzeti Biztonsági Stratégia egyértelműen kijelöli a fejlesztési irányokat, amelyek a hamarosan megjelenő szakpolitikai stratégiákban is tükröződni fognak. Szervezetileg is elindult egy fejlesztés a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program keretében.

[67] Public-Private Partnership, A PPP-ben a felek - vagyis az állam és a magánszféra - a közszolgáltatás nyújtásának felelősségét és kockázatát közösen viselik, a hagyományos gyakorlattal ellentétben az állam a közszolgáltatás hosszú távú biztosítását rendeli meg a magánszférától.

Mindazonáltal a nemzetközi példákat látva a további szervezeti átalakításnak is lennének hozadékai, úgy a személyi felkészültség összevonása és tudásátadása, mint a hatékonyságnövelés szempontjából. Az információs műveletek égisze alatt a pszichológiai műveletek, a kiberműveletek és a többi nem kinetikus képesség koordinált alkalmazása elengedhetetlennek tűnik, ahogy ezt több ország már felismerte. Ez azonban nem egy újkeletű kérdés, hiszen az információs műveletek tudományos irodalma ezt már korábban is tárgyalta.

Egy ilyen összhaderőnemi integrálódás azonban minden állam és szervezet számára rendkívüli költségeket jelent mind technikai, mind személyi állomány tekintetében. A legtöbb állam számára kihívás a megfelelő képzettségű szakemberek képzése és szervezetben való tartása. Ennek megoldásaként átgondolandó az elvárt képzési szintek meghatározása, a belső és külső továbbképzések szervezése és a meglévő állomány át- és továbbképzése. Ezt a feladatot látja el a 2019-ben felállított Kibervédelmi Akadémia a Kiberparancsnokság felügyelete alatt. A képzések területén a Nemzeti Közszolgálati Egyetemen 2007 óta létezik a védelmi infokommunikációs rendszertervező mesterképzési szak, valamint 2019-ben elindult kiberbiztonsági mesterképzési szak. A felsőfokú, egyetemi végzettséget adó képzéseken túl – miután nem minden feladat ellátására szükséges ennyire elmélyült tudás – érdemes lenne egyfelől rövidebb, általánosabb részképzéseket, kurzusokat – amellyel a más szakterületekről érkező állomány készülhetne fel –, másfelől az általános képzésen túl szakfeladatra szabott moduláris képzéseket is figyelembe venni.

A támadó kiberképességek fejlesztése magával vonhat egyfajta kiberbiztonsági dilemmát is, miután az államok – elrettentés céljából – nemcsak védekező, hanem támadó képességeiket is fejleszteni fogják. Ez komoly kihívást és egyben egyensúlyra törekvést jelent nemzeti és európai szinten. A nemzetközi környezetben jelenleg kevés, mindenki által elfogadott norma van, és a megengedett, megengedhető válaszlépések sem tisztázottak. A terület mindenképpen folyamatos figyelmet és felügyeletet érdemel, kiemelve az együttműködést mind a katonai és a civil szektor között, mind a szövetség szintjén, miután jelenleg egy közös kibertér létezik.

A fejezetben bemutattam Magyarország katonai kiberképességeinek helyzetét SWOT-elemzéssel, valamint javaslatot tettem jövőbeni fejlesztési lehetőségekre.

Jelen fejezet az [154] publikációmat dolgozta fel és egészítette ki.

5. Összegzett kövekeztetések

Feldolgoztam és értelmeztem a katonai kibertérrel, kiberműveletekkel és a képességfejlesztéssel kapcsolatos alapfogalmakat. Összefoglaltam a kibertér lényegi jellemzőit, annak megjelenését a doktrínákban. A kiberteret, mint önálló műveleti területet azonban négy megkülönböztető jellemző teszi különállóvá a többi műveleti területtől: hogy (1) teljes mértékben emberi alkotás; hogy (2) folyamatosan változik; hogy (3) nem csak a konfliktus idején, hanem békeidőben is jelen van; hogy (4) 'mindenhollevősége' van, speciális viszonya van térhez és időhöz. A kiberműveletek része az információs műveleteknek és mint erőszorzó, nagyobb és szélesebb hatást tud kelteni, hiszen a kommunikáció, az információ átadásának színtere ma már a kibertér.

Mindezeket figyelembe véve azt a következtetés vonom le, hogy a **jövőben nem várható egy egységesen elfogadott definíció meghozatala** – egész egyszerűen azért, mert a nemzetállamoknak nem érdekük korlátozni saját lehetőségeiket, illetve olyan pragmatikus okokból is, mert gyorsabban változik a technológia, mintsem az szabályzókkal, doktrínákkal lekövethető lenne. Ezeket figyelembe véve, a kellő szabadságot meghagyva alkottam meg egy, a disszertációban használható, definiciót.

Ismertettem a képességfejlesztést akadályozó tényezőket és **javaslatot tettem az agilis módszertan használatára a kiberképességfejlesztése területén**. Véleményem szerint minden tagállam jelentős erőfeszítéseket fog tenni továbbra is a kiberképességek fejlesztésére, és ennek egyik módja az általam bemutatott akadályok elhárítása: (1) a doktrínák "frissen tartása", (2) a szervezetek esetében az integráció nehézségei, (3) a kiber karrierpálya, előmenetel hiánya, (4) a gyorsan fejlődő technika beszerzésének nehézségei, (5) az oktatás és képzések fenntartása költséges, (6) a személyzeti kérdések és (7) a létesítmények kialakításának költségei.

A felsorolt akadályokra válaszként ismertettem az agilis módszertant, amely az IT területén bevett képességfejlesztési keretrendszer. **A módszertan előnyei a katonai képességfejlesztésben a rugalmasság, manőverezhetőség és gyorsaság**. Ezek mellett tovább fejleszti az együttműködést, fokozza az alkalmazkodóképességet, rezilienciát, elősegítik a kreatív problémamegoldást és számszerűsített elszámolhatóságot biztosít a teljesítmény mérésre. Összességében az agilis módszertanok segíthetik a katonai alakulatok hatékonyabb és eredményesebb munkáját, különösen olyan helyzetekben, amikor a környezet folyamatosan változik – például a kibertérben, és meglátásom szerint alkalmas arra, hogy a hadseregen belül alkalmazásra kerüljön.

Összehasonlítottam a kiberműveletek kialakulását a légierő kialakulásával. Összefoglaltam a két műveleti domén hasonlóságait és különbözőségeit. Ahogyan eleinte nehézséget okozott a hadsereg és a tengerészet parancsnokainak integrálni a légierő adta lehetőségeket, úgy jelenleg a kiberműveleteknek is nehéz megjelenniük az összhaderőnemi műveletekben, gyakorlatokban, tervezésekben. Amíg a légierő számára a stratégiai bombázás volt a függetlenségének megváltása, addig a kiberműveletek terén még várjuk az effajta áttörést. **A kiberműveletek jobb megértéséhez a légierő által használt helyzetképet mutattam be.** A kiberhelyzetképnek szintúgy a gyűjtés - elemzés - vizualizáció a feladata, azonban lényegesen komplexebb környezetet kell figyelemmel kísérnie, mint a légierőnek. Azonban annak háromszíntű modelljének csak az első kettő szintjét sikerült ezidáig megvalósítani a kiberteret illetően: az adatok gyűjtését és értelmezését. A vizualizációt tekintve vannak kezdeményezések, azonban nehéz úgy prezentálni egy valós helyzetképet (és jövőben várható eseményeket, hatásokat) akár térképen, akár diagramokon, hogy azok ne okozzanak információs túlterhelést a döntéshozó számára.

Áttekintettem és bemutattam Magyarország katonai kiberképességeit, az ezért felelős szervezeteket és jogi hátteret. A SWOT-elemzés technikáját alapul véve megállapítottam, hogy Magyarország kiberképességei megfelelnek a környező országokéval, nincsenek lemaradásban, mint ahogy igaz az is, hogy hasonló problémákkal néz szembe (technológiai változások gyorsasága, magas bekerülési költségek, személyzet megtartása).

Új tudományos eredmények

A disszertációm során a következő új tudományos eredményekre jutottam.

1. **Megvizsgáltam** a katonai kibertér definícióit és **megállapítottam**, hogy a *kiberhadviselés a kiberműveleti képességek teljes spektrumának használatát igényli, mindezeknek teljes összhangban kell lennie a hazai jogszabályokkal, valamint a mindenkori Tallinni-kézikönyv ajánlásaival a sikeres képességfejlesztés érdekében.*

A kiberműveleti képességek fejlődésének üteme a jövőben nem látszik lassulni, ezért szükséges egy olyan tág keretet hagyni, amely ezt figyelembe véve úgy alkalmazza, hogy azok jogszerűek és a nemzetközi normákkal összhangban legyenek.

2. **Bizonyítottam,** hogy a jelenlegi kiberképességfejlesztés módszertana nem alkalmas a képességfejlesztés elérésére, fenntartására. Az agilis módszertan alkalmas a katonai kiberképességfejlesztés elősegítésére, figyelembe véve a szervezet korlátait. Tovább gondolva a módszertan alapjait **kidolgoztam annak alkalmazási lehetőségét és javaslatot tettem annak alkalmazására** akár pilot-projektként is.

A második fejezetben feltérképeztem a kiberképesség-fejlesztést akadályozó tényezőket. Ehhez a DOTLMPF keretrendszert alkalmaztam, miután az eredeti, PMESII keretrendszer alkalmatlannak bizonyult a kutatásaim során. A vizsgálódásaim során arra jutottam, hogy a legtöbb ország doktrinálisan, általánosságban foglalkozik a kiberképességekkel. Az elmúlt 15 évben egyre több ország hozott létre kiberparancsnokságokat a katonai szervezetek között. Azoknak „tartalma” eltérő abban, hogy „szűk” kiberteret érint-e (mondjuk SIGINT vagy elektronikai hadviselés), vagy „szélesebb” kibertér-elgondolással ruházták fel (például információs műveletek). A kiképzés, képzés és állomány tekintetében a vizsgált országok mind hasonló problémákkal néztek szembe: többek között a szakemberek vonzása és megtartása, a szakterület sajátosságai és a katonai kultúra összehangolása. A logisztika területén a beszerzések nehézségeivel szembesültek, mind általánosságban („vízesés” típusú beszerzési rendszer), mind egyébként az elmúlt évek ellátási láncainak lassulása okán. Ezekre a fejezet második részében válaszként bemutattam az agilis módszertant, amely rugalmasságával képes ezen akadályok egy részét kiküszöbölni. A kis létszámú, agilis alapelvekre épített állománnyal rövid időn belül sikerült képességfejlesztéseket elérni, amely eredmények a munkám során láthatóak.

3. **Összehasonlítottam** a kiberhelyzetképet és a légierő helyzetképpel és **javaslatot tettem** előbbi fejlesztési lehetőségeire.

A harmadik fejezetben összevetettem a kibertér és a légierő fejlődését, hasonlóságait és különbözőségeit. Mindkét haderőnem megküzdött, megküzd helyének kivívásában a „hagyományosnak" mondható haderőnemek mellett. A kibertér számára azonban az egyik legfőbb „előd" a légierő esetében a helyzetkép. Bemutattam a hagyományos helyzetkép fejlődését egészen a kiberhelyzetképig (amely végleges „formája" napjainkban is alakul még). A kiberhelyzetkép kialakítását nehezíti a kibertér duális volta, nem csak a katonai és polgári vonalon, hanem a kritikus infrastruktúrák tekintetében is. Hazai és nemzetközi szinten is fontos a bizalom kialakítása és fenntartása ahhoz, hogy valós helyzetkép alakulhasson ki.

4. **Kidolgoztam** a hazai kiberképességfejlesztés metodikáját és **javaslatot tettem** a kiberképességfejlesztés irányaira, ütemeire.

A negyedik fejezetben a hazai katonai kiberképességeket mértem fel egy SWOT-analízis keretében. Regionálisan a magyar képességfejlesztés nem marad el, és meglátásom szerint az erősségek és lehetőségek ellensúlyozzák a kockázatokat és kihívásokat. A nemzetközi példákat látva, a további szervezeti átalakításnak is lennének hozadékai, úgy a felkészült személyek összevonása és tudásátadása, mint a hatékonyságnövelés szempontjából. Átgondolandó az elvárt képzési szintek meghatározása a különböző pozíciókra, illetve ennek megjelenése egy hierarchikus szervezetben. A támadó kiberképességek fejlesztése magával vonhat egyfajta kiberbiztonsági dilemmát is, amelynek nyomán a nemzetközi normák alakulását folyamatosan figyelemmel kell kísérni.

Ajánlások

- A dolgozatomban megfogalmazottak alapján javaslom a közös kibertéri terminológia kialakítását és összehangolását a szövetségesekkel. A
- A kidolgozott fejlesztési módszertant javaslom a Magyar Honvédség kiberképességeinek tervezése során felhasználni.
- A kiberhelyzetkép kialakítása nélkülözhetetlen az összhaderőnemi műveletek tervezésekor és végrehajtásakor, annak megismeréséhez javaslom a szakterület minél koraibb bevonását a gyakorlatok tervezési folyamatokba.
- A kiberhelyzetkép kialakításához javaslom a kiberfelderítési képesség fejlesztése. Ez nemcsak a környezet technikai megértéséhez (fenyegetettség, motivációik, TTP-k, infrastruktúra, hálózataik) szükséges, hanem a tágabb kontextus megértését is elősegíti (értékelni és korlátozni a másod- és harmadrendű hatásokat).
- Elrettentés céljából kommunikáljuk a támadó kiberképességet anélkül, hogy eszkalációt okozna. Ennek egyik módja a kibergyakorlatokon való részvétel.

Irodalomjegyzék

[1] William F. Gibson: The Economist, 2003. december 4. sz.

[2] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny, 2020/81., 2101–2119. Elérhető: https://magyarkozlony.hu/dokumentumok/6c9e9f4be48fd1bc620655a7f249f81681f8ba67/letoltes (Letöltés időpontja: 2022. 02. 05.)

[3] HAIG Zs., KOVÁCS L., VÁNYA L., VASS S., NÉMETH A. (szerk.): Elektronikai hadviselés. Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[4] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: EU Policy on Cyber Defence JOIN(2022) 49 final https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022JC0049

[5] Damjan Strucl: Comparative study on the cyber defence of NATO Member States, NATO CCDCOE, 2021. https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf (Látogatás dátuma: 2022. 07. 22.)

[6] Ambrus Éva: Az összadatforrású elemzés és prediktív modellezés, HADMÉRNÖK 12: Különszám pp. 180–189., 10 p. (2017).

[7] Haig Zsolt: Információs műveletek a kibertérben, Budapest Dialóg Campus Kiadó, 2018.

[8] Ambrus Éva: Az összadatforrású elemzés és prediktív modellezés HADMÉRNÖK 12: Különszám pp. 180–189., 10 p. (2017).

[9] Gibson F., William: Neuromancer, New York, Ace Books, 1984.

[10] Jordan Branch: What's in a Name? Metaphors and Cybersecurity. International Organization, pp. 1–32., Cambrige University Press, 2020.

[11] Luisa Cruz Lobato és Kai Michael Kenkel: Discourses of cyberspace securitization in Brazil and in the United States., Revista Brasileira de Política Internacional, 58. évf. 2. sz., pp. 23–43. 2015.

[12] Daniel Ventre (szerk.): Cyber Conflict: Competing National Perspectives, 2013. Hoboken: John Wiley & Sons.

[13] Lt Gen (Dr) R S Panwar: 21st Century Warfare: from "battlefield" to "battlespace", Concepts and Doctrines, Information Operations, Network Centric Warfare, 2017. 10. 06., https://futurewars.rspanwar.net/21st-century-warfare-from-battlefield-to-battlespace/ (Látogatás dátuma: 2022. 10. 10.)

[14] Martin C. Libicki: Cyberdeterrence and cyberwar, RAND Project Airforce, 2009. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (Látogatás dátuma: 2022. 06.22.)

[15] Daniel T. Kuehl: ‘From cyberspace to cyberpower: Defining the problem.’ In Franklin D Kramer, Stuart H Starr and Larry K Wentz (szerk.): Cyberpower and National Security. Washington, DC: National Defense University, 2009.

[16] Binxing Fang: Cyberspace Sovereignty. Reflections on Building a Community of Common Future in Cyberspace. Beijing, Springer, 2018.

[17] Max Smeets: No Shortcuts: Why states struggle to develop a military cyber-force, Oxford University Press, 2022.

[18] NATO Glossary of Terms and Definitions AAP-06 Edition 2018 https://nso.nato.int/nso/ZPUBLIC/_BRANCHINFO/TERMINOLOGY_PUBLIC/NON-CLASSIFIED%20NATO%20GLOSSARIES/AAP-6.PDF (Látogatás dátuma: 2021.07.21.)

[19] Kovács László doktori értekezésében, KOVÁCS L.: Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmzhatósága a Magyar Honvédségben. Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem, 2003.

[20] Aaron Brantly és Max Smeets: Military Operations in Cyberspace, In: Handbook of Military Sciences, DOI:10.1007/978-3-030-02866-4_19-1, Springer, 2020. https://link.springer.com/content/pdf/10.1007/978-3-030-02866-4_19-1.pdf (Látogatás dátuma: 2022. 08. 21.)

[21] NIST: Compuster Security Resource Center: Computer Network Operation Center https://csrc.nist.gov/glossary/term/computer_network_operations (Látogatás dátuma: 2022.05.12.)

[22] Alix Desforges: Representations of Cyberspace: A Geopolitical Tool. In Hérodote, No. 152–153., pp. 67–81. 2014.

[23] Mark Grzegorzewski és Christopher Marsh: Incorporating the cyberspace domain: how Russia and Chine exploit assymetric advantages in the great power competition. 2021.03.15., Modern War Institute, West Point Academy. https://mwi.usma.edu/incorporating-the-cyberspace-domain-how-russia-and-china-exploit-asymmetric-advantages-in-great-power-competition/ (Látogatás dátuma: 2022. 01. 23.)

[24] NATO CCDCOE: Cyber Commander's Handbook. 1. kiadás, 2021.

[25] Andy Greenber: The Wired Guide to Cyberwar, 2019. 08. 23. https://www.wired.com/story/cyberwar-guide/ (Látogatás dátuma: 2022. 08.11.)

[26] John Arquilla és David Ronfeldt: Cyberwar is Coming, RAND, 1993. p. 38. https://www.rand.org/pubs/reprints/RP223.html (Látogatás dátuma: 2020. 01. 30.)

[27] U.S. Department of Justice: White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, https://www.ojp.gov/ncjrs/virtual-library/abstracts/white-paper-clinton-administrations-policy-critical-infrastructure (Látogatás dátuma: 2022. 10. 22.)

[28] Richard A. Clarke és Robert Knake: Cyber War: The Next Threat to National Security and What to Do About It, Ecco, 2011. p. 320.

[29] John B. Sheldon és Britannica, The Editors of Encyclopaedia. "cyberwar". Encyclopedia Britannica, 2022. 12. 15. https://www.britannica.com/topic/cyberwar. (Látogatás dátuma: 2023. 01. 15.)

[30] Cameran Ashraf, Defining cyberwar: towards a definitional framework, Defense & Security Analysis, 2021, 37. évf. 3. sz., pp. 274–294, DOI: 10.1080/14751798.2021.1959141

[31] Ambrus Éva: EGY ÚJ DIMENZIÓ: TANULSÁGOK A LÉGIERŐ FEJLŐDÉSÉBŐL A KIBERTÉR SZÁMÁRA, KOMMENTÁR 2:2 pp. 111–116. , 6 p. (2021)

[32] Paul. J. Springer (szerk.) Encyclopedia of cyber warfare Santa Barbara, US, 2017.

[33] NATO ACT Framework for Future Alliance Operations 2018 Report, 2018, https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18.pdf (Látogatás dátuma: 2021. 11. 20.)

[34] NATO, “AAP-06 Edition 2018 NATO GLOSSARY OF TERMS AND CONDITIONS.” NATO, 2018.

[35] Prague Summit Declaration (2012), NATO, Elérhető: https://www.nato.int/cps/en/natohq/official_texts_19552.htm, (A letöltés dátuma 2020. szeptember 7.)

[36] Wales Summit Declaration (2014), NATO, Elérhető: https://www.nato.int/cps/en/natohq/official_texts_112964.htm (A letöltés dátuma 2020. szeptember 7.)

[37] NATO Cyber Defense Pledge (2016). NATO. Elérhető: https://www.nato.int/cps/en/natohq/official_texts_133177.htm (látogatás dátuma: 2020. szeptember 7.)

[38] NATO: Cyber defence: Evolution: https://www.nato.int/cps/en/natohq/topics_78170.htm (látogatás dátuma: 2020. szeptember 11.)

[39] Jens Stoltenberg (2019): NATO will defend itself, Prospect Magazine. Elérhető: https://www.prospectmagazine.co.uk/content/uploads/2019/08/Cyber_Resilience_October2019.pdf (A letöltés dátuma 2020. szeptember 9.)

[40] Brian Bartholomew és Juan Andres Guerrero-Saade: Wave your false flags! Deception tactics muddying attribution in targeted attacks. Kaspersky Lab. Elérhető: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf (A letöltés dátuma 2020. szeptember 9.)

[41] Merriam-Webster dictionnary: domain. https://www.merriam-webster.com/dictionary/domain (Letöltés dátuma: 2022. 11. 08.)

[42] Michael P. Kreuzer: Cyberspace is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age, The Strategy Bridge, https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age (A látogatás dátuma: 2022. 09. 30.)

[43] Jason Rivera: A Theory of Cyberwarfare: Political and Military Objectives, Lines of Communication, and Targets, Georgetown Security Studies Review vol. 10. 1. szám, https://georgetownsecuritystudiesreview.org/2014/06/10/a-theory-of-cyberwarfare-political-and-military-objectives-lines-of-communication-and-targets/ (Letöltés dátuma: 2022. 09. 30.)

[44] Riza Azmi, Kautsarina Kautsarina, Ima Apriany és William J. Tibben: Revisiting „Cyber" definition: Context, History and Doman in Windred Yaokuman et al. (szerk.): Modern Theories and Practices for Cyber Ethics and Security Compliance, 2020. DOI: 10.4018/978-1-7998-3149-5.ch001

[45] NATO AJP 3-20: Allied Joint Doctrine for Cyberspace Operations

[46] Haig Zsolt: Információs műveletek a kibertérben, Budapest Dialóg Campus Kiadó, 2018.

[47] Julie E. Cohen: Cyberspace As/And Space. Columbia Law Review, Vol. 107, No. 1, pp. 210-256, 2007, Georgetown Public Law Research Paper No. 898260, Elérhető SSRN: https://ssrn.com/abstract=898260

[48] John B. Sheldon: "Deciphering Cyberpower: Strategic Purpose in Peace and War." Strategic Studies Quarterly, vol. 5, no. 2, 2011, pp. 95–112. JSTOR, http://www.jstor.org/stable/26270559. (Letöltés dátuma: 2022. 11. 03.)

[49] Gregory Rattray, Strategic Warfare in Cyberspace, MIT Press, 2001. https://doi.org/10.7551/mitpress/6483.001.0001

[50] ENISA: Definition of Cybersecurity – Gaps and overlaps in standardisation, https://www.enisa.europa.eu/publications/definition-of-cybersecurity (Látogatás dátuma: 2022. 05. 22.)

[51] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat. Elérhető: https://njt.hu/jogszabaly/2013-1139-30-22.1 (Látogatás dátuma: 2020. 12. 13.)

[52] Kovács László: A kibertér védelme, 2018. Budapest, Magyarország: Dialóg Campus Kiadó, Nordex Kft., 354 p. ISBN: 9786155889639

[53] Marie Baezner és Sean Cordey, „National Cybersecurity Strategies in Comparison – Challenges for Switzerland", CSS Cyber Defense (2019, március), https://css.ethz.ch/en/services/digital-library/publications/publication. xhtml/8794e2d6-cd71-4e3b-937c-edd3f4aaca40." (Látogatás dátuma: 2022. 11. 30.)

[54] Piret Pernik: „Preparing for Cyber Conflict: Case Studies of Cyber Command", Nemzetközi Védelmi és Biztonsági Központ, (2018, december), https://icds.ee/wpcontent/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_2.pdf;December_201 (Látogatás dátuma: 2022. 11. 07.)

[55] Kyle Fendorf és Jessie Miller: Tracking Cyber Operations and Actors in the Russia-Ukraine War, Council on Foreign Relations, https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war (Letöltés dátuma: 2022. 12. 16.)

[56] Crowdstrike: Technical Analysis of the WhisperGate Malicious Bootloader, 2022. 01. 19., https://www.crowdstrike.com/blog/technical-analysis-of-whispergate-malware/ (Letöltés dátuma: 2022. 10. 09.)

[57] Sarah P. White: Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine. Doctoral dissertation, Harvard University, Graduate School of Arts & Science, 2019.

[58] T. Rona, „Washington Headquarters Services," 1976. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf. [Letöltés dátuma: 4 május 2023].

[59] C. Krasznay, „Kiberbiztonsági K+F+I Európában," in *Információ- és kiberbiztonság*, Budapest, Ludovika Egyetemi Kiadó, 2020, pp. 83-98.

[60] Z. Haig és L. Kovács, Kritikus Infrastruktúrák és kritikus információs infrastruktúrák, Budapest: Nemzeti Közszolgálati Egyetem, 2012.

[61] Lockheed Martin Cyber Kill Chain, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html Letöltve:2023.05.05.

[62] Nemzeti Kibervédelmi Intézet, „A Sandworm APT csoport sikertelen kibertámadást hajotott végre egy ukrán energiaszolgáltató ellen," 13 április 2022. [Online]. Available: https://nki.gov.hu/it-biztonsag/hirek/a-sandworm-apt-csoport-sikertelen-kibertamadast-hajtott-vegre-egy-ukran-energiaszolgaltato-ellen/. [Hozzáférés dátuma: 5 május 2023].

[63] S. Bhamidipati, „The Art of Reconnaissance - Simple Techniques," SANS, Budapest, 2001.

[64] „NY Post," 7 Március 2022. [Online]. Available: https://nypost.com/2022/03/07/anonymous-hacks-russian-state-tv-with-footage-of-ukraine-war. [Hozzáférés dátuma: 5 május 2023].

[65] Nemzeti Közszolgálati Egetem online lexikon: Információs hadviselés. https://lexikon.uni-nke.hu/szocikk/informacios-hadviseles/ [Hozzáférés dátuma: 5 május 2023].

[66] James Mahoney és Daniel Schensul: Historical Context and Path Dependence. Oxford University Press, 2006.

[67] João Correia: Military capabilities and the strategic planning conundrum, Security and Defence Quarterly ISSN 2300-8741 eISSN 2544-994X 2019 June Volume 24 Number 2 https://doi.org/10.35467/sdq/108667

[68] Cherie Noteboom et al.: Agile Project Management: A Systematic Literature Review of Adoption Drivers and Critical Success Factors, Proceedings of the 54th Hawaii International Conference on System Sciences | 2021, https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/37cf9dea-7864-4a93-ab68-b52e44488e53/content (Látogatás dátuma: 2022. 04. 05.)

[69] Helena Carrapico és André Barrinha: The EU as a Coherent (Cyber)Security Actor?, Journal of Common Market Studies, 2017., 55. évf. 6. sz., https://doi.org/10.1111/jcms.12575, pp. 1254-1272.

[70] EEAS: 706 REV4: European Union Military Vision and Strategy on Cyberspace as a Domain of Operations, 2021, https://www.statewatch.org/media/2879/eu-eeas-military-vision-cyberspace-2021-706-rev4.pdf (Látogatás dátuma: 2022. 04. 05.)

[71] Max Smeets, 'The Strategic Promise of Offensive Cyber Operations', Strategic Studies Quarterly 12:3 (2018).

[72] Herb Lin: 'Thinking about Nuclear and Cyber Conflict: Same Questions, Different Answers', (Lecture, Hoover Institution/Center for International Security and Cooperation, Stanford University, CA, 2015, May 15),

https://sipa.columbia.edu/sites/default/files/Thinking%20about%20Nuclear%20and%20Cyber%20Conflict-Columbia-2015-05-14.pdf. (Látogatás dátuma: 2022. 09. 01.)

[73] Adam P. Liff (2012) Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War, Journal of Strategic Studies, 35:3, 401–428, DOI: 10.1080/01402390.2012.663252

[74] Lennart Maschmeyer; The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. International Security 2021; 46 (2): 51–90. doi: https://doi.org/10.1162/isec_a_00418

[75] Harold R. Winton, "On Military Change" in David R. Mets és Harold R. Winton (szerk.): The Challenge of Military Change, University of Nebraska, 2000.

[76] Thomas Parker és Warren Parker: Cyber Warfare Doctrine Already Exists, US Naval Institute Proceedings, 2019, Vo. 145 (2). https://www.usni.org/magazines/proceedings/2019/february/cyber-warfare-doctrine-already-exists (Látogatás dátuma: 2022. 03. 03.)

[77] The national cybersecurity strategy 2021–2025. https://ccdcoe.org/uploads/2018/10/Slovakia_National_Cybersecurity_Strategy-2021-2025_2021_English.pdf (látogatás dátuma: 2022. 07. 10.)

[78] Cybersecurity Strategy of the Republic of Poland 2019–2024. https://www.cyberwiser.eu/sites/default/files/Poland_Strategia_Cyberbezpieczeństwa_RP_w_języku_angielskim.pdf (látogatás dátuma: 2022. 07. 10.)

[79] Issie Lapowsky, "The Pentagon is Building a Dream Team;" "AUSA Cyber Hot Topic 2018, Panel 3: Cyber Support to Corps and Below.", https://www.wired.com/story/pentagon-dream-team-tech-savvy-soldiers/ (Látogatás dátuma: 2022. 02. 22.)

[80] Joint Publication 3-12: Cyberspace Operations II-4 – II-6., 2018 június 8. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (Látogatás dátuma: 2022. 05. 03.)

[81] Max Smeets: NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis, Elérhető: https://ccdcoe.org/uploads/2019/06/Art_09_NATO-Members-Organizational-Path.pdf (A letöltés dátuma: 2020. szeptember 9.)

[82] Tomas Minarik: Nationa Cybersecurity Organisation: Czech Republic, 2016. NATO CCDCOE. https://ccdcoe.org/uploads/2018/10/CS_organisation_CZE_032016.pdf (látogatás dátuma: 2022. 05.03.)

[83] Ministry of Defence and Armed Forces of the Czech Republic: Cyber Forces Command. https://www.army.cz/en/armed-forces/organisational-structure/cyb/cyber-forces-command-218593/ (Látogatás dátuma: 2022. 06.01.)

[84] Brita Achberger és Max Smeets: The Opportunities and Challenges of Military Cyber Exercises, 2022. 03. 24., Council on Foreign Relations, https://www.cfr.org/blog/opportunities-and-challenges-military-cyber-exercises (Látogatás dátuma: 2022. 06.01.)

[85] Jennie W. Wenger, Caolionn O'Connell és Maria C. Lytell: Retaining the Army's Cyber Expertise. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1978.html. (Látogatás dátuma: 2022. 09. 02.)

[86] Chad Bates és Charlene Rose: UNDERSTANDING—AND FIXING—THE ARMY'S CHALLENGE IN KEEPING CYBER TALENT, Modern Institue of War at the West Point, 2022. 05. 17., https://mwi.usma.edu/understanding-and-fixing-the-armys-challenge-in-keeping-cyber-talent/ (Látogatás dátuma: 2022. 09. 09.)

[87] Josh Lospinoso, "Fish Out of Water: How the Military Is An Impossible Place for Hackers, and What to Do About It," War On the Rocks, 2018.07., https://warontherocks.com/2018/07/fish-out-of-water-how-the-military-is-an-impossible-place-for- hackers-and-what-to-do-about-it/ (Látogatás dátuma: 2022. 10. 01.)

[88] Siena Anstis, Government procurement law and hacking technology: The role of public contracting in regulating an invisible market, Computer Law & Security Review, Volume 41, 2021, https://doi.org/10.1016/j.clsr.2021.105536.

[89] Kiáltvány az agilis szoftverfejlesztésért, https://agilemanifesto.org/iso/hu/manifesto.html (Látogatás dátuma: 2022. 09. 10.)

[90] Principles behind the Agile Manifesto, https://agilemanifesto.org/principles.html, (Látogatás dátuma: 2022. 09. 10.)

[91] WHAT IS THE PLAN-DO-CHECK-ACT (PDCA) CYCLE? https://asq.org/quality-resources/pdca-cycle (Látogatás dátuma: 2022. 09. 10.)

[92] Martin Dufour: Will artificial intelligence challenge NATO interoperability?, NDC Brief, 2018. https://www.ndc.nato.int/news/news.php?icode=1239 (Látogatás dátuma: 2022. 10. 10.)

[93] Dr. Linda Jones: DEFENSE ACQUISITION UNIVERSITY SCRUM IMPLEMENTATION FOR ARMY Lessons Learned, 2022. 05. 05. https://www.dau.edu/Lists/Events/Attachments/590/DCO-SCRUM-DAU%205.5.22.pdf (Látogatás dátuma: 2022. 10. 12.)

[94] Ambrus Éva: A kiberképességekhez szükséges szervezeti háttér
In: Hausner, Gábor (szerk.): Szemelvények a katonai műszaki tudományok eredményeiből II. Budapest, Magyarország : Ludovika Egyetemi Kiadó (2021) 347 p. pp. 11–25. , 15 p.

[95] Steven J. Anderson: Airpower Lessons for an Air Force Cyber-Power Targeting Theory. Drew Paper No. 23, Air University Press, 2016, ISBN 9781585662388

[96] Graham Allison és Philip Zelikow, Essence of Decision: Explaining the Cuban Missile Crisis (2nd Edition), New York: Longman, 1999.

[97] Posen, The Sources of Military Innovation. Cornell University Press, 2014.

[98] Stephen Rosen: Winning the Next war: Innovation and the Modern military. Cornell University Press, 1994.

[99] Mahnken, Uncovering Ways of War: U.S. Intelligence and Foreign Military Innovation, 1918–1941, Cornell University Press, 2002.

[100] Morton H. Halperin, Bureaucratic Politics and Foreign Policy, Brookings Institution Press, 2002.

[101] John A. Nagl, Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam, Chicago: The University of Chicago Press, 2002.

[102] Austin Long, The Soul of Armies: Counterinsurgency Doctrine and Military Culture in the U.S. and U.K. New York: Cornell University Press, 2016.

[103] Terry C. Pierce, Warfighting and Disruptive Technologies: Disguising Innovation, New York: Frank Cass, 2004.

[104] Zachary M. Smith: Airpower History and the Cyber Force of the Future
How Organization for the Cyber Domain Outpaced Strategic Thinking and Forgot the Lessons of the Past, 2016. MA thesis. https://apps.dtic.mil/sti/pdfs/AD1031578.pdf

[105] U.S. DEPARTMENT OF DEFENSE, THE DICTIONARY OF MILITARY TERMS 261 (2009).

[106] B. Müller Tamás: KIBERHADVISELÉS ÉS KATONAI KIBERVÉDELEM, infojegyzet, 2019/49. ORSZÁGGYŰLÉS HIVATALA, KÉPVISELŐI INFORMÁCIÓS SZOLGÁLAT,
https://www.parlament.hu/documents/10181/1789217/Infojegyzet_2019_49_Kiberhadviseles.pdf/11686cc6-54a5-8388-87db-54233ab8a32d?t=1573810309857 (látogatás dátuma: 2022. 01. 22.)

[107] Daniele Moore: Offensive Cyber Operations: Understanding Intangible Warfare, Oxford University Press, 2022.

[108] William A. Owens, Kenneth W. Dam,és Herbert S. Lin, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, Washington, DC: The National Academies Press, 2009.

[108] Kovács László: Hadviselés a 21. században: kiberműveletek, Budapest, Ludovika Egyetemi Kiadó 2023.

[109] Crowdstrike: WHAT IS THE CYBER KILL CHAIN? PROCESS & MODEL, https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/ (Látogatás dátuma: 2022. 07.07.)

[110] Mica R.Endsley: Situation awareness global assessment technique(SAGAT). In Aerospace and Electronics Conference, 1988. Proceedings of the IEEE, 789–795. 1988.

[111] Claire Laudy: Semantic Knowledge Representations for Soft Data Fusion, 2011, In book: Efficient Decision Support Systems – Practice and Challenges From Current to Future. DOI:10.5772/17762

[112] Munir, Arslan, Alexander Aved, and Erik Blasch. 2022. "Situational Awareness: Techniques, Challenges, and Prospects" AI 3, no. 1: 55–77. https://doi.org/10.3390/ai3010005

[113] Solti I.: Az OSINT információgyűjtő eszközeiről, Nemzetbiztonsági Szemle, 7. évfolyam (2019) 2. szám

[114] Vadász P.: Információkeresés a nyílt forrású hírszerzésben, Felderítő Szemle, 14. évfolyam 1. szám 2015. március, http://www.knbsz.gov.hu/hu/letoltes/fsz/2015-1.pdf

[115] VIDA CS.: A hírszerzés. In: Resperger I. (szerk.) A nemzetbiztonság elmélete a közszolgálatban, Dialóg Campus Kiadó, Budapest, 2018.

[116] MERCADO, S. C. : Reexamining the Distinction Between Open Information and Secrets, Studies in intelligence, vol. 49. no.2., 2007, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi- publications/csi-studies/studies/Vol49no2/reexamining_the_distinction_3.htm

[117] INFORMATORIUM: Információs túltelítődés – Information overload, szó-kalauz, 2016, http://www.bgalapitvany.hu/2016/05/informacios-tultelitodes-information-overload/

[118] ELDRIDGE, C., HOBBS, C. & MORAN, M.: Fusing algorithms and analysts: open-source intelligence in the age of ‘Big Data’, Intelligence and National Security, 2017, https://kclpure.kcl.ac.uk/portal/files/108996612/Fusing_Algorithms_and_Analysts_ELDRIDGE_Published_Onli ne_2017_GREEN_AAM.pdf

[119] P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning et al.: “Cyber sa: Situational awareness for cyber defense,” in Cyber situational awareness, pp. 3–13.Springer, 2010.

[120] Hooman Alavizadeh et al.: A Survey on Threat Situation Awareness Systems: Framework, Techniques, and Insights, 2021. https://arxiv.org/pdf/2110.15747.pdf (Látogatás dátuma: 2022. 10. 11.)

[121] Tactical Operations Center. https://man.fas.org/dod-101/sys/land/wsh/246.pdf (látogatás dátuma: 2022. 11.03.)

[122] Earl D. Matthews, Dr. Harold J. Arata III és Brian L. Hale: Cyber Situation Awareness. Cyber Defense Review. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Cyber%20Situational%20Awareness_Matthews_Arata_Hale.pdf?ver=2018-07-31-093724-720 (látogatás dátuma: 2022. 10. 10.)

[123] Mark Pomerleau: The US Army will soon be able to see itself in cyberspace on the battlefield, 2021. https://www.c4isrnet.com/cyber/2021/10/11/the-us-army-will-soon-be-able-to-see-itself-in-cyberspace-on-the-battlefield/ (Látogatás dátuma: 2022. 11. 05.)

[124] Mark Pomerleau: Army set to field new cyber tool to improve situational awareness, https://www.fedscoop.com/army-set-to-field-new-cyber-tool-to-improve-situational-awareness/ (Látogatás dátuma: 2022. 11. 07.)

[125] Prof. dr. Kovács László előadásából (2022.04.11.)

[126] Wolters Kluwer, „Netjogtár,” 2013. [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv. [Hozzáférés dátuma: 5 május 2023].

[127] Z. Kovács, „Kibervédelem és biztonság,” in *Kibervédelem a bűnügyi tudományokban*, Budapest, Dialóg Campus, 2020, pp. 65-89.

[128] Magyarország Kormánya, „Nemzeti Kiberbiztonsági Koordinációs Tanács,” 2011. [Online]. Available: https://cybersecurity.me.gov.hu/. [Hozzáférés dátuma: 5 május 2023].

[129] NKI, „Nemzeti Kibervédelmi Intézet,” [Online]. Available: https://nki.gov.hu/. [Hozzáférés dátuma: 5 május 2023].

[130] Rendőrség, „Készenléti rendőrség,” 2023. [Online]. Available: https://www.police.hu/hu/a-rendorsegrol/testulet/teruleti-szervek/keszenleti-rendorseg. [Hozzáférés dátuma: 5 május 2023].

[131] 2011. évi CXIII. Törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről, 2011.

[132] 40/A. A katonai kibertér műveletekre vonatkozó különös szabályok, 62/A. § pont.

[133] Magyarország Nemzeti Katonai Stratégiája, 2012.

[134] 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról, 2013.

[135] Benkő Tibor: A Magyar Honvédség jelene és jövője. Elérhető: http://mhtt.eu/hadtudomany/2019/2019_1_2/2019eA%20Magyar%20Honvédseg%20jelene_Benko%20Tibor.pd f (A letöltés dátuma 2020. szeptember 2.)

[136] Kovács László: Kiberbiztonság és Stratégia, Budapest, Dialóg Campus, 2018.F

[137] 81/2011. (VII. 29.) HM utasítás a honvédelmi tárca Kibernetikai Védelmi Koncepció kialakításához szükséges feladatok meghatározásáról, 3. §. (5–6)

[138] 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról.

[139] 16/2013. (VIII. 30.) HM rendelet a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről (hatályon kívül).

[140] 22/2016. (II. 17.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet módosításáról, 1. §.

[141] Honvedelem.hu: Fókuszban a Kiberbiztonság. 2021. https://honvedelem.hu/hirek/fokuszban-a- kiberbiztonsag.html (látogatás dátuma: 2022. 07.07.)

[142] 1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról

[143] 259/2021. (V. 20.) Korm. rendelet a közbiztonság erősítése érdekében egyes kormányrendeletek módosításáról, 26. §. (3)

[144] 3/2022. (I. 27.) HM utasítás a honvédelmi szervezet 2022. évi kiemelt feladatainak, valamint a 2023– 2024. évi fő célkitűzéseinek meghatározásáról;

[145] Honvedelem.hu: Megpróbálunk felkészülni mindenre. https://honvedelem.hu/hirek/megprobalunk-felkeszulni-mindenre.html (Látogatás dátuma: 2022. 11. 30.)

[145] Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában, Honvédségi Szemle 2020 évi 5. szám, 3–18. DOI: 10.35926/HSZ.2020.5.1,

[146] Rain Liivoja - Maarja Naagel - Ann Väljataga: Autonomous Cyber Capabilities under International Law, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Elérhetőség: https://ccdcoe.org/uploads/2019/07/Autonomy-in-Cyber-Capabilities-under-International-Law_260619-002.pdf (A letöltés dátuma 2020. szeptember 6.)

[147] Dorothy E. Denning: ‘Framework and Principles for Active Cyber Defence’ Computers & Security vol. 40. 2013.

[148] Draveczki-Ury Ádám: „Egy korszerű harckocsi is számítógép-hálózat, csak 70 tonna vas veszi körül”, honvedelem.hu, https://honvedelem.hu/hirek/hazai-hirek/egy-korszeru-harckocsi-is-szamitogep-halozat-csak-70-tonna-vas-veszi-korul.html
(A letöltés dátuma 2022. szeptember 6.)

[149] Jegyzőkönyv az Országgyűlés Honvédelmi és rendészeti bizottságának 2020. december 8-án, kedden, 11 óra 04 perckor az Országház Széll Kálmán termében (főemelet 64.) megtartott, részben zárt üléséről p. 29. https://www.parlament.hu/documents/static/biz41/bizjkv41/HOB/2012081.pdf

[150] 1995. évi CXXV. Törvény a nemzetbiztonsági szolgálatokról: 6. § g) pont

[151] Szentgáli Gergely: Csendben szolgálni, Hadtudomány, 3–4. szám Elérhető: http://real.mtak.hu/29827/1/2015_3_4_8.pdf (A letöltés dátuma 2020. szeptember 7.)

[152] Honvédelmi Minisztérium költségvetés 2020. Országgyűlés. Elérhető: https://www.parlament.hu/irom41/10710/adatok/fejezetek/13.pdf (A letöltés dátuma 2020. szeptember 7.)

[153] A Magyar Honvédség Parancsnoksága (2020), honvedelem.hu, Elérhető: https://honvedelem.hu/a-magyar- honvedseg-parancsnoksaga.html (A letöltés dátuma 2020. szeptember 7.

[154] Ambrus Éva: Lehetőségek a magyar kiberműveleti képességek fejlesztérésre in Taktikák és stratégiák a kiberhadviselésben (szerk. Krasznay Csaba), Ludovika Egyetemi Kiadó, Budaepst, 2023.

[155] Magyar Kereskedelmi és Iparkamara Exportkalauz, https://mkikexport.uzletahalon.hu/?q=exportprojekt/elemzes/fogalomtar

[156] Mező András: A katonai stratégiaalkotás és doktrínafejlesztés Magyarországon Doktori (PhD) értekezés, Budapest, 2019. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12585/mezo_andras_doktori_ertekezes_2019.pdf;jsessionid=39007A318C3A6C89D154FEA2A84F25BA?sequence=1

[157] Hertelendi L. & Hornyik Zs. (2022). „A kiberbiztonság jelentősége a mindennapokban". Inter- jú Kovács László dandártábornokkal, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Karának egyetemi tanárával. Belügyi Szemle, 70(6), 1327–1337. https://doi.org/10.38146/BSZ.2022.6.11 pp. 1333-1334

[158] Nemzeti Kibervédelmi Intézet: Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve 2022 (SecOnSys) https://seconsys.eu/wp-content/uploads/2023/02/SeConSys_kezikonyv_aktual_2023_jan.pdf

[159] Politico: https://www.politico.eu/article/is-there-a-war-on-big-eu-powers-miss-nato-spending-targets-again-allies/

[160] Tobias Liebetrau (2022) Cyber conflict short of war: a European strategic vacuum, European Security, 31:4,497-516, DOI: 10.1080/09662839.2022.2031991

[161] Spitzer Jenő, Vikman László: A honvédelmi szabályozás egyes lehetséges külföldi mintáinak áttekintése, Védelmi-Biztonsági szabályozási és kormányzástani műhelytanulmányok, 2022/31., https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK%20MT_2022_31_SPITZER%20Jenő_VIKMAN%20László_A%20honvédelmi%20szabályozás%20egyes%20lehetséges%20külföldi%20mintáinak%20áttekintése.pdf

[162] Nemzeti Kibervédelmi Intézet: Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve 2022 (SecOnSys) https://seconsys.eu/wp-content/uploads/2023/02/SeConSys_kezikonyv_aktual_2023_jan.pdf

Ábrajegyzék

Fogalmak és rövidítések jegyzéke

5V: volume, variety, velocity, veracity viability, visualization.

APT: advanced persistent threat

C2: command and control

CAIH: cyber academia and innovation hub

CERT: cyber emergency response team

CIDCC: cyber and innovation coordination center

CIR: cyber und informationsraum

CISA: cybersecurity and infrastructure security sgency

CISIO: communication and information system infrastructure operations

CISRO: cyberspace intelligence, surveillance and reconnaissance operations

CNO: computer network operation

COP: cyber operational picture

CPS: cyber-physical system

CRF: cyber ranges federation

CRRT: cyber rapid response team

CTI: cyber threat intelligence

CTIRISP: cyber threats and incident response information sharing platform

CSA: cyber situational awareness

CSIRT: cyber security incident respone team

DCO: defensive cyber operations

DDOS: distributed denial of service

DOTLMPF: doctrine, organization, training, materiel, leadership, personnel and facilities,

ENISA: european network and information security agency

FIRST: forum of incident response and security teams

TI: trusted introducer

IWWN: international watch and warning network,

CECSP: central european cyber security platform

ENSZ: Egyesült Nemzetek Szövetsége

EU: Európai Unió

GEOINT: geospatial intelligence

IKT: infokommunikációs technológia

IOC: initial operational capability

IT: információs technológia

JSOC: joint security operations center

KBVP: közös biztonság és védelempolitika

MDO: multidomain operaitons

NATO CCDCOE: North Atlantic Threaty Organization Cyber Cooperative Cyber Defense Centre of Excellence

NATO: North Atlantic Threaty Organization

NCIRC: NATO's Computer Incident Response Capability

OCO: offensive cyber operations

OSINT: open source intelligence

PLC: programmable logic controller

PESCO: permanent structured cooperation

PETIO: people, exploits, toolset, infrastructure and organization

SA: sitautional awareness

SIGINT: signals intelligence

SOC: security operation center

STRATCOM: strategic communications

SWOT: strenght, weakness, opoortunity, threat

TOC: tactical operational center

TRADOC: US Army Training and Doctrinal Command

TTP: tactics, techniques and procedures

V4: Visegrádi Együttműködés