HADMÉRNÖK
VÉDELEMINFORMATIKA
21. évfolyam (2026) 1. szám 57–75.
DOI: 10.32567/hm.2026.1.4

Pozderka Gábor[1]

A kibertér sajátosságából adódó civil–katonai kapcsolatok vizsgálata

Examination of Civil-Military Relations Arising from the Specificity of Cyberspace

Absztrakt

A civil–katonai kapcsolatok már a civilizációk kialakulásának kezdeti szakaszában is jelen voltak, irányaikat kijelölték az adott korszakra jellemző uralkodói és társadalmi elvárások. Jelen publikáció célja annak a folyamatnak a vizsgálata, hogy a 20. és 21. században kialakult civil–katonai kapcsolatok milyen módon alakultak át a kibertérben felerősödő folyamatok hatására, illetve a jövőben milyen speciális feladatokra kell felkészülnie a katonai szektornak a műveleti feladat-végrehajtás sikeressége érdekében. A civil szektor támogatása nélkül a jelen kor katonai műveletei már nem hajthatók végre, ennek érdekében a szükséges együttműködési platformokat ki kell alakítani, a közös feladat-végrehajtás kereteit ki kell dolgozni. Kiemelt figyelmet kell fordítani a folyamatok begyakoroltatására, ennek érdekében közös nemzeti és nemzetközi gyakorlatok tervezése és végrehajtása szükséges.

Kulcsszavak: civil–katonai kapcsolatok, kibertér, együttműködés, információmegosztás

Abstract

Civil-military relations were already present in the early stages of the formation of civilisations, and their directions were determined by the characteristics of the ruler and social expectations of the given era. The aim of this publication is to examine the process of how civil–military relations transformed in the 20th and 21st centuries as a result of the intensifying processes in cyberspace, and what special tasks the military sector should prepare for in the future

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: pozderka.gabor@hm.gov.hu

in order to be successful in the execution of operational tasks. Without the support of the civilian sector, the military operations of the present era can no longer be carried out, and in order to achieve this, the necessary cooperation platforms must be established and the framework for joint task execution must be developed. Special attention must be paid to the practice of the processes, for which joint national and international practices must be planned and implemented.

Keywords: civil–military relations, cyberspace, cooperation, information sharing

Bevezetés

Az információs és kommunikációs technológiák rohamos fejlődése az elmúlt évtizedekben alapjaiban formálta át a nemzetbiztonsági környezetet. A kibertér nem csupán új műveleti térként jelent meg, hanem olyan komplex térként, ahol a katonai és civil szereplők kapcsolatrendszere, döntéshozatali mechanizmusai és stratégiai tervei alapjaiban változtak meg.[2] Míg a hagyományos hadszíntéren a szereplők hierarchikus, jól meghatározott viszonyok alapján működtek, a kibertérben a határok elmosódnak, a szereplők változatosak és gyakran nehezen beazonosíthatók. Ez a környezet komoly kihívás elé állítja a civil–katonai kapcsolatok hagyományos modelljeit. Az évszázadok során kialakult CIMIC,[3] amely eddig főként békeműveletek és válságkezelés során bizonyított, a digitális térben újfajta adaptációt igényel az új típusú kihívások hatékony kezelése érdekében. Tradicionálisan a CIMIC szerepe abban áll, hogy a civil infrastruktúra, a humanitárius szervezetek, helyi hatóságok és más nem katonai szereplők működését összhangba hozza a katonai tevékenységekkel, különösen válságkezelési és konfliktusmegoldási környezetben.[4] A 21. század digitális kihívásai új dimenziókat adtak ehhez a hagyományosan fizikai térben működő szakterülethez. A tanulmány célja, hogy feltárja a kibertér sajátosságait, bemutassa a civil–katonai kapcsolatok átalakulását, és javaslatot adjon arra, hogy a CIMIC az információs műveletek részeként miként tud hatékonyan alkalmazkodni a kibertér követelményeihez, miközben biztosítja a katonai célok és a társadalmi érdekek egyensúlyát.

A kibertér, amely magában foglalja az információs és kommunikációs rendszereket, hálózatokat és adatfeldolgozó egységeket, egyre fontosabb operatív környezetté válik nemcsak a katonai, hanem a civil szereplők számára is – különösen mivel a kritikus infrastruktúra[5] és a közszolgáltatások nagymértékben függenek a digitális rendszerektől.[6] A kibertér működését a hagyományos hadszíntértől alapvetően három tényező különbözteti meg: a téridő nemlinearitása, a technológiák kettős felhasználhatósága és a szereplők sokszínűsége. Ezen tényezők hatékony kezelése és integrálása a korábban kialakított eljárásrendekbe nélkülözhetetlen érdek a siker érdekében, az erőforrás-menedzsment részeként szükséges megvizsgálni a meglévő erőforrások egy időben történő felhasználását, szükség szerint újrafelosztását.

[2] Clarke–Knake 2019.
[3] CIMIC, Civil–Military Cooperation.
[4] NATO Standardization Office 2025.
[5] Hunorfi–Farkas 2025.
[6] Haig 2023.

A kibertér sajátosságai

A téridő dimenzió elmosódása azt jelenti, hogy egy kibertámadás vagy információáramlás percek alatt globálisan hat, függetlenül a földrajzi elhelyezkedéstől, a rendszer viselkedése bonyolultabb, és kis változások is okozhatnak nagy vagy váratlan hatásokat. Ez a sajátosság alapvetően változtatja meg a stratégiai tervezést, hiszen a hagyományos logika, miszerint a fenyegetések fizikailag pontosan beazonosíthatók, a kibertérben már nem, vagy csak csekély mértékben érvényesek.

A technológiai eszközök kettős felhasználása szintén bonyolítja a helyzetet. Egyes platformok és szoftverek egyszerre szolgálhatnak katonai és civil célokat, legyen szó adatfeldolgozásról, kommunikációról vagy fenyegetésfelderítésről. Ez a kettős jelleg jogi, etikai és stratégiai kérdéseket vet fel, hiszen a civil felhasználásra szánt eszközök katonai alkalmazása felelősség- és hatáskörproblémákat generálhat. Ez a problémakör már a kezdeti lépéseknél megjelenik, hiszen a fejlesztések során felmerülhetnek olyan speciális katonai ágazati igények, amelyek a civil szektor részére nem jelentenek prioritást, így erőforrásokat szükséges átcsoportosítani, esetlegesen elvonni. A gyors technológiai fejlődés és a folyamatos innováció miatt a védekezési mechanizmusok is állandóan változnak. Amit ma hatékony védelemnek tekintünk, az rövid időn belül elavult lehet. Ez különösen a kritikus infrastruktúrák védelmében és a katonai információbiztonság terén jelent komoly kihívást. A civil és katonai szervezeteknek folyamatosan frissíteniük kell eljárásrendjeiket, és rendszeres képzéseket, gyakorlatokat kell biztosítaniuk a személyzet számára, természetesen ennek érdekében biztosítani kell a források rendelkezésre állását.

A szereplők sokszínűsége a kibertérben azt jelenti, hogy nemcsak állami szereplők, hanem magánvállalatok, civil kutatóintézetek, önkéntes csoportok és hacktivisták[7] is képesek befolyásolni a nemzetbiztonsági helyzetet. A civil szereplők között találjuk a kritikus infrastruktúrákat üzemeltető vállalatokat, informatikai cégeket, kutatóintézeteket, nonprofit szervezeteket és különböző szakmai közösségeket, míg a katonai oldalon a fegyveres erők és a nemzetbiztonsági szervezetek biztosítják a stratégiai felügyeletet és a reagálást. A képet tovább árnyalja, hogy egyes szeplők szerepkörei keveredhetnek egymással, a megszerzett tudás birtokában akár szerepkört is válthatnak, amivel alapjaiban változtathatják meg a korábban kialakult erőviszonyokat. Egy támadás forrása gyakran nehezen azonosítható, a motivációk és a hatások pedig összetettek.[8] A civil–katonai kapcsolatokban ezért olyan mechanizmusokat kell kialakítani, amelyek figyelembe veszik e sokszereplős környezetet, és lehetővé teszik a hatékony koordinációt, az információmegosztást és a gyors reagálást a fenyegetésekre.

Civil–katonai kapcsolatok a kibertérben

A civil–katonai kapcsolatok hagyományosan a békeműveletek, válságkezelés és humanitárius segítségnyújtás során a hatékony koordinációt, információmegosztást

[7] Krasznay 2024.
[8] Deibert 2003.

és erőforrás-optimalizálást szolgálják. A kibertérben azonban a kapcsolatok új jelentést kapnak, ez a folyamat a digitalizáció elterjedésével már korábban megkezdődött, a civil IT és logisztikai szolgáltatók már jelenleg is szoros kapcsolati hálót alakítottak ki a katonai ágazattal, nélkülük a kommunikáció és logisztikai ellátás már elképzelhetetlen. A katonai és civil szereplők közötti kommunikáció és együttműködés gyorsasága és pontossága élet-halál kérdése lehet, hiszen egy kibertámadás percek alatt jelentős károkat okozhat, legyen szó állami rendszerek, kritikus infrastruktúrák vagy magáncégek működésének megbénításáról.

A közös szabványok és protokollok kialakítása elengedhetetlen, mivel a civil és katonai szervezetek működési mechanizmusai eltérők, összehangolásuk nélkül a hatékony válaszadás nem biztosítható. Emellett a képzés és tudatosság növelése is nélkülözhetetlen. A kibertér folyamatosan változó fenyegetései miatt a szereplőknek rendszeresen kell gyakorolniuk a reagálást, szimulációkat végezniük, és közös munkacsoportok keretében fejleszteni a kommunikációs készségeket. A civil–katonai együttműködés tehát nem csupán technikai vagy stratégiai kérdés, hanem folyamatos emberi és szervezeti tanulási folyamat is.

A hagyományos CIMIC-hálózatok hierarchikus, lineáris kapcsolati struktúrákra épültek, ahol a feladatok és felelősségek jól meghatározottak voltak. A kibertér azonban ezzel szemben dinamikus, gyorsan változó és sokszereplős, így a CIMIC-nek alkalmazkodnia kell ehhez a környezethez. A megújulási folyamat részeként, nem csupán új eljárásrendekre van szükség, hanem egy olyan működési szemléletre, amely képes kezelni a valós idejű fenyegetéseket, integrálni a különböző szereplők tapasztalatait és biztosítani a gyors, koordinált válaszlépéseket.[9] A CIMIC jövőbeni szakértőinek így kettős kompetenciával kell rendelkezniük: egyszerre kell érteniük a hagyományos civil–katonai együttműködés működéséhez és a kiberműveletek sajátosságaihoz. Csak így képesek hidat képezni a katonai célok és a társadalmi érdekek között, miközben a civil lakosság és a kritikus infrastruktúrák védelme is biztosított marad.[10] A CIMIC szerepe a kibertérben tehát nem csupán koordinációs, hanem stratégiai is: az adaptív, hálózatszerű működés lehetővé teszi, hogy a civil és katonai szereplők integrált, rugalmas kiberhálóban működjenek együtt, amely gyorsan alkalmazkodik a folyamatosan változó fenyegetésekhez. A cél ezzel egyértelmű: olyan civil–katonai kiberháló kialakítása, amely elősegíti a közös kiberbiztonsági tudatosságot, növeli a rezilienciát, és hosszú távon fenntartható módon biztosítja a katonai célok és a társadalmi igények egyensúlyát.[11]

Civil és katonai szereplők a kibertérben

A kibertér civil szereplői rendkívül sokszínűek, és tevékenységük közvetlenül vagy közvetve befolyásolja a nemzetbiztonságot. A kritikus infrastruktúrákat üzemeltető vállalatok elsőként érzékelhetik a kibertámadásokat, legyen szó energiaellátásról,

[9] NATO Standardization Office 2025.
[10] NATO CIMIC Centre of Excellence 2025b.
[11] Kott et al. 2018.

közlekedési rendszerekről vagy kommunikációs hálózatokról. Ők rendelkeznek azzal a technikai szakértelemmel és adatokkal, amelyek lehetővé teszik a támadások gyors azonosítását és a hatékony reagálást. Ugyanakkor nem csak a nagyvállalatok számítanak aktív szereplőnek; a kutatóintézetek és egyetemek például folyamatosan fejlesztik a fenyegetés felderítéséhez szükséges módszereket, modellezik a kibertámadások hatásait, és így közvetlenül járulnak hozzá a kiberbiztonsági innovációhoz. Nonprofit szervezetek, szakmai közösségek és hacktivista csoportok pedig gyakran reagálnak gyorsabban, mint a formális állami struktúrák, különösen az incidensek korai szakaszában. Ez a sokszínűség előnyökkel és kihívásokkal is jár. A civil szereplők gyakran nem kötődnek központi parancsstruktúrához, és működésük eltérő szabályok, jogi és etikai keretek szerint zajlik. A katonai és állami szervezeteknek ezért rugalmasan kell kezelniük ezeket az interakciókat, miközben biztosítaniuk kell a gyors információáramlást és a koordinált reagálást.

A katonai és nemzetbiztonsági szervezetek feladata a kibervédelemben elsősorban a stratégiai tervezés, a fenyegetések azonosítása és a gyors reagálás biztosítása. Ők képezik a struktúrát, amely a különböző civil információforrásokat rendszerezi és integrálja a védelmi mechanizmusokba. A katonai szereplőknek a kibertérben nem elég a hagyományos parancs-irányítási logikát követniük, mert a fenyegetések gyorsan változnak, és sok esetben decentralizált vagy nem állami szereplőktől erednek. Ebben a környezetben a koordinációs mechanizmusok rendkívül fontosak. Például egy kritikus infrastruktúrát ért támadás esetén a civil üzemeltetők adatait össze kell hangolni a katonai fenyegetésfelderítéssel és az állami reagálási protokollokkal. A koordináció célja, hogy minden résztvevő számára világos legyen a szerepe, ugyanakkor a döntéshozatal gyors és adaptív maradjon. E mechanizmusok közé tartozik a közös incidenskezelési protokollok kidolgozása, valós idejű információcsere, valamint a rendszeres közös gyakorlatok és szimulációk szervezése. Fontos kialakítani a bizalmi hálót és biztonságos technikai platformokat, ellenkező esetben a hatékony reagálás nem lesz lehetséges.

A civil és katonai szereplők együttműködésének gyakorlati modelljei különbözők lehetnek. Egyes esetekben központi koordináció érvényesül, ahol állami vagy katonai egység gyűjti össze a civil és katonai információkat, elemzi azokat, és koordinált válaszlépéseket kezdeményez együttműködésben a civil szereplőkkel. Ez a modell előnyös a stratégiai irányítás és a konszolidált döntéshozatal szempontjából, ugyanakkor korlátozott rugalmassággal rendelkezik, különösen a helyi incidensek gyors kezelésében. Más esetekben decentralizált, hálózatszerű működés alakul ki, ahol a civil és katonai szereplők közvetlenül kommunikálnak egymással. Itt a koordinációs mechanizmusok segítő jellegűek, a hangsúly a gyors reagáláson, a helyi adaptáción és a folyamatos információmegosztáson van. Ez a modell előnyös a gyors fenyegetésfelderítésnél és az innovatív megoldások alkalmazásánál, ugyanakkor nagyobb felelősséget követel a résztvevőktől, mivel a döntések decentralizáltak. A gyakorlatban gyakran hibrid megoldások alkalmazhatók,[12] amelyek kombinálják a központi koordináció előnyeit a hálózatszerű rugalmassággal. Ebben a struktúrában a CIMIC például szerepelhet a civil–katonai koordináció egyik elemeként, de nem kizárólagos mechanizmusként,

[12] Resperger–Kiss–Somkuti 2014.

hanem a partnerségi kapcsolatok és információmegosztás biztosítására. A hangsúly azonban a rendszer sokszereplős, adaptív jellegén van, ahol a katonai és civil szereplők egyenrangú, de különböző funkciókkal rendelkező partnerek. Az azonban minden esetben kijelenthető, hogy a kapcsolati háló kialakítása és naprakészen tartása, valamint a folyamatok készségszintű begyakorlása kulcsfontosságú lesz a feladat-végrehajtás során; ha ez nem történik meg egy esemény bekövetkezése előtt, akkor arra az esemény kezelése közben már nem lesz lehetőség.[13]

Az országok katonai kiberparancsnokai kulcsszereplők a modern hadsereg és a kormányzat digitális biztonságának fenntartásában. Ez a funkció mind a NATO, mind az EU[14] esetében a nemzetek által dedikált funkcióként jelenik meg. Elsődleges feladatuk a katonai kibertér műveleti erők irányítása és koordinálása.[15] Ugyanakkor szerepük messze túlmutat a katonai műveleteken, és szoros kapcsolatot igényel a civil szektorral. A kiberparancsnokok gyakran kapcsolatot tartanak a polgári kormányzati szervekkel, például a belügyi tárcákkal, hírszerző ügynökségekkel vagy a kritikus infrastruktúrák üzemeltetőivel. Ez a kapcsolat biztosítja, hogy a civil döntéshozók időben értesüljenek a kiberfenyegetésekről, az információáramlás és a figyelmeztetések kulcsfontosságúak a hatékony védelemhez. Válsághelyzetekben, például kibertámadások során, a kiberparancsnok feladata a katonai és civil reagálás összehangolása. A civil szervek gyakran nem rendelkeznek a támadások elleni speciális tapasztalattal vagy erőforrásokkal, így a katonai kibererők támogatása elengedhetetlen. A parancsnok biztosítja, hogy a válsághelyzetben minden érintett fél egy koordinált stratégiát kövessen. Ezzel csökkenthető a károk mértéke és gyorsítható a helyreállítás, emellett stratégiai tanácsadóként is működik a kormányzat számára. Elemzi a fenyegetéseket, és javaslatokat ad a szükséges védelmi intézkedésekre, így a civil döntéshozók tudatosan és reálisan mérhetik fel a kiberkockázatokat. A katonai kiberparancsnokok szerepe azonban nem csupán reagáló, hanem megelőző jellegű is. Részt vállalnak a civil szakemberek képzésében és tudatosságuk növelésében, ezzel elősegítve, hogy a polgári szervezetek jobban felkészüljenek a potenciális támadásokra. A parancsnokok segítik a kommunikációs csatornák kialakítását a civil és katonai szervezetek között, ez a kapcsolat lehetővé teszi az információ gyors és pontos cseréjét. A kiberparancsnok szerepe ezért alapvető a bizalom és az együttműködés erősítésében is, részt vesz a kiberbiztonsági stratégia kidolgozásában és frissítésében. A katonai és civil szféra közötti koordináció különösen fontos a kritikus infrastruktúrák védelmében. Az áram-, víz- vagy pénzügyi rendszerek elleni kibertámadások gyors és hatékony reagálást igényelnek, ezen infrastruktúrák rendelkezésre állása számos esetben szintén elengedhetetlen a katonai műveletek sikeres végrehajtásához, ennek érdekében a parancsnok biztosítja, hogy a katonai erők támogassák a civil védelmet. A kibertér műveleti erők feladata, hogy a katonai és civil műveletek összhangban legyenek, és az erőforrások hatékonyan legyenek felhasználva. A fenti szempontokat figyelembe véve a katonai kiberparancsnokok tevékenysége így egyszerre stratégiai, taktikai és koordinációs jellegű feladat.

[13] Balogh 2025.
[14] The Joint Cyberspace Command Participates In The Cyberco 2024.
[15] 2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről.

A fenti elemzésből láthatjuk, hogy a kibertér civil–katonai kapcsolatai komplexek, dinamikusak és folyamatosan változnak. A civil szereplők technológiai tudása és gyors reagálása, valamint a katonai szervezetek stratégiai irányítása és koordinációs képessége együtt teremthet hatékony védelmet és gyors reagálást a kibertámadásokkal szemben. A CIMIC ebben a kontextusban egy példa a koordinációra mint meglévő képesség, de nem az egyetlen lehetséges forma, azonban érdemes megvizsgálni az abban rejlő lehetőségeket. A sikeres együttműködés kulcsa az interoperabilitás, a bizalom, az információáramlás gyorsasága és a szereplők folyamatos adaptációs képessége.

Nemzetközi keretek és gyakorlatok

A kibertér globális jellege miatt a civil–katonai kapcsolatok nem csupán nemzeti szinten értelmezhetők. A kibertámadások hatásai gyorsan átléphetik az államhatárokat, és a felelősség, a reagálás és a védelem gyakran nemzetközi együttműködést igényel.[16] Ebből következően a civil és katonai szereplők közötti koordináció nemcsak belső struktúrákon alapul, hanem a nemzetközi jogi, szabályozási és stratégiai keretek figyelembevételével is. A kibertérben történő műveletek jogi szabályozása komplex feladat, mert egyszerre kell figyelembe venni a nemzetközi humanitárius jogot, az államok szuverenitását, valamint a polgári és katonai szereplők tevékenységét. A nemzetközi egyezmények, például az ENSZ Alapokmányának[17] vonatkozó rendelkezései, az EU kibervédelmi irányelvei (NIS/NIS2,[18] Cybersecurity Act, GDPR[19]) vagy a NATO kiberbiztonsági protokolljai[20] meghatározzák a katonai műveletek kereteit, és alapot biztosítanak a civil–katonai együttműködéshez. A jogi keretek szerepe kettős, egyrészt biztosítják a tevékenységek törvényességét, másrészt elősegítik a felelősség és hatáskör egyértelmű meghatározását. Például egy kritikus infrastruktúrát ért kibertámadás során világosan definiálni kell, hogy mely állami szervek, katonai egységek vagy civil cégek jogosultak beavatkozni, és milyen eljárásrend szerint történik az incidens kezelése.

Számos nemzetközi példa mutatja, hogy a civil és katonai szereplők hatékony együttműködése a kibertérben lehetséges, ha jól definiált koordinációs mechanizmusok léteznek. A NATO kiberbiztonsági kezdeményezései, például a Cooperative Cyber Defence Centre of Excellence (CCDCOE), lehetővé teszik, hogy a tagállamok katonai és civil szervei közös szimulációkban és gyakorlatokban vegyenek részt, így javítva a koordinációt és a gyors reagálást. Az EU szintén folyamatosan fejleszti a civil–katonai koordinációt, különösen a kritikus infrastruktúrák és kiberincidensek kezelésében. A közös adatbázisok, fenyegetésfigyelő rendszerek és valós idejű információmegosztási platformok lehetővé teszik, hogy a civil és katonai szereplők gyorsan reagáljanak a fenyegetésekre, és minimalizálják a károkat. Nem minden együttműködési modell centralizált, sok esetben hálózatszerű, decentralizált megoldások bizonyultak hatékonynak.

[16] Bencsik–Karpiuk 2021.
[17] United Nations [é. n.].
[18] Network and Information Security Directive, NIS.
[19] General Data Protection Regulation, GDPR.
[20] NATO Standardization Office 2020.

A nemzetközi gyakorlatban több eset bizonyítja, hogy a civil–katonai koordináció elengedhetetlen a kibervédelemben. Az EU-ban történt kiberincidensek kezelésében a civil szolgáltatók és katonai elemzők közös munkacsoportokat hoztak létre, amelyek koordináltan azonosították a fenyegetést, és előkészítették a válaszlépéseket. Hasonló mechanizmusokat alkalmaz a NATO a baltikumi országokban a kritikus infrastruktúra védelmére irányuló gyakorlatok során. Ezek a példák rámutatnak arra, hogy a sikeres koordináció nem csupán a technológiai eszközökön múlik, hanem a szervezeti kultúrán, a kommunikációs csatornákon és a jogi kereteken is. A civil és katonai szereplők közötti bizalom, az információmegosztás gyorsasága és a közös szimulációkban szerzett tapasztalatok kritikus tényezők a hatékony reagálás szempontjából.

Ebben a kontextusban a CIMIC-szakterület esetében figyelembe kell venni, hogy a kiberbiztonság nem csupán technikai kérdés, hanem a civil társadalom és a katonai erők együttműködésének új terepe.[21] A NATO CIMIC Centre of Excellence (CCOE) hangsúlyozza, hogy a hibrid fenyegetések kezelése – beleértve a kiberincidenseket – csak úgy lehetséges, ha a civil és katonai elemzők, döntéshozók és végrehajtók közösen dolgoznak a reziliencia növelésén és a fenyegetések csökkentésén. A CCOE szakmai műhelyei, tanulmányai és esettanulmányai rámutatnak arra, hogy a kiber- és információs műveletek hatással vannak a CIMIC operatív célokra, és ezeket a hatásokat a CIMIC elemzési kereteibe és gyakorlatába integrálni szükséges. Nemzetközi gyakorlatban ez a felismerés különböző szinteken valósul meg. A NATO-tagállamok és -partnerszervezetek együttműködnek a kiberbiztonsági képzésben, közös gyakorlatokban és információmegosztási mechanizmusokban, amelyek célja a civil és katonai szereplők közötti interoperabilitás erősítése a kiberdimenzióban is. Az Európai Unió és a NATO közötti kibervédelmi konzultációk, amelyek a diplomáciai és katonai kiberparancsnokok között jöttek létre, szintén a civil–katonai koordináció gyorsabb és hatékonyabb működésére irányulnak a kiberfenyegetésekkel szemben. A CIMIC klasszikus feladatai – mint a humanitárius segítség koordinálása vagy a civil kritikus infrastruktúra védelmének támogatása – ma már egyre inkább kiegészülnek olyan elemekkel, amelyek a digitális infrastruktúra biztonságát, az információbiztonságot és a kiberrezilienciát is magukba foglalják. Ez a bővülő szerep azonban nem jelenti a CIMIC katonai kiberműveleti tevékenységgé válását, hanem azt a felismerést tükrözi, hogy a modern válságok és konfliktusok nem választják szét a fizikai és digitális dimenziókat, a civil lakosságot, infrastruktúrát és intézményeket érintő kiberfenyegetések kezelése alapvető része a hatékony civil–katonai együttműködésnek is.[22] A NATO megfogalmazása szerint: a CIMIC „must be recognized in every domain of operations and in all effects dimensions — physical, virtual, and cognitive", ami alátámasztja, hogy nem a katonai kiberhadviselés kiszélesítéséről van szó, hanem a civil tényezők beemeléséről a kiberbiztonsági szemléletbe. Más szóval, a NATO a gyakorlatban is érvényesíti azt az elvet, hogy a modern válságkörnyezetben a fizikai és digitális tér egymásra hatása miatt a CIMIC feladata a civil társadalom kibertérben való védelmének támogatása. A NATO Allied Command Transformation (ACT) 2025-ös elemzése szerint[23] a CIMIC

[21] Varga 2022.
[22] NATO CIMIC Centre of Excellence 2025c.
[23] NATO's Strategic Warfare Development Command 2025.

COE kulcsszerepet játszik abban, hogy a NATO erői képesek legyenek a civil tényezők integrálására a műveleti tervezésbe, különösen a komplex, hibrid fenyegetésekkel terhelt környezetben. A dokumentum rámutat, hogy a modern műveletekben a civil infrastruktúra elleni kibertámadások gyakran nagyobb hatással vannak a műveletek sikerére, mint a hagyományos katonai fenyegetések. A CIMIC feladata, hogy a civil szereplőkkel együttműködve feltárja a kritikus infrastruktúrák sérülékenységeit, és biztosítsa a katonai műveletekhez szükséges feltételeket. A NATO ACT szerint a CIMIC nem válik kiberműveleti szerepkörré, de a civil környezet digitális sérülékenységeinek kezelése nélkülözhetetlen a műveleti sikerhez. Az elemzés hangsúlyozza, hogy a civil és katonai szereplők közötti együttműködés ma már a kibertérben is elengedhetetlen, mivel a civil rendszerek elleni támadások közvetlenül befolyásolják a katonai műveletek végrehajtását. Ez a megközelítés jól illeszkedik ahhoz a felismeréshez, hogy a modern válságok nem választják szét a fizikai és digitális dimenziókat.

A nemzetközi példák közül kiemelhető a CIOR CIMEX (Civil–Military Exercise)[24] a NATO tartalékos tisztjeit tömörítő CIOR éves, többnapos civil–katonai együttműködési gyakorlata, amely 2012 óta készíti fel a résztvevőket összetett válsághelyzetek kezelésére. A gyakorlat *table top* formában zajlik, és olyan többdimenziós NATO-műveleti környezetet modellez, ahol a civil hatóságokkal, intézményekkel és infrastruktúrákkal való koordináció kulcsfontosságú. A szcenáriók között rendszeresen megjelennek kibertámadásokkal kombinált krízisek, például árvíz vagy tömeges migráció esetén fellépő digitálisinfrastruktúra-zavarok. Ezekben a helyzetekben a CIMIC feladata nem a kiberműveletek végrehajtása, hanem a civil lakosságot és szolgáltatásokat érintő hatások elemzése és a helyreállítás támogatása. A CIMEX gyakorlatai szintén alátámasztják, hogy a modern válságokban a fizikai és digitális dimenziók elválaszthatatlanok. A civil infrastruktúrát érő kiberfenyegetések kezelése ezért ma már a hatékony CIMIC-tevékenység alapvető részét kell hogy képezzék, anélkül, hogy a CIMIC kiberműveleti szerepkörré válna. Ez a nemzetközi példa pontosan alátámasztja azt a felismerést, hogy a civil–katonai együttműködésnek ma már a digitális térben jelentkező fenyegetésekre is reagálnia kell.

Magyarországhoz hasonlóan Németországban is megkezdődött a kiber- és információs műveleti képességek átstruktúrálása egy szervezetbe. Ennek részeként a Bundeswehren belül a Cyber- und Informationsraum (CIR) nevű önálló szervezetben összpontosulnak ezen képességek, amely szervezet felel a kiber- és információs műveletekért, továbbá a kapcsolódó felderítési feladatokért is. Bár jelenleg a CIMIC képesség a Joint Support Command alárendeltségében működik, a Bundeswehr műveleti tervezési és végrehajtási rendszerében a két terület szoros együttműködésben dolgozik, különösen többdimenziós *(multidomain)* műveletek esetén. A CIR biztosítja a digitális és információs környezet feletti műveleti képességeket, míg a CIMIC a civil szereplőkkel, hatóságokkal és szervezetekkel való koordinációt végzi. A német modell eljárási és műveleti szinten valósítja meg az integrációt, az elkövetkező időszakban elemzik annak hatékonyságát, és a tapasztalatok figyelembevételével tesznek további javaslatokat az esetleges további integrációra.

[24] Lásd: https://cior.net/activities/civil-military-exercise/

Az USA-ban használt gyakorlat lényege, hogy a Civil Affairs (CA) – amely a CIMIC amerikai megfelelője – és a kiberműveleti szervek együttműködése nem különálló feladat, hanem a teljes műveleti ciklusba beépített eljárásrend. Az USA kiberstratégiája[25] a civil és katonai szereplők összehangolt működését alapkövetelményként határozza meg, mivel a kibertámadások elsődleges célpontjai jellemzően civil infrastruktúrák, amelyeket a hadsereg önmagában nem tud megvédeni. A CA feladata ezért az, hogy kapcsolatot tartson a kritikus infrastruktúrák üzemeltetőivel, felmérje a kibertámadások civil hatásait, és közvetítse ezeket a katonai kiberparancsnokság felé. A NATO Cyber Coalition gyakorlatok amerikai részvétele is azt mutatja, hogy a CA és a kibererők közösen dolgoznak a helyzetértékelésen, a civil szolgáltatások helyreállításán és a lakosság tájékoztatásán. A CCDCOE kutatásai alapján az amerikai modell egyik sajátossága, hogy a kiberfenyegetések kezelésébe rendszeresen bevonja a magánszektort is, különösen a technológiai vállalatokat és az infrastruktúra-üzemeltetőket, ami a CIMIC-szemlélet digitális kiterjesztésének tekinthető. A CA és a Cyber Command közötti együttműködés így nem *ad hoc,* hanem intézményesített: közös helyzetértékelés, információmegosztás, civil hatásvizsgálat és válságkezelési koordináció formájában jelenik meg. A NATO-val közös amerikai gyakorlatok azt is megerősítik, hogy a CA-egységek kulcsszerepet játszanak a civil lakosság rezilienciájának fenntartásában kibertámadások idején, például az energia- vagy egészségügyi rendszerek sérülésekor. Összességében megállapítható, hogy az amerikai eljárásrend lényege, hogy a CA a kiberhadviselésben kapcsolati és koordinációs csomópontként működik, amely összeköti a katonai kiberképességeket a civil infrastruktúrákkal, a helyi hatóságokkal és a lakossággal. Ez a modell a NATO-ban is iránymutatónak számít, és a kiberfenyegetések növekedésével várhatóan tovább erősödik majd, a Magyar Honvédség a gyakorlatok során megkezdte ennek a modellnek a tesztelését és rendszerbe történő integrálását.

A nemzetközi példák és jogi keretek azt mutatják, hogy a civil–katonai kiberkoordináció lehetséges, de csak akkor, ha a szereplők képesek adaptálódni a gyorsan változó fenyegetésekhez, és rugalmasan kezelik az együttműködést; a hangsúly a szereplők közötti partnerségen, a gyors információáramláson, a jogi és etikai kereteken, valamint a folyamatos tanuláson van. A globális kiberfenyegetések egyre összetettebbé válnak, ezért a civil–katonai kapcsolatok nem csupán operatív, hanem stratégiai szinten is kulcsfontosságúak. A tapasztalatok azt mutatják, hogy a hatékony együttműködés alapja a világos szerepkörök, a közös gyakorlatok, a bizalom és az interoperabilitás, amelyek lehetővé teszik, hogy a civil és katonai szereplők egységes, adaptív hálózatként reagáljanak a kibertámadásokra.

Magyarországi civil–katonai kiberkoordináció

Magyarországon, mint a legtöbb NATO- és EU-nemzet esetében, a kibertér védelme és a civil–katonai együttműködés egyre nagyobb hangsúlyt kap, különösen az állami,

[25] White House 2026.

katonai és kritikusinfrastruktúra-szereplők között. A hazai Nemzeti Biztonsági Stratégia[26] és más ágazati stratégiai szintű dokumentumok kiemelten foglalkoznak a kiberbiztonsággal. A polgári és katonai szervezetek közötti kiberkoordinációs együttműködés a kiberbiztonság és kibervédelem területén több szinten és intézményrendszerben valósul meg. Magyarország jogi szabályozással támogatja a kiberbiztonsági tevékenységek koordinációját, 2024-ben hatályba lépett a magyar kiberbiztonságról szóló törvény[27] és annak végrehajtási rendelete, amely előírja a nemzeti kiberbiztonsági munkacsoport létrehozását. Ennek a testületnek feladata a kiberbiztonsági politika koordinálása, amelyben mind az állami, mind a magánszektor, továbbá a polgári és katonai szervezetek képviselői részt vesznek. A szabályozás nemzeti kapcsolattartó pontot is kijelöl, amely a határon átnyúló kibervédelem és incidenskezelés során az információcserét koordinálja. Ezek a dokumentumok jogi alapot és stratégiai irányt adnak arra, hogyan kell integrálni a polgári és katonai kapacitásokat a kibervédelemben.

Magyarországon a polgári kiberbiztonsági koordináció központi szereplője a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NKI vagy National Cyber Security Center Hungary) mint kormányzati szervezet kiberbiztonsági támogatást nyújt a hazai közigazgatás és önkormányzati informatikai rendszerek védelméhez, illetve a civil szereplők biztonsági tudatosságának növeléséhez. Fontos elemként jelenik meg a Nemzeti Koordinációs Központ (NCC-HU), amely az EU kiberbiztonsági kompetenciahálózatának hazai csomópontja, feladatai közé tartozik a hazai civil szereplők – ipar, kutatás, oktatás, közszféra – tevékenységének összehangolása, projektfinanszírozás támogatása, tudásépítés és nemzetközi együttműködés elősegítése.

Honvédelmi ágazati szinten a Honvédelmi Minisztérium, a Katonai Nemzetbiztonsági Szolgálat és a Magyar Honvédség különböző szervezeti egységei hajtanak végre szakterületük vonatkozásában kiberterületi koordinációt, amely a honvédelmi és nemzetközi kötelezettségeket szolgálja, valamint az igazságügyi, rendészeti és terrorelhárítási szervek, amelyek polgári és katonai információcserét is végeznek.

A civil szektor részéről a kritikus infrastruktúrák üzemeltetői, informatikai cégek és kutatóintézetek nyújtanak technikai szakértelmet és valós idejű információkat. A civil és katonai szereplők közötti együttműködés folyamatosan fejlődik, különösen a közös képzések, szimulációk és gyakorlatok révén. Magyarországon az oktatási intézmények fontos szerepet játszanak abban, hogy a civil és katonai szereplők a kiberbiztonság területén hatékonyan tudjanak együttműködni. A Nemzeti Közszolgálati Egyetem különleges helyzetben van, mivel egy intézményen belül készíti fel a honvédelmi, rendészeti, közigazgatási és nemzetbiztonsági területen dolgozó szakembereket, így a hallgatók már a képzés során megismerik egymás gondolkodásmódját, feladatait és működési kereteit. Ezt a megközelítést egészítik ki a műszaki és informatikai profilú egyetemek, például a Budapesti Műszaki és Gazdaságtudományi Egyetem és az Óbudai Egyetem, amelyek a kiberbiztonság technikai hátterét adják, valamint kutatási és fejlesztési munkájukkal közvetlenül is támogatják az állami és honvédelmi szervezeteket. A jogi és társadalomtudományi képzések szintén hozzájárulnak ahhoz, hogy a kibertérben zajló együttműködés jogszerű és felelős módon valósuljon meg.

[26] Kovács 2020.
[27] 2024. évi LXIX. törvény Magyarország kiberbiztonságáról.

Az egyetemek emellett olyan szakmai találkozási pontokat is biztosítanak – konferenciák, képzések és közös gyakorlatok formájában –, ahol a civil és katonai szakemberek személyes kapcsolatokat építhetnek ki. Ezek a kapcsolatok a gyakorlatban megkönnyítik az információcserét és a közös fellépést, ami válsághelyzetben gyorsabb reagálást és kiszámíthatóbb együttműködést tesz lehetővé, ezáltal erősítve az ország ellenálló képességét a kibertérben. Tendenciaként megfigyelhető, hogy a honvédelmi ágazat gyakorlataiba, egyre inkább már a tervezés fázisában, is bevonják az egyetemi hallgatókat.

Magyarországon a civil–katonai szerepek adaptációja szoros összefüggésben áll a kibertér gyors változásaival. A katonai szervezeteknek rugalmasabbá kell válniuk, és alkalmazkodniuk kell a civil szektor gyors reagálásához és technológiai innovációihoz. Ugyanakkor a civil szereplők számára is létfontosságú, hogy megértsék a katonai és állami struktúrák működését, hogy a közös munkában ne alakuljon ki félreértés vagy késlekedés. A hazai civil–katonai kiberkoordináció és az összkormányzati gyakorlatok azt mutatják, hogy a kibertérben az együttműködés lehetőségei széles spektrumon mozognak. A siker kulcsa a gyakorlatias képzés, az interoperabilitás, az adaptáció és a bizalom, a valódi érték a szereplők közötti partnerségből és a folyamatos tanulásból származik, a feladatrendszer folyamatosan fejleszthető és kiegészíthető.

A tartalékos rendszer a kiber szakterület számára kifejezetten sok lehetőséget kínál a jövőben, mivel a kibervédelemben szükséges tudás és tapasztalat jelentős része a civil szférában halmozódik fel, különösen az informatikai és távközlési területeken. A rendszer egyik legnagyobb előnye, hogy lehetővé teszi magasan képzett szakemberek bevonását anélkül, hogy hosszú távon el kellene őket vonni a civil munkahelyüktől, így az állam és a honvédség hozzáférhet a legfrissebb technológiai ismeretekhez és piaci tapasztalatokhoz. A kibetartalékosok révén gyorsan bővíthetők az erőforrások válsághelyzetben vagy megnövekedett fenyegetettség idején, miközben békeidőben a rendszer fenntartása kisebb költséggel jár, mint egy teljesen hivatásos állományé. Emellett a tartalékos szolgálat hidat képez a civil és katonai szféra között, mivel az érintett szakemberek mindkét környezet működését ismerik, és képesek közvetíteni az eltérő szervezeti kultúrák és eljárások között. A célzott kiképzések és gyakorlatok révén a tartalékos állomány bekapcsolható incidenskezelési, elemzési vagy tanácsadói feladatokba, ami növeli a rendszer rugalmasságát és alkalmazkodóképességét. Összességében kijelenthető, hogy a kiberszakterülethez illesztett tartalékos rendszer hozzájárulhat a nemzeti kiberreziliencia erősítéséhez, mivel egyszerre növeli a szakmai kapacitást, csökkenti a kiszolgáltatottságot, és javítja a civil–katonai együttműködés gyakorlati működését.

Jogi kérdések és javaslatok a civil–katonai kiberkoordináció feladataira

A kibertér sajátosságai és a civil–katonai kapcsolatok vizsgálata rávilágítanak arra, hogy a hagyományos állami és katonai struktúrák önmagukban nem képesek teljes mértékben kezelni a kibervédelmi fenyegetéseket.[28] A civil szereplők – a kritikus

[28] Ertan et al. 2020.

infrastruktúrát üzemeltető vállalatok, technológiai cégek[29] vagy kutatóintézetek – gyors reagálásukkal és szakértelmükkel jelentősen hozzájárulnak a kibervédelmi képességekhez. A korábbi pontokban bemutatott nemzetközi és hazai példák alapján világossá vált, hogy a civil–katonai koordináció nem pusztán technikai feladat, hanem szervezeti, stratégiai és jogi dimenziókat is magában foglal, amelyek összehangolt működés nélkül nem biztosítják a hatékony reagálást.

A vizsgálat során két fő jellegzetesség rajzolódott ki. Egyrészt a civil és katonai szereplők közötti interakció egyre inkább többszereplős, hálózatszerű rendszerré alakult, amely lehetővé teszi a gyors reagálást, ugyanakkor folyamatos koordinációt és tapasztalatcserét igényel. Az ilyen hálózatok előnye, hogy minden résztvevő azonnal hozzá tud járulni a fenyegetésfelderítéshez, és gyorsan be tudja vinni a saját szakterületi ismereteit a döntéshozatali folyamatokba. Másrészt a civil–katonai koordinációban a formalizált mechanizmusok, például az incidenskezelési protokollok és a jogi keretek biztosítják, hogy a felelősségi viszonyok világosak maradjanak, és a döntések jogszerűen történjenek.[30] A legjobb eredmény akkor születik, ha a decentralizált hálózatok rugalmassága és a formalizált koordinációs mechanizmusok egyaránt érvényesülnek.

Ugyanakkor a koordináció során több kihívással is szembesülünk. A bizalom és az adatmegosztás kérdése gyakran kritikus tényező, hiszen a civil szereplők érzékeny adatokat kezelnek, és nem minden esetben hajlandók azokat azonnal megosztani katonai vagy állami szereplőkkel. További nehézséget jelent a technológiai és képességbeli eltérés, ami miatt a civil és katonai szereplők nem mindig azonos szinten reagálnak az incidensekre, és a koordináció során késlekedések vagy félreértések léphetnek fel. A jogi keretek kulcsfontosságúak a civil–katonai együttműködésben, mivel meghatározzák, hogy milyen tevékenységek jogszerűek, milyen szereplők milyen mértékben avatkozhatnak be, és hogyan kezelhetők a polgári jogi szempontok. Ahogyan a korábbi fejezetekben már vizsgáltuk, nemzetközi jogi keretek között az ENSZ Alapokmánya és az államok közötti kiberműveletekre vonatkozó normák biztosítják az általános kereteket, míg a NATO és az EU kiberbiztonsági protokolljai és irányelvei konkrét útmutatást adnak a civil és katonai szereplők közötti információmegosztásra és incidenskezelésre. Magyarországon a hazai jogszabályok és az adatvédelmi szabályok biztosítják, hogy a civil–katonai koordináció jogszerű keretek között működjön, és a polgári érdekek ne sérüljenek. A jogi keretek nem csupán formális követelmények, hanem a civil–katonai együttműködés alapját is adják. Világossá teszik, hogy ki, mikor és milyen feltételekkel avatkozhat be egy incidens során, és biztosítják a felelősségi körök tisztaságát. A jogi megfelelés hozzájárul a bizalom kialakulásához, elősegíti az információmegosztást, és csökkenti az esetleges félreértésekből vagy visszaélésekből eredő kockázatokat.

[29] Bonnyai–Kiss–Tóth 2023.
[30] Szádeczky 2018.

Javaslatok és ajánlások a hatékonyabb civil–katonai kibertéri koordinációhoz

A vizsgálat és a gyakorlati tapasztalatok egyértelműen rámutatnak arra, hogy a civil–katonai kiberkoordináció fejlesztése nem egyetlen intézkedéssel, hanem egymásra épülő szervezeti, technológiai és humán lépések sorozatával érhető el.[31] Alább olyan javaslatok olvashatók, amelyek nemcsak elvi következtetéseket vonnak le, hanem konkrét, rövid távon is megvalósítható ajánlásokat fogalmaznak meg a hatékony rendszer kialakítása érdekében.

Interoperabilitás és technológiai kompatibilitás

A vizsgálat alapján megállapítható, hogy az eltérő technikai megoldások és információkezelési eljárások akadályozzák a gyors és pontos helyzetértékelést, ami válsághelyzetben közvetlenül rontja a reagálás hatékonyságát. Amennyiben a civil és katonai szereplők nem azonos vagy kompatibilis rendszereket használnak, az információáramlás megszakadhat vagy torzulhat.

Javaslat: indokolt egy közös technikai minimumkövetelmény-rendszer kialakítása, valamint olyan szabványosított adatmegosztási és kommunikációs felületek bevezetése, amelyek biztosítják a rendszerek közötti folyamatos interoperabilitást, ezeket nem elég kiépíteni, folyamatos karbantartást igényelnek.

Közös képzések és szimulációk

A tapasztalatok azt mutatják, hogy a koordináció hiányosságai leginkább éles helyzetben válnak láthatóvá, amikor már nincs lehetőség a szerepek és eljárások tisztázására. A rendszeres közös gyakorlatok hiánya növeli a bizonytalanságot és a döntési késedelmet.[32]

Javaslat: szükséges intézményesíteni az évente ismétlődő, civil–katonai részvétellel zajló kiberbiztonsági szimulációkat, amelyek során a résztvevők gyakorolhatják a közös döntéshozatalt, az információmegosztást és a jogi keretek gyakorlati alkalmazását. A katonai ágazat gyakorlataiba minél szélesebb körben kell bevonni a civil szereplőket.

Rugalmasság és adaptáció

A központosított irányítás önmagában nem képes kezelni a kibertér gyorsan változó és gyakran lokális jellegű fenyegetéseit. A túlzott centralizáció lassíthatja a reagálást, míg a teljes decentralizáció stratégiai széttagoltsághoz vezethet.

[31] Boeke–Heinl–Veendaal 2018.
[32] Krasznay–Hámornik 2019.

Javaslat: olyan hibrid koordinációs modellt szükséges kialakítani, amely stratégiai szinten központi irányítást biztosít, ugyanakkor operatív szinten felhatalmazza a helyi szereplőket az önálló, gyors döntéshozatalra, meghatározott keretek között. A kiberparancsnok és az MH kibertér műveleti erőinek feladat-végrehajtását integrálni kell ebbe a feladatrendszerbe, a civil szereplőknek ismerniük kell lehetőségeiket és feladatukat.

Bizalom és kommunikáció erősítése

Az elemzés rámutat arra, hogy a bizalom hiánya információ-visszatartáshoz és párhuzamos intézkedésekhez vezethet, ami jelentősen csökkenti az együttműködés hatékonyságát. A bizalom kialakulása azonban nem spontán folyamat, hanem tudatos szervezeti erőfeszítést igényel.

Javaslat: célszerű állandó kapcsolattartási pontokat és gyors kommunikációs csatornákat létrehozni a civil és katonai szervezetek között, valamint rendszeres, nem válsághelyzethez kötött szakmai egyeztetéseket tartani a kölcsönös megértés erősítése érdekében.

Jogi megfelelés és etikai szempontok integrálása[33]

A jogi és etikai keretek figyelmen kívül hagyása rövid távon gyorsabb reagálást eredményezhet, hosszú távon azonban aláássa az együttműködés legitimitását és a társadalmi bizalmat. A jogi bizonytalanság különösen válsághelyzetben bénító hatású lehet.

Javaslat: indokolt közös jogi és etikai iránymutatások kidolgozása, valamint célzott képzések szervezése annak érdekében, hogy a résztvevők pontosan tisztában legyenek jogosultságaikkal és kötelezettségeikkel a kiberkoordináció során. A gyakorlatok ezen a területen is lehetőséget biztosítanak a folyamatok szimulációjára, amennyiben nem egyértelműek a döntési pontok, akkor ezek finomhangolása még a konfliktusokat megelőzően lehetséges.

Szervezeti és stratégiai ajánlások

A nem egyértelmű felelősségi viszonyok és a hiányos incidenskezelési protokollok késleltetik a reagálást és növelik a szervezeti súrlódásokat. Ezzel szemben a tanuló szervezeti megközelítés hosszú távon növeli a rendszer ellenálló képességét.

Javaslat: szükséges a civil–katonai együttműködésben érintett szervezetek feladat- és hatáskörének egyértelmű rögzítése, valamint egy közös incidensértékelési és tapasztalatfeldolgozási mechanizmus bevezetése, amely biztosítja a folyamatos fejlődést. Célszerű a CIMIC-szakterület korábban kialakult feladatai kiterjesztésének vizsgálata a *kiberdomain* irányába,[34] a tapasztalatok átadása más civil szereplők részére is.

[33] Schmitt 2017.
[34] NATO CIMIC Centre of Excellence 2025a.

A kibertartalékos-rendszer kialakítása egyszerre képes növelni a nemzeti reziliencia szintjét, valamint racionalizálhatja a felhasznált erőforrásokat.

Összegzés

A tanulmányban a megfogalmazott célokkal összhangban azonosítottam a kibertér alapfogalmait és sajátosságait, végigkövettem a civil–katonai kapcsolatok alakulását annak érdekében, hogy kellő megalapozottsággal tudjak javaslatokat megfogalmazni a jövőbeni civil–katonai kibertérkapcsolatok koordinációjához. Vizsgálat alá vontam, hogy a CIMIC az információs műveletek részeként miként tud hatékonyan alkalmazkodni a kibertér követelményeihez a szakmai megújulás érdekében, hogyan tudja a jelenlegi és jövőbeni feladatrendszert racionalizálni és aktualizálni.

Összességében a civil–katonai kapcsolatok a kibertérben komplex, sokszereplős, adaptív hálózatként működnek. A CIMIC példája jól szemlélteti, hogyan lehet a koordinációt formálisan is támogatni, de az együttműködés teljes képe ennél jóval komplexebb, a siker kulcsa a folyamatos tanulás, a rugalmas szervezeti struktúra, a partnerség, a bizalom és a jogi megfelelés. Az evolúciós és tanulási folyamatok eredményeként folyamatosan új szerepkörök jelennek meg mind civil, mind katonai területen, ennek egyik látványos példája a kiberparancsnokok hálózata. Figyelemmel kísérve feladatrendszerük átalakulását, egyértelműen kijelenthető, hogy a katonai hálózatok felügyelete és irányítása mellett egyre hangsúlyosabb szerepet kap portfóliójukban a civil képességek időszakos irányítása a katonai művelet végrehajtásának érdekében. Ez merőben új szemléletet követel a katonai kibertérműveleti erők és a civil vállalati vezetők részéről is, meg kell találni az egészséges egyensúlyt és a közös nyelvet a feladat-végrehajtás során. A civil és katonai szereplőknek képesnek kell lenniük arra, hogy egységesen reagáljanak a kibervédelmi fenyegetésekre, miközben megőrzik autonómiájukat és alkalmazkodnak a gyorsan változó technológiai és társadalmi környezethez. Azok az országok, amelyek sikeresen integrálják a jogi kereteket, a képzéseket, a szimulációkat és a folyamatos tapasztalatcserét, hosszú távon fenntartható és hatékony civil–katonai kiberkoordinációt biztosíthatnak.

Jelenleg már több országban létezik kibertartalékos-rendszer, ahol IT- és kiberbiztonsági szakembereket vonnak be a nemzeti kiberbiztonság támogatására különösen háborús válság vagy komplex, több szektort érintő kibertámadás esetén. A rendszerek formája országonként eltérő, vannak formális tartalékos programok, önkéntes gyakorlatok, valamint különleges katonai vagy kormányzati egységek, amelyek tartalékos szakértelmet integrálnak. Ezen a területen jó példák léteznek, azonban uniformizált megoldások nem, minden nemzetnek a céljaihoz kapcsolódóan kell kialakítania az ideális koncepciót. Az ilyen jellegű kezdeményezések stratégiai elrettentő hatással is rendelkeznek, mert ebben az esetben az állam nyíltan jelzi, hogy nemcsak egy szűk, állandó kibererőre támaszkodik, hanem szükség esetén több száz vagy ezer, valós piaci tapasztalattal rendelkező szakembert (akár komplett, összeszokott céges csapatokat) tud mozgósítani; ebben az esetben a támadó fél számára megnő a bizonytalanság és a kockázat. Nem tudja előre, mekkora védelmi kapacitással, milyen gyors reagálással és milyen szakértelemmel fog szembesülni. A kibertartalékos-rendszer kialakítása

során a hatékonyság fokozása érdekében célszerű vizsgálni az információs műveletek teljes spektrumát, így adva új, korábban nem alkalmazott megoldási javaslatokat a szakterületi szakemberhiányból adódó problémákra.

A Magyar Honvédség a döntési folyamatok gyorsabbá és hatékonyabbá tételének érdekében a publikációban szereplő egységes alapelvek használatát már 2022. január 1-jén megkezdte a Kiber- és Információs Műveleti Központ megalakításával, amelynek feladatrendszere magába foglalja többek között a Magyar Honvédség kiberműveleti (CYBER OPS), civil–katonai együttműködési (CIMIC), lélektani műveleti (PSYOPS) és információskörnyezet-elemző (IEA) képességeinek biztosítását is. A publikációban szereplő javaslatok felhasználása lehetőséget biztosít a továbblépésre, azok tesztelését követően célszerű megkezdeni fokozatosan az integrációs folyamatot.

Felhasznált irodalom

2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről. Online: https://net.jogtar.hu/jogszabaly?docid=a2100140.tv

2024. évi LXIX. törvény Magyarország kiberbiztonságáról. Online: https://net.jogtar.hu/jogszabaly?docid=a2400069.tv

Balogh Péter (2025): Kibertérbeli műveletek 2016-ot követően – A kiberhadviselés mintázatai, trendjei, szereplői és kapcsolódásaik. *Hadtudomány,* 35(E-szám). Online: https://doi.org/10.17047/Hadtud.2025.35.E.1

Bencsik, András – Karpiuk, Mirosław (2023): The Legal Status of the Cyberarmy in Hungary and Poland. *Central European Journal of Social Sciences and Humanities,* 11(2), 19–31. Online: https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi-10_35467_cal_174696

Boeke, Sergei – Heinl, Caitríona – Veenendaal, Matthijs A. (2018): Civil-Military Relations & International Military Cooperation in Cyber Security: Common Challenges & State Practices Across Asia and Europe. In Maybaum, M. – Osula, A.-M. – Lindström, L. (szerk.): *2015 7th International Conference on Cyber Conflict.* Tallinn: CCD COE. Online: https://doi.org/10.1109/CYCON.2015.7158469

Bonnyai Tünde – Kiss Adrienn – Tóth András szerk. (2023): *Nagyvállalati biztonságtudatosság és nyílt forrású információszerzés. Kiber- és információbiztonsági tanulmányok.* Budapest: Ludovika. Online: https://doi.org/10.36250/01170_00

Clarke, Richard A. – Knake, Robert K. (2019): *The Fifth Domain.* New York: Penguin.

Deibert, Ronald J. (2003): Black Code: Censorship, Surveillance and the Militarization of Cyberspace. *Journal of International Studies,* 15(2), 33–56. Online: https://thesociologycenter.com/supscibiblog/BlackCode.pdf

Ertan, Amy et al. szerk. (2020): *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* Tallinn: CCD COE. Online: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

Haig Zsolt (2023): A kibertéri műveletek fejlődése: a számítógép-hálózati műveletektől a kibertéri befolyásolásig. In Krasznay Csaba (szerk.): *Taktikák és stratégiák a kiberhadviselésben.* Budapest: Ludovika, 41–60. Online: https://tudasportal.

uni-nke.hu/xmlui/handle/20.500.12944/102124?key=Kiberv%C3%A9delem%20%C3%A9s%20nemzetbiztons%C3%A1g%20kiss
Hunorfi, Péter – Farkas, Tibor (2025): Cybersecurity of Operational Technology in Critical Infrastructures. *Belügyi Szemle,* 73(1Ksz.), 183–197. Online: https://doi.org/10.38146/bsz-ajia.2025.v73.i1SI.pp183-197
Kovács László (2020): A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148(5), 12–34. Online: https://doi.org/10.35926/HSZ.2020.5.1
Krasznay, Csaba (2024): Hacktivists, Proxy Groups, Cyber Volunteers. *Academic and Applied Research in Military and Public Management Science,* 23(3), 107–124. Online: https://doi.org/10.32565/aarms.2024.3.6
Krasznay, Csaba – Hámornik, Balázs Péter (2019): Human Factors Approach to Cybersecurity Teamwork – The Military Perspective. *Advances in Military Technology,* 14(2), 291–305. Online: https://doi.org/10.3849/aimt.01296
Kott, Alexander et al. (2018): Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153. *ArXiv.* Online: https://doi.org/10.48550/arXiv.1804.07651
NATO CIMIC Centre of Excellence (2025a): *CIMIC in the Cyberspace Domain: Fact Sheet*. Online: www.cimic-coe.org/wp-content/uploads/2025/03/20250303-uc-ccoe-factsheet-cyberspace-final.pdf
NATO CIMIC Centre of Excellence (2025b): *CIMIC Case Studies*. Online: www.cimic-coe.org/wp-content/uploads/2025/05/acaCIMICs_Case-Studies.pdf
NATO CIMIC Centre of Excellence (2025c): *CIMIC Handbook 2.1 NATO CIMIC*. Online: www.cimic-coe.org/handbook-entries/welcome-to-the-cimic-handbook/ii-fundamentals/2-1-nato-cimic/
NATO Standardization Office (2020): *Allied Joint Publication-3.20. Allied Joint Doctrine for Cyberspace Operations.* Online: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf
NATO Standardization Office (2025): *Standard AJP-3.19. Allied Joint Doctrine For Civil-Military Cooperation ED B V1.* Online: https://assets.publishing.service.gov.uk/media/685a8bdce9509f1a908eb108/AJP_3_19_EdB_CIMIC.pdf
NATO's Strategic Warfare Development Command (2025): *Strengthening Civil-Military Cooperation: The Role of NATO's Civil-Military Cooperation Centre of Excellence.* Online: www.act.nato.int/article/cimic-coe-2025/
Resperger István – Kiss Álmos Péter – Somkuti Bálint (2014): *Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással.* Budapest: Zrínyi.
Schmitt, Michael N. szerk. (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. Online: https://doi.org/10.1017/9781316822524
Szádeczky, Tamás (2018): Cybersecurity Authorities and Related Policies in the EU and Hungary. *Central Eastern European eDem & eGov Days,* 331, 287–299. Online: https://doi.org/10.24989/ocg.v331.24
United Nations [é. n.]: *United Nations Charter.* Online: https://www.un.org/en/about-us/un-charter/full-text

VARGA Zsófi (2022): Civil-katonai együttműködés alkalmazása komplex hadműveleti környezetben. *Biztonságtudományi Szemle,* 4(1), 63–73. Online: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/207/179

White House (2026): *President Trump's Cyber Strategy for America.* Online: www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf