Bányász Péter – Krasznay Csaba – Tóth András

A kibervédelem szakpolitikai szintjének helyzete és kihívásai Magyarországon, az EU-ban és a NATO-ban

Military and Intelligence CyberSecurity Research Paper
2022/8.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROGRAM


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

2022 végén úgy véljük, magabiztosan kijelenthető, a kiberbiztonság életünk minden szegmensében létfontosságú.[1] A bennünket körülvevő infokommunikációs eszközök nem csupán a társadalmi együttélés, hanem a társadalom működését biztosító infrastruktúrák megkerülhetetlen részévé váltak. A technológiai fejlődés, a mindent behálózó internetes eszközök azonban roppant törékeny ökoszisztémát alakítottak ki, amelynek akár egy kis mértékű sérülése is komplett rendszereket tehet tönkre.

A 2007-ben Észtország kormányzati és gazdasági létfontosságú rendszerelemeit ért, hetekig tartó kibertámadás felkészületlenül érte a megtámadott országot, illetve szövetségeseit. Észtországot NATO tagállamként érte ez a támadás, azonban senki nem tudott választ adni, hogy milyen lépéseket adhatna a NATO, mint katonai védelmi szövetség. A bizonytalansággal a NATO nem volt egyedül, számos ország próbálta értelmezni azt az új stratégiai helyzetet, ami az észt rendszereket érte a kibertérből. Mindez elindított egy rendkívül intenzív stratégiai gondolkodást, ami nem csupán a kibervédelmi ellenállóképességre, de a reagálóképesség kialakítására is vonatkozott.

2007 óta sok bit lefolyt az optikai kábelekben, számos olyan paradigmaváltó esemény következett be (például a 2016-os amerikai elnökválasztásba történő beavatkozás, az új típusú koronavírus járvány kiberbiztonsági aspektusai, a 2022. februárja óta zajló ukrán-orosz háború), amelyek a megalkotott stratégiák újragondolását követelték meg.

A tanulmány ezt a stratégiai fejlődést kívánja feldolgozni a címben szereplő három entitás aspektusából. Mivel a kiberbiztonság egy rendkívül komplex szakterület, így a kiadvány terjedelmi korlátai nem teszik lehetővé, hogy az egyes stratégiai dokumentumokat a szerzők részletesen vizsgálják. Remélhetőleg e közlemény eligazodást nyújt a stratégiai dokumentumok sűrűjében.

A KIBERVÉDELEM SZAKPOLITIKAI SZINTJÉNEK HELYZETE ÉS KIHÍVÁSAI MAGYARORSZÁGON

Magyarországon az elektronikus információbiztonság szabályozása hosszú múltra tekint vissza. Az első vonatkozó rendelkezés 1981-ben jelent meg, amikor az 1/1981. (I.27.) BM rendelet a számítástechnikai rendszerek titok-, vagyon-, és tűzvédelméről hozta be a közgondolkodásba az elektronikus információs rendszerek védelmét. Ezt követte 1987-ben a 3/1988. (XI.22.) KSH rendelkezés az államtitok és szolgálati titok számítástechnikai védelméről. ezek a jogszabályok is mutatják, hogy a magyar szabályozás már a rendszerváltás előtt is

[1] A mű a Katonai Nemzetbiztonsági Szolgálat TKP2021-NVA-24 azonosító számú „A mesterséges intelligencia alkalmazásának kutatása a katonai nemzetbiztonsági célú adatszerző, adatfeldolgozó és vizualizációs eljárásokban, és kapcsolódó fejlesztések elvégzése” elnevezésű projektje keretében, az Innovációs és Technológiai Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával valósult meg.

komolyan vette a frissen megjelenő informatikai rendszerek információbiztonságú szempontú védelmét, melyet a rendszerváltást követően, az informatika széleskörű közszolgálati elterjedésével párhuzamosan számos más szabályozás is követett.

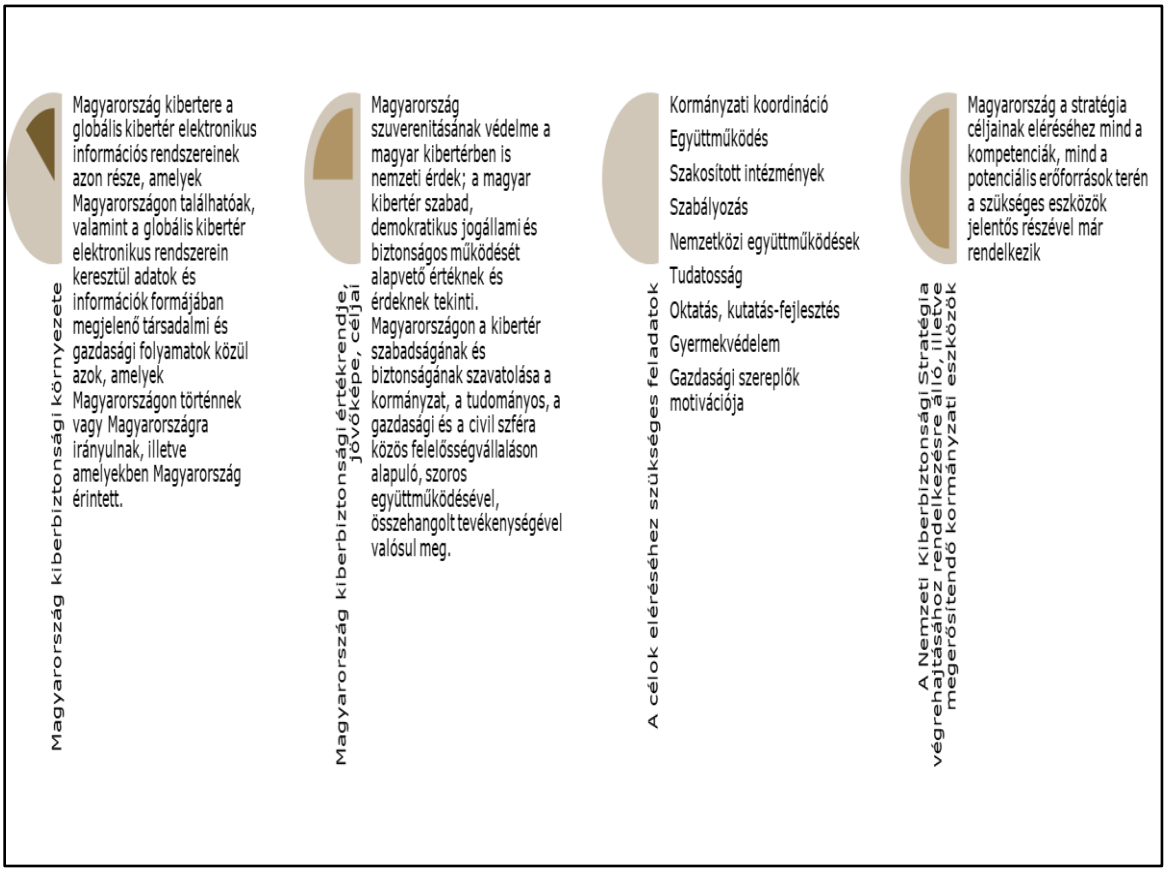
1994-ben a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága jelentette meg az Informatikai Biztonsági Módszertani Kézikönyvet, melyet MEH ITB 8-as számú ajánlásként ismerünk. Ezt követte 1996-ban, szintén a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottságának kiadásában az Informatikai Rendszerek Biztonsági Követelményei, azaz a MEH ITB 12-es számú ajánlás, mely sorozatot 1997-ben a Common Criteria szabvány magyar fordítása, az Informatikai termékek és rendszerek biztonsági értékelésének módszertana, azaz az ITB 16-os számú ajánlás zárt le. Az 1990-es években tehát megteremtődött annak a lehetősége, hogy a magyar közszolgálat az akkor legfrissebb szabványokból, a ma ISO 27000-ként és ISO 15408-ként ismert szabványokból tudjon magyar nyelven dolgozni.

Az 1990-es évek ajánlásai hosszú ideig érvényben voltak, egészen a 2000-es évek második feléig, 2008-ig nem jelent meg olyan új kiadvány, amely lehetővé tette volna azt, hogy a magyar közszolgálat elektronikus információbiztonsága lépést tudjon tartani a rohamosan változó technológia jelentette új típusú fenyegetésekkel. 2008-ban a Miniszterelnöki Hivatal Közigazgatási Informatikai Bizottsága adta ki a Magyar Informatikai Biztonsági Ajánlások (MIBA), azaz a KIB 25. számú ajánlásnak új köteteit, melyben egyrészt az ISO 27000 szabványhoz hasonló, másrészt pedig az ISO 15408 (Common Criteria) szabványt feldolgozó ajánlások jöttek létre Magyar Informatikai Biztonsági Keretrendszer (MIBIK), illetve Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) néven. Ezt egészítette ki az az ajánlás, mely a kis szervezetek számára nyújtott útmutatót az információbiztonság megvalósítása érdekében (Informatikai Biztonsági Iránymutató Kis Szervezetek Számára – IBIX). A 2000-es években jött létre az az intézményrendszer, mely lehetővé tette a magyar közszolgálat komplex védelmét a kibertérből érkező fenyegetésekkel szemben. Ekkor a Puskás Tivadar Közalapítvány (PTA) keretében működő CERT-Hungary Központ lett a magyar kormány hálózatbiztonsági központja. A közigazgatási hálózatbiztonsági központ felállítása céljából a PTA az Informatikai és Hírközlési Minisztérium támogatásával 2004-ben kezdte meg a CERT-Hungary program beindítását.[2]

Az igazán jelentős változások a magyar információbiztonság szabályozásában viszont a 2010-es évektől kezdődtek el. Ennek az első jele a 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról volt. Ebben a jogszabályban a kiberteret már, mint komoly fenyegető tényezőt jelölik meg a jogalkotók, felhívva a figyelmet arra, hogy szükségessé vált egy olyan komplex szabályozási rendszer létrehozása, melynek segítségével

[2] Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése*. Budapest, Nemzeti Közszolgálati Egyetem, 2018.

Magyarország felkészülhet az internetről, tágabb értelemben pedig a kibertérből érkező fenyegetések kezelésére. A 2012-es Nemzeti Biztonsági Stratégiából eredeztethetően jelent meg a 1139/2013. (III. 21.) Korm. Határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, mely az első olyan jogszabály volt a magyar jogrendben, mely kimondottan a kibertér biztonságával foglalkozott. A 2013-as kormányhatározat jelenleg is érvényben van, így annak frissítése elkerülhetetlen. A 1163/2020. (IV. 21.) Korm. Határozat Magyarország Nemzeti Biztonsági Stratégiájáról egyértelműen leírja, hogy a 2013-as Nemzeti Kiberbiztonsági Stratégia elavult, és számos olyan változás történt a fenyegetési térben, mely indokolja egy új stratégia kibocsátását. Eszerint:

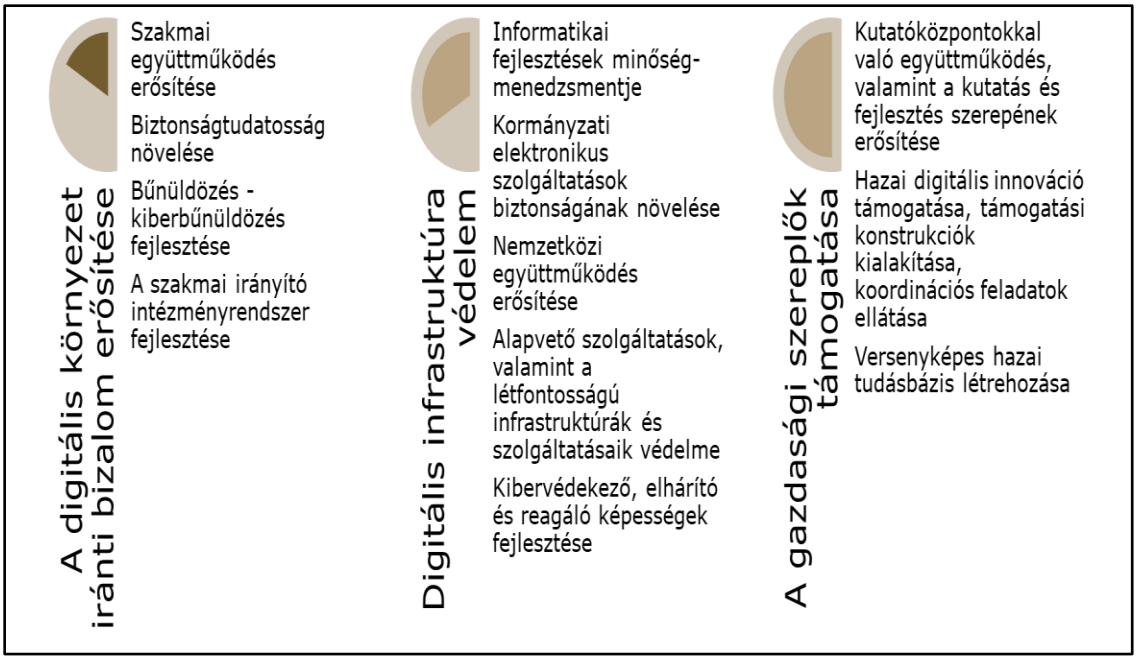


1. ábra: 1139/2013. (III. 21.) Korm. Határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Forrás: saját szerkesztés

„178. A biztonság egyes részterületeiért felelős állami szervezeteknek a Magyarország Nemzeti Biztonsági Stratégiában megfogalmazott iránymutatásokkal összhangban kell megalkotniuk és felülvizsgálniuk a tevékenységükre vonatkozó szakági szabályzókat, különös tekintettel a nemzeti katonai, a rendészeti, a nemzetbiztonsági, a terrorelhárítási, a

katasztrófavédelmi, a kiberbiztonsági és a migrációs területekre."[3]

Hozzá kell tenni, hogy 2018-ban az Európai Unió hálózati és információs rendszerek biztonságára vonatkozó (NIS) direktívájának következményeképpen létrejött egy olyan stratégia, mely részben kiegészíti, részben pedig felülírja a 2013-as eredeti stratégiát. Ez a 1838/2018. (XII. 28.) Korm. Határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról, mely szintén érvényben van, így a tanulmány írásának idején két olyan hatályos stratégiával rendelkezik Magyarország, mely a kibertérre vonatkozik, és részben kiegészítik, részben ellentmondanak egymásnak. Az új stratégia megjelenéséig tehát Magyarország érvényben levő Nemzeti Biztonsági Stratégiája jelent útmutatót számunkra azzal kapcsolatban, hogy a magyar kormány hogyan gondolkodik a kibertér veszélyeiről.



2. ábra: 1838/2018. (XII. 28.) Korm. Határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról. Forrás: saját szerkesztés

Magyarország Nemzeti Biztonsági Stratégiájának alapvetése a következő: *„Nemzeti szuverenitásunk olyan megkérdőjelezhetetlen alapérték, amely természetes módon van jelen hazánk kül- és belpolitikájában egyaránt. Elsődleges biztonságpolitikai érdekünk a folyamatosan változó viszonyok között a magyar állam önrendelkezésének, cselekvési szabadságának oltalmazása, megőrzése és erősítése. Magyarország és a magyar állampolgárok mindenoldalú – politikai, gazdasági, pénzügyi, társadalmi, technológiai, környezeti, egészségügyi,*

[3] 1163/2020. (IV. 21.) Korm. Határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

katonai, rendészeti, információs és kibertérbeli – biztonsága alapvető érték. Biztonságunk megteremtése, fenntartása és erősítése olyan követelmény, amely minden további kormányzati célkitűzés teljesülésének előfeltétele."

Ahogy ebből a tézisből is kiolvasható, a katonai biztonság, illetve az információ- és kibertérbeli biztonság megteremtése egyenlő súllyal jelenik meg a magyar kormány biztonsági gondolkodásában. A Nemzeti Biztonsági Stratégia ezt az alapvetést a továbbiakban részletesen is kibontja. Egyrészt alapvető adottságaink között felsorolja hibrid támadásokkal szembeni felkészülés igényét, másrészt a kiberbiztonsággal kapcsolatos képességek megteremtésének fontosságát:

„31. Hibrid támadással szembeni ellenálló képességünket növeli a nemzet egysége, demokráciánk szilárdsága, a közös nyelv, a felgyorsított döntéshozatali képesség, valamint a honvédelmi és rendvédelmi erők szoros együttműködése egymással és a releváns polgári infrastruktúrával. Az új biztonsági kihívások miatt azonban folyamatosan szükséges fejleszteni az információs és kiberhadviselés elleni védekezés rendszerét.

32. Magyarország Kormánya mindent megtesz hazánk kiberbiztonsága érdekében, kapacitásainkat e területen is folyamatosan fejlesztjük. Tekintettel arra, hogy a kormányzati és más kulcsfontosságú infokommunikációs rendszerek elleni támadások száma növekszik és kifinomultságuk erősödik, folyamatos erőfeszítés szükséges az infokommunikációs rendszerek védelmének erősítése érdekében. Általános jelenség továbbá a felhasználók információbiztonsági tudatosságának alacsony szintje, holott a felhasználók megfelelő információbiztonsági tudatossága a kiberincidensek megelőzésének egyik kulcseleme."

A Nemzeti Biztonsági Stratégiában tehát megjelenik a belbiztonság, illetve a honvédelem konvergenciája a kibertér védelmének érdekében. Ez nem újdonság, hiszen a magyar kibervédelmi szabályozásban a kezdetektől érzékelni lehet a két védelmi terület egyértelmű lehatárolását, közben együttműködésre késztetését, az évtizednyi jogfejlődésben viszont észrevehetően nőtt a katonai terület fontosságának hangsúlyozása. A nemzetközi példákban egyébként két kiberbiztonsági stratégiaalkotási megközelítéssel lehet találkozni. Az egyik az államközpontú, a másik pedig a külső felek bevonását és együttműködését támogató stratégiaalkotás. Míg az államközpontú stratégiák kimondottan belbiztonsági, illetve katonai feladatként tekintenek a kibervédelemre, és elsősorban az állam, a kritikus infrastruktúrák és a honvédség saját rendszereinek védelmére törekednek, addig más, nyitottabb kiberbiztonsági stratégiák figyelembe veszik az államon kívüli szereplők, így a magánszektorban működő cégek, az akadémiai szereplők, illetve a civil szervezetek igényeit is, valamint a védelmi megközelítés mellett gazdasági lehetőségként is tekintenek a kiberbiztonságra.[4] Magyarország a stratégiákból jól kiolvasható módon elsősorban belbiztonsági és katonai

[4] Kovács László: *Kiberbiztonság és -stratégia*. Budapest, Dialóg Campus, 2018.

biztonsági feladatként fogja fel a kibervédelmet, nem törekszik a széles körű bevonásra.

Eközben, amikor Magyarország biztonsági környezetéről ír a Nemzeti Biztonsági Stratégia, számos olyan szempontot is felsorol, mely óhatatlanul igényli az államon és a kritikus infrastruktúra üzemeltetőkön kívül más szereplők bevonását is. A Stratégia 48. pontja így fogalmaz:

„A hatalmi vetélkedés mindinkább kiterjed a globális közjavakra is: fokozódó küzdelem folyik a nemzetközi vizek és az ott található erőforrások, az északi sarkvidék és a világűr ellenőrzéséért, valamint a kibertér dominanciájáért. Az emberiség technológiai szintjének rohamos fejlődésével [digitalizáció, ötödik generációs vezeték nélküli hálózat (5G), űrtechnológia, stb.] folyamatosan új lehetőségek és kihívások jelennek meg, amelyek hatást gyakorolnak hazánk biztonságára. Az 5G jelentette technológia olyan forradalmi fejlesztéseket tehet lehetővé perspektivikusan, amelyek számottevő változásokat generálhatnak társadalmunk és gazdaságunk viszonylatában."

Az itt megjelenített technológiák olyan komplex ökoszisztémát jelentenek, melyeket az kritikus infrastruktúrákat szabályozó kiberbiztonsági jogszabályok nem tudnak teljesen lefedni. Az ellátási láncok kiberfenyegetései beláthatatlan hatással vannak a digitális társadalmak és digitális gazdaságok működésére, így azok komplex védelme a szabályozáson túlmenően az állami és nem állami szereplők együttműködésével valósítható meg sikeresen. A nem állami szereplők szerepét pedig nem csak az együttműködésben, hanem a fenyegetések között is tetten lehet érni.

„69. A technikai fejlődéssel és vívmányainak elterjedésével folytatódik a biztonságot veszélyeztető, nehezen kontrollálható nem állami szereplők – például szervezett bűnözői körök, nemzetközi terrorszervezetek, kiberbűnözői csoportok, szélsőséges vallási közösségek, magán biztonsági cégek, egyes nem kormányzati szervezetek és egyéb transznacionális hálózatok – súlyának növekedése a nemzetközi biztonságpolitikában. Ezek mögött sokszor nehezen azonosítható érdekek és csoportok húzódnak meg, és könnyen szolgálhatnak rejtett állami szándékokat. Mindez átrendezi és áttekinthetetlenebbé teszi egyes térségek biztonsági helyzetét, ami hazánk számára is kihívást jelent.

70. Az információs technológia rohamos fejlődéséből és terjedéséből kifolyólag az állam és a társadalom működése egyre inkább a digitalizációra épül. Az elektronikus információs rendszerek sérülékenységei ezért biztonsági kockázatot hordoznak magukban. Világméretű tendencia, hogy a kibertérben végzett, ártó szándékú tevékenységek egyre gyakoribbak, egyre kifinomultabbak és egyre nagyobb kárral járnak.

71. Növekvőben van azoknak az államoknak és nem állami szereplőknek a száma, amelyek a kiberteret kritikus adatok illegális megszerzésére, valamint az elektronikus információs rendszerekben vagy azokon keresztül történő – akár fizikai – károkozásra használják. Ezért a kibertér ma már a szárazföld, a tengerek, a levegő és a világűr mellett külön műveleti térnek számít. A jövőbeli konfliktusok nagy

valószínűséggel még inkább ki fognak terjedni a kibertérre."

Összegezve, a biztonsági környezet leírásában megjelenik mindaz, amely indukálja a kibervédelem megerősítésének igényét Magyarországon. Foglalkozik az új technológiák megjelenésével, a kiberbűnözés, a kiberhadviselés, a kiberkémkedés, illetve a hacktivista és kiberterrorista csoportok kérdéskörével. Megemlíti az információs műveletek veszélyét is az állami és nem állami szereplők szempontjából, illetve foglalkozik a katonai képességfejlesztés kérdésével is. Ennek során hivatkozik arra, hogy az ötödik műveleti tér, a kibertér is hasonlóan fontos, mint a másik négy műveleti tér Magyarország számára.

Tovább elemezve a Nemzeti Biztonsági Stratégiát, az alapvető érdekeinket felsoroló témák között két érdekes pontot lehet felfedezni. A 101. pont szerint

„Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat fegyveres agressziónak tekinti, amelyre a fizikai térben megvalósuló válaszadás is lehetséges. A kiberműveletek sokszor nehezen bizonyítható attribúciójára, az elkövető azonosítására, megnevezésére való tekintettel a válaszlépések különösen körültekintő, eseti elbírálást igényelnek az érintett kormányzati szervezek bevonásával."

Ez a megfogalmazás teljes mértékben megegyezik a NATO, illetve az Európai Unió különböző szabályozásaival, doktrínáival, egyben kifejezi azt, hogy Magyarország is a kibertéri elrettentés stratégiáját követi, fölhívva a figyelmet minden ellenérdekelt ország számára, hogy egyrészt felkészülünk a válaszadásra, másrészt pedig szövetségeseinkkel együttműködve fogunk diplomáciai vagy akár katonai választ adni a magyar kiberteret érő bármilyen támadásra. Továbbmenve az alapvető érdekek felsorolásában, a 106. pontot kell még megemlíteni, mely szerint

„A forradalmi technológiák fejlesztése stratégiai fontosságú kérdés. Hazánk biztonsága megkívánja, hogy a kulcsfontosságú területeken – mint például a kibervédelem, a mesterséges intelligencia, az autonóm rendszerek, a biotechnológia – kiemelt figyelmet fordítsunk a kutatás-fejlesztésre és annak védelmi összetevőjére."

A védelmi innováció hangsúlyozása a magyar kormány számára évek óta kiemelten fontos, párhuzamosan a haderőnemi fejlesztésekkel, és ahogy a stratégiából kiolvasható, ebben a fejlesztésben a kibervédelemnek is kiemelt szerepe van. Ha ehhez hozzátesszük azt, hogy a mesterséges intelligencia is szerepel a felsorolt technológiák között, akkor egyértelműen következik, hogy a magyar állam tudomásul vette a mesterséges intelligencia alkalmazásának elkerülhetetlenségét, melynek következtében ezek a technológiák meg kell, hogy jelenjenek hazánk kibervédelmében is.

A Nemzeti Biztonsági Stratégia a kiemelt biztonsági kockázatok között, a 124. pontban fogalmazza meg a következőket

„A változékony globális környezetben számos kihívás, kockázat és fenyegetés irányulhat hazánk vagy szövetségi rendszereink ellen. Magyarország Nemzeti

Biztonsági Stratégiájában meghatározott értékeink és adottságaink alapján, az elemzett biztonsági környezetben a következő kihívások nemzeti érdekeinkre gyakorolt hatása a leginkább jelentős: (…)

d) jelentős károkat okozó kibertámadások a kormányzati informatikai rendszerek, az E-közigazgatás, a közműszolgáltatók, a stratégiai vállalatok, a létfontosságú infrastruktúra egyéb elemei és más, a társadalom működésében fontos szervezetek számítógépes hálózatai ellen;"

Elemezve ezt a pontot, továbbra is megerősítve láthatjuk, hogy Magyarország jellemzően államközpontú kibervédelem megvalósításában gondolkodik, egyrészt az állam számára fontos stratégiai adatok, másrészt pedig a kritikus infrastruktúrák védelme szerepel a kiemelt védendő területek között. Ahogy azt az egyéb releváns jogszabályokban is látni lehet, az adat, illetve az infrastruktúra védelmének együttes hangsúlyozása folyamatosan megjelenik. Az adat esetében a bizalmasság, a sértetlenség és a rendelkezésre állás, az infrastruktúra esetében a sértetlenség és a rendelkezésre állás biztosítása a kiemelten fontos feladat.

A Stratégia 135. határozza meg explicit módon a Magyar Honvédség kibertéri feladatkörét:

„135. A Magyar Honvédségnek jól felszerelt és jól kiképzett erőkkel, valamint rugalmas, hatékonyan alkalmazható, telepíthető és fenntartható, a szükséges mértékben interoperábilis képességekkel kell rendelkeznie, a mennyiségi mellett a minőségi mutatók javítására törekedve. Hagyományos országvédelmi és nemzetközi válságkezelési feladatai mellett egyaránt alkalmasnak kell lennie a tömeges bevándorlás okozta válsághelyzet, vagy a terrorveszély-helyzet kezeléséhez történő hozzájárulásra, a hibrid támadások elhárításában való szerepvállalásra, valamint a természeti vagy ipari katasztrófák következményeinek felszámolásában való közreműködésre. A haderőt úgy kell fejleszteni, hogy képes legyen hatásokat kiváltani a hazánk szempontjából releváns összes műveleti térben: a szárazföldön, a levegőben és a kibertérben egyaránt."

A kibertér kiemelése, mint a Magyar Honvédség számára fontos műveleti tér jelzi azt is, hogy olyan képességeket kell fejleszteni, amelyek túlmennek korábbi képességein, és természetszerűleg ezeket a képességeket fel kell tudnia ajánlani a szövetségi rendszerben is. Ebben a pontban ki kell még emelni a hibrid fenyegetésekre való hivatkozást, hiszen, ha együtt kezeljük a kibertérben, illetve az információs térben szereplő veszélyek együttesét, akkor jól érthető, hogy miért alakult át a Magyar Honvédség szervezeti rendszere 2019-től kezdődően és jött létre az MH Kiber- és Információs Műveleti Központ, illetve miért konvergálnak egymáshoz a klasszikus információs műveletek, illetve a kibertéri katonai műveletek.

A Stratégia az átfogó feladatok és eszközök felsorolása között a 159. pontban tovább elemzi a különböző teendőket, és így fogalmaz

„A kibertérben jelentkező kihívások, kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelmi feladatok ellátására, a nemzeti létfontosságú információs infrastruktúra zavartalan működésének biztosítására

Magyarországnak készen kell állnia. Elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális kihívások, kockázatok és fenyegetések azonosítása és nyomon követése, a kormányzati koordináció erősítése, a kibertér jogi szabályozásának fejlesztése, a felhasználók biztonságtudatos viselkedésének elősegítése, a kormányzati infokommunikációs rendszerek, a nemzeti létfontosságú információs infrastruktúra, a minősített információk és a nemzeti adatvagyon védelmének erősítése, valamint a kiberbiztonsággal kapcsolatos nemzetközi együttműködés bővítése. A katonai kibervédelmet növekvő mértékben alkalmassá kell tenni a haderő kinetikus műveleteinek kibertérbeli támogatására, ki kell alakítani a kiberműveletekben alkalmazható offenzív képességeket. Ennek érdekében fejleszteni kell a Magyar Honvédség kibervédelmi és kiberműveleti erőit."

Ez a pont gyakorlatilag keretbe foglalja Magyarország 2013-tól létrejövő információbiztonsági és kibervédelmi szabályozásait. Reflektál mindazokra a pontokra, melyek az egyes jogszabályokban megtalálhatóak, viszont újdonságként kiemeli a kiberműveletekben alkalmazható offenzív képességek megteremtésének szükségességét. A korábbi nemzeti szabályozás nem foglalkozott az offenzív képességek fontosságával, sőt, amikor a korábbi jogalkotási szakaszban előkerült az offenzív képességek fejlesztésének igénye, akkor a 2010-es években az ehhez szükséges politikai támogatást nem sikerült megszerezni. A 2020-as Stratégia tehát jelentős eltérést mutat a korábbi gondolkodástól, és deklaráltan jelzi Magyarország ellenérdekelt országainak számára, hogy hazánk offenzív kibertéri képességével számolni kell.

A 160. pont szintén a nem állami szereplők bevonásának szükségességére hívja fel a figyelmet, akik nélkül a kiberképességek fejlesztése, az új technológiákhoz kapcsolódó innováció és ezek használatának elterjesztése elképzelhetetlen:

„Elengedhetetlen a nemzeti kibervédelmi képességek hazai bázisú kutatás-fejlesztéssel megalapozott erősítése, a korszerű technikai eszközök biztosítása. A kibervédelmi feladatok összetettsége miatt partnerséget kell kialakítani az állami és a magánszektor szereplői, az oktatási és a tudományos intézmények és az egyéni felhasználók között."

Ahogy arra is rávilágít a joganyag, hogy a nemzeti kibervédelem nemzetközi együttműködés nélkül nem működik. Ezt az együttműködést elsősorban a szövetségi rendszerben kell elképzelni, melynek alapja a bizalom kiépítése és megerősítése, oly módon, hogy akár politikai, akár technológiai szinten gyorsan és hatékonyan lehessen fellépni az országot érő kibertéri támadásokkal szemben.

„162. A kibertérrel kapcsolatos kihívások hatékony kezelése nemzetközi együttműködés nélkül elképzelhetetlen. Aktívan részt veszünk a globális kibertérben való felelős viselkedést szabályozó normák és a globális kiberbiztonság fokozására szolgáló bizalomerősítő intézkedések kidolgozására és végrehajtására irányuló nemzetközi erőfeszítésekben."

A Stratégia zárógondolata Magyarország biztonságának

megteremtéséről is kiemeli a kibertér jelentette fenyegetések kezelését:

„175. A tömegpusztító fegyverek, a terrorizmus, a kibertámadások, a hibrid műveletek és a katasztrófák elleni védelem egyaránt megköveteli hazánk nemzeti ellenálló képességének fokozását."

A KIBERVÉDELEM SZAKPOLITIKAI SZINTJÉNEK HELYZETE ÉS KIHÍVÁSAI A NATO-BAN

A hidegháborút követően a NATO-nak a '90-es évek végén, a 2000-es évek elején máris egy újabb kihívással került szembe, amely addig elképzelhetetlen volt, még a szakembereknek is csak egy nagyon szűk köre volt, aki ezzel foglalkozott, erre próbálta felhívni a figyelmet. Ez a számítógépes hálózatok ért támadások, amelyeket ma kibertámadásoknak nevezünk, és amelyekkel a NATO elsőként az 1999-es koszovói bombázásokat követően szembesült leginkább. 1999. március 24-én, miután a NATO főtitkár bejelentette, hogy csapást mér a szerb célpontokra, megindultak az első kibertámadások a NATO ellen. A támadások alapvető célja a műveleti központ működésének zavarása, valamint a szövetségi honlapok elérhetetlenségének kiharcolása volt. Ezen túlmenően a támadásokért felelős szerb hackercsoport, a Fekete Kéz (Crna Ruka) politikai üzeneteket helyezett el több kormányzati weboldalon, valamint több alkalommal megpróbált betörni a Szövetség parancsnoki szervereire, többnyire sikertelenül. Mindazonáltal sikeresen behatoltak a légierő számítógépes hálózatába, azonban ott nem tudtak hozzáférni semmilyen érzékeny információkhoz. Miután a belgrádi kínai nagykövetséget is bombatámadás érte kínai és később orosz hackerek is csatlakoztak a támadókhoz, akik a jelentések szerint legalább 14 katonai és állami honlapot támadtak meg és tettek elérhetetlenné a balkáni háború alatt. Ezek a támadások viszonylag kisebb jelentőségűek voltak, súlyosságuk nem érte el azt a szintet, amikor ténylegesen átlépték volna azt a határt, ahol katonai kollektív védelemre lenne szükség.

A koszovói és az azt követő kiberincidensek azonban nagyban hozzájárultak ahhoz, hogy a döntéshozók felismerték a kibervédelem fontosságát. Ennek megfelelően a 2002-es prágai csúcstalálkozón kimondták, hogy a szövetségnek meg kell erősítenie a kibertámadások elleni védekezési képességeit, ami arra utal, hogy a szövetségesek ráébredtek a kibertámadások veszélyeire. Ezt erősíti meg az a tény is, hogy elindították a NATO kibervédelmi programját, amely magában foglalta a NATO számítógépes incidensekre való reagálási képességének (NATO Computer Incident Response Capability – NCIRC) kifejlesztését. Az e képesség mögött álló szervezet alapvető célja a NATO-rendszerekbe történő behatolások észlelése és szükség esetén a válaszadás.

Ezt követően a védelmi miniszterek 2007. június 14-i brüsszeli találkozóján a résztvevők a tagállamok kibervédelmi erőfeszítései egységesítésének szükségességére hívták fel a figyelmet. Ennek eredményeként a NATO 2008-ban új kibervédelmi irányelvet fogadott el e

folyamatok összehangolása érdekében. Ennek kialakítását nagyban ösztönözte a 2007-ben történt átfogó kibertámadás sorozat Észtország ellen, amelyben Európa egyik leginkább digitalizált országát támadták meg. A támadássorozat volt az első, amely megmutatta, hogy mit is eredményezhet pontosan egy kiberháború a valóságban, ami számos politikai és katonai vezetőt elgondolkodtatott, hogy komoly lépéseket kell tenni a területen.[5] Az egy évvel későbbi orosz-grúz konfliktus ismét rávilágított az információs műveletek, köztük a kiberhadviselés növekvő szerepére. A csúcstalálkozó során a NATO tisztviselői és kiberszakértők áttekintették az észtországi tapasztalatok tanulságait. A 2008-as bukaresti csúcstalálkozó vezetői nyilatkozatának 47. szakasza kimondta, hogy:

„47. A NATO továbbra is elkötelezett, hogy megerősítse a Szövetség kulcsfontosságú információs rendszereit a kibertámadásokkal szemben. Nemrég elfogadtuk a Kibervédelmi Irányelvet, és továbbra is fejlesztjük az ezt megvalósító szervezeteket és hatóságokat. A Kibervédelmi Irányelv hangsúlyozza, hogy a NATO-nak és a nemzeteknek is meg kell védeniük kulcsfontosságú informatikai rendszereiket saját felelősségi körükben; meg kell osztaniuk a legjobb gyakorlatokat és biztosítaniuk kell azokat a képességet, amelyekkel erre vonatkozó kérést követően egy szövetséges állam segítségére siethetnek egy kibertámadás elhárítására. Bízunk benne, hogy folytatódik a NATO kibervédelmi képességeinek fejlesztése és a kapcsolatok erősítése a NATO és a nemzeti hatóságok között."[6]

Mindezek eredményeképpen 2008 májusában létrejött a NATO Kooperatív Kibervédelmi Kiválósági Központ (NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE) a NATO által akkreditált tudásközpont és képzési intézmény, amelynek fő feladata kutatások és fejlesztések, valamint konzultációk, képzések és gyakorlatok szervezése és lebonyolítása a kiberbiztonság területén, a nemzetközi katonai környezetre összpontosítva. A Központ küldetése a képességek, az együttműködés és az információcsere fokozása a NATO, a szövetségesek és a partnerek között a kibervédelem területén.

A NATO a 2010-es lisszaboni csúcstalálkozón új stratégiai koncepciót fogadtak el, amelynek során az Észak-atlanti Tanácsot (North Atlantic Council – NAC), a NATO legfőbb döntéshozó testületét megbízták egy alapos kibervédelmi politika kidolgozásával és az erre vonatkozó cselekvési terv elkészítésével. A dokumentumszövetség vezetői remélik, hogy a várva várt dokumentum megerősíti a transzatlanti köteléket, és felkészíti a NATO-t az új kihívások hatékony kezelésére. A csúcstalálkozón hozott döntésekkel kapcsolatban Jamie Shea, főtitkárhelyettes a következőket mondta:

[5] Bányász Péter – Krasznay Csaba – Tóth András: A NATO kibervédelmi szakpolitikája. In: Szenes Zoltán (szerk.): *A mai NATO : A szövetség helyzete és feladatai.* Budapest, HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft., 2021, 130–149. o.

[6] Szentgáli Gergely: A NATO kibervédelmi politikájának fejlődése. *Bolyai Szemle,* 2012/2. szám, 80–85. o.

"Az új NATO-politika nemcsak azt teszi lehetővé, hogy a NATO gyorsabban és hatékonyabban védje saját hálózatait, hanem sokkal több segítséget nyújt a szövetségeseknek és a partnereknek a kiberbiztonság mindhárom kulcsfontosságú területén: megelőzés, a kibertámadások kezelése és hatásuk csökkentése, valamint a megtámadott országok segítése a létfontosságú információs rendszereik gyors visszaállításában és helyreállításában".

A csúcstalálkozót követően a tagállamok egy, a számítógépes rendszerek elleni támadások elhárítására összpontosító gyakorlatot tartottak Cyber Coalition 2010 néven. A gyakorlat során több tagállam és a főparancsnokság számítógépes rendszereit külső támadás érte, és a cél az volt, hogy a lehető leggyorsabban és legpontosabban azonosítsák az elkövetőket vagy a támadás eredetét. Az ilyen gyakorlatok mindenesetre hozzájárulnak a NATO kiberelhárítási képességeinek javításához, nem utolsósorban az elrettentés erősítéséhez.[7]

2011 júniusában a NATO védelmi miniszterei jóváhagyták a kibervédelemről szóló második NATO-irányelvet, amely a gyorsan változó fenyegetések és technológiai környezet összefüggésében egy szövetségen belüli összehangolt kibervédelmi erőfeszítésekre vonatkozó jövőképet fogalmazott meg. Ezt egy végrehajtási cselekvési terv kísérte. Az átdolgozott kibervédelmi irányelv a következő fő célokat tűzte ki:

- A kibervédelmi megoldások és elképzelések integrálása a NATO struktúráiba és tervezési folyamataiba a NATO kollektív védelemmel és válságkezeléssel kapcsolatos alapvető feladatainak ellátása érdekében.
- A NATO és a szövetségesek számára létfontosságú kibereszközök ellenálló képességére és védelmére, valamint a támadások megelőzésére való összpontosítás.
- Erős kibervédelmi képességek fejlesztése és a NATO saját hálózatai védelmének központosítása.
- A NATO alapvető feladatai szempontjából kritikus nemzeti hálózatok kibervédelmére vonatkozó minimumkövetelmények kidolgozása.
- Segítségnyújtás a szövetségeseknek a kibervédelem minimális szintjének eléréséhez és a nemzeti kritikus infrastruktúrák sebezhetőségének csökkentéséhez.
- Együttműködés a partnerekkel, nemzetközi szervezetekkel, a magánszektorral és a tudományos közösséggel.[8]

2012 áprilisára a kibervédelem is a NATO védelmi tervezési folyamatának részévé vált, így azóta a védelmi tervezési folyamatok keretében folyamatosan azonosítják és rangsorolják a vonatkozó kibervédelmi követelményeket. A 2012 májusi chicagói csúcstalálkozón a szövetséges vezetők megerősítették a

[7] Bányász Péter – Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. *Hadtudomány,* 2013/elektronikus szám, 188–209. o.

[8] NATO: *Defending the networks*. (2011. augusztus 19.).

szövetség kibervédelmének javítása iránti elkötelezettségüket azáltal, hogy a NATO összes hálózatát központosított védelem alá helyezték, és egy sor fejlesztést hajtottak végre az NCIRC – a NATO kibervédelmi képességének – tekintetében. Mindezekkel kapcsolatban a résztvevők az alábbiakat fogalmazták meg:

„49. A kibertámadások száma továbbra is jelentősen növekszik, és egyre kifinomultabbá és összetettebbé válnak. Megerősítjük a lisszaboni csúcstalálkozón tett kibervédelmi kötelezettségvállalásokat. Lisszabont követően tavaly elfogadtuk a kibervédelmi koncepciót, irányelvet és cselekvési tervet, amelyeket most hajtunk végre. A NATO meglévő képességeire építve 2012 végére létrejönnek a NATO számítógépes incidensekre való reagálási képességének (NCIRC) kritikus elemei, beleértve a legtöbb helyszín és felhasználó védelmét is. Kötelezettséget vállaltunk arra, hogy biztosítjuk a forrásokat és végrehajtjuk a szükséges reformokat, hogy valamennyi NATO-szervetet központosított kibervédelem alá vonjuk, annak biztosítása érdekében, hogy a megerősített kibervédelmi képességek megvédjék a NATO-ba történő kollektív befektetésünket. A kibervédelmi intézkedéseket tovább fogjuk integrálni a szövetségi struktúrákba és eljárásokba, és mint egyes nemzetek, továbbra is elkötelezettek vagyunk a nemzeti kibervédelmi képességek azonosítása és megvalósítása mellett, amelyek erősítik a szövetségi együttműködést és interoperabilitást, többek között a NATO védelmi tervezési folyamatain keresztül. Továbbfejlesztjük a kibertámadások megelőzésére, felderítésére, az ellenük való védekezésre és az azokból való helyreállításra irányuló képességeinket. A kiberbiztonsági fenyegetések kezelése és közös biztonságunk javítása érdekében elkötelezettek vagyunk amellett, hogy a konkrét együttműködés fokozása érdekében eseti alapon együttműködjünk az érintett partnerországokkal, valamint nemzetközi szervezetekkel, többek között az EU-val – megállapodás szerint – az Európa Tanáccsal, az ENSZ-szel és az EBESZ-szel. Teljes mértékben ki fogjuk használni az észtországi Kooperatív Kibervédelmi Kiválósági Központ által kínált szakértelmet is."[9]

2012 júliusában a NATO ügynökségeinek reformja keretében létrehozták a NATO Kommunikációs és Információs Ügynökségét (NATO Communications and Information Agency – NCIA). Ezekkel a lépésekkel és intézkedésekkel a NATO elmélyítette a kapcsolatot más nemzetközi szervezetekkel, és kezdetét vette az együttműködések kialakítása, amely nagymértékben hozzájárul a létfontosságú információs infrastruktúrák védelméhez.

2013-ban megjelent a Tallinni Kézikönyv (Tallinn Manual), amely alapvetően azokkal a kiberműveletekkel foglalkozik, amelyek sértik az erőszak alkalmazásának tilalmát, feljogosítják az államokat az önvédelem jogának gyakorlására, vagy fegyveres konfliktus során történnek, és elemzi a nemzetközi jog kiberhadviselésre való alkalmazásának köreit. Kiemeli az egyes elemzett esetek

[9] NATO: *Chicago Summit Declaration.* (2022. július 05.).

vonatkozásában az államok lehetséges szerepét, a nemzetközi humanitárius jog és a semlegesség jogának kérdéseit, továbbá a szuverenitást.

2014 februárjában a szövetséges védelmi miniszterek megbízták a NATO illetékes szervezeteit, hogy dolgozzanak ki egy új, továbbfejlesztett kibervédelmi politikát a kollektív védelem, a szövetségeseknek nyújtott segítség, az egységes kormányzás, a jogi megfontolások és az iparral való kapcsolatok tekintetében. Ennek eredményeképpen a 2014 szeptemberi walesi csúcstalálkozón a szövetségesek jóváhagyták a NATO új kibervédelmi irányelvét, és jóváhagytak egy cselekvési tervet, amely az irányelvvel együtt hozzájárul a szövetség alapvető feladatainak teljesítéséhez. A NATO kollektív védelemmel kapcsolatos alapvető feladatának részeként ismerték el a kibervédelmet, és a szövetségesek egyetértettek abban, hogy a kibertérben a nemzetközi jog alkalmazandó. Az ezt megfogalmazó nyilatkozat a kibervédelmet az átfogó védelmi csomag részévé tette, ami azt jelzi, hogy a NATO továbbra is komoly problémának tekintette a kiberfenyegetéseket, amelyek a kibertámadások elleni kollektív védekezést igénylik. A csúcstalálkozó nyilatkozata a továbbiakban megerősítette a kibővített kibervédelmi irányelvet:

"72. Ahogy a Szövetség a jövőbe tekint, a kiberfenyegetések és -támadások egyre gyakoribbá, kifinomultabbá és potenciálisan károsabbá válnak. E változó kihívással való küzdelem érdekében kiterjesztett kibervédelmi irányelvet fogadtunk el, amely hozzájárul a Szövetség alapvető feladatainak teljesítéséhez. A politika megerősíti a szövetségi biztonság, valamint a megelőzés, a felderítés, az ellenálló képesség, a helyreállítás és a védelem oszthatatlanságának elvét. Figyelmeztet arra, hogy a NATO alapvető kibervédelmi felelőssége saját hálózatainak védelme, és hogy a szövetségeseknek nyújtott segítséget a szolidaritás szellemével összhangban kell kezelni, hangsúlyozva a szövetségesek felelősségét a nemzeti hálózatok védelmére vonatkozó képességek kifejlesztésében. Irányelvünk azt is elismeri, hogy a nemzetközi jog, beleértve a nemzetközi humanitárius jogot és az ENSZ Alapokmányát, a kibertérben is alkalmazandó. A kibertámadások elérhetik azt a küszöböt, amely a nemzeti és euroatlanti jólétet, biztonságot és stabilitást veszélyezteti. Hatásuk ugyanolyan káros lehet a modern társadalmakra, mint egy hagyományos támadás. Ezért megerősítjük, hogy a kibervédelem a NATO kollektív védelmi alapfeladatának része. Arról, hogy egy kibertámadás mikor vezetne az 5. cikk alkalmazásához, az Észak-atlanti Tanács eseti alapon döntene."[10]

Ezzel először fogalmazták meg, hogy egy kibertámadás akár az 5. cikk hatálya alá is tartozhat, ennek megfelelően egy tagállam kibertérben történő megtámadása minden tagállam elleni támadásnak minősül, ennek megfelelően támogatni fogják a megtámadott felet vagy feleket akár fegyveres erő alkalmazásával is. Ebben a megfogalmazásban leginkább a kibertámadások hatásával foglalkoztak, és hogy a kibertérben végrehajtott műveletek

[10] NATO: *Wales Summit Declaration*. (2022. július 04.).

hatása megegyezhet a hagyományos támadásokéval. A walesi csúcstalálkozó döntései azt is megerősítették, hogy a kibervédelmi képességek fokozása érdekében tovább kell fejleszteni az ipari együttműködést, amellyel kapcsolatosan a NATO húsz területet határozott meg a kibervédelem minimális képességeinek fejlesztésével kapcsolatosan. Ezek közé a területek közé tartozik többek között a stratégiafejlesztés, az együttműködés, az oktatás és az információbiztonság.[11]

A 2012-es chicagói csúcstalálkozón elhangzottak megerősítéseképpen 2016. február 10-én a NATO és az EU technikai megállapodást kötött a kibervédelemről, amelynek alapvető célja, hogy mindkét szervezet hatékonyabban tudja megelőzni a kibertámadásokat, illetve jobban tudjon reagálni rájuk. Az NCIRC és az EU Számítógépes Vészhelyzeti Reagáló Csoportja (Computer Emergency Response Team for the EU – CERT-EU) közötti technikai megállapodás keretet biztosít az információcseréhez és a legjobb gyakorlatok megosztásához a vészhelyzeti reagáló csoportok (Emergency Response Team) között.

A 2016 júniusi varsói csúcstalálkozón a szövetséges állam- és kormányfők elismerték, hogy a kibertér olyan műveleti terület, amelyen a NATO-nak ugyanolyan hatékonyan kell védekeznie, mint a levegőben, a szárazföldön és a tengeren. Ez javította a NATO védelmi képességeit, amelyekkel kapcsolatosan a csúcstalálkozóról készített nyilatkozat a következőt mondja:

„70. A kibertámadások egyértelműen kihívást jelentenek a Szövetség biztonsága szem-pontjából, és ugyanolyan károsak lehetnek a modern társadalmak számára, mint a hagyományos támadások. Walesben megállapodtunk abban, hogy a kibervédelem része a NATO kollektív védelmi feladatainak. Most Varsóban megerősítjük a NATO védelmi mandátumát, és elismerjük a kiberteret olyan műveleti területnek, amelyben a NATO-nak olyan hatékonyan kell megvédenie magát, mint a levegőben, a szárazföldön és a tengeren. Ez javítani fogja a NATO azon képességét, hogy ezeken a területeken védje és végezze műveleteit, és minden körülmények között megőrizze cselekvési és döntéshozatali szabadságát. Továbbá támogat-ja a NATO szélesebb körű elrettentését és védelmét: a kibervédelem továbbra is beépül a működési tervezésbe és a Szövetség műveleteibe és küldetéseibe, és együtt fogunk dolgozni, hogy hozzájáruljanak a sikerhez. Ezenkívül biztosítja a NATO-kibervédelem hatékonyabb megszervezését és az erőforrások, készségek és képességek jobb kezelését. Ez a NATO hosszú távú alkalmazkodásának része. Továbbra is végrehajtjuk a NATO-nak a kibervédelemre vonatkozó továbbfejlesztett politikáját, és megerősítjük a NATO kibervédelmi képességeit, kihasználva a legújabb élvonalbeli technológiákat.”[12]

Mindez azt mutatja, hogy a vezetők célul tűzték ki a kibervédelem javítását,

[11] Bányász Péter: *A közösségi média lehetőségei és kihívásai a védelmi szférában*. Doktori (PhD) értekezés, Budapest, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola 2018.

[12] Paráda István: A NATO kibervédelmi irányelveinek fejlődése. *Honvédségi Szemle*, 2018/3. szám. 3–13. o.

annak nagyobb mértékű integrálását a tervezési folyamatokba, valamint a nemzeti és szövetséges hálózatok védelmének fokozását a legmodernebb technológiák alkalmazásával. Varsóban mindezek mellett elfogadtak egy Kibervédelmi Vállalást (Cyber Defence Pledge) is, amelyben nyilatkoztak arról, hogy jelentősen fejleszteni fogják nemzeti hálózataik és infrastruktúráik védelmét. Ennek megfelelően kötelezettséget vállaltak arra, hogy a védelmi szervezetekben kiépítik a kibervédelmi képességek teljes skáláját, megfelelő forrásokat különítenek el a nemzeti szintű képességfejlesztésre, elmélyítik a fenyegetések és védelmi tevékenységek azonosítására és értelmezésére irányuló együttműködést, valamint fokozzák a kibervédelmi oktatást és képzést. Ezekkel egyidejűleg a 2014-es walesi csúcstalálkozót követően a varsói csúcstalálkozón a vezetők megerősítették a kollektív védelem kibertérre történő kiterjesztésére tett döntésüket, ezzel hivatalosan is deklarálva azt.[13]

2017. februárjában a szövetséges védelmi miniszterek jóváhagyták a kibervédelmi cselekvési terv aktualizált változatát, valamint a kibertér, mint műveleti terület megvalósításának ütemtervét. Ez nagymértékben hozzájárult a szövetségesek együttműködési képességének, a képességek fejlesztésének és az információmegosztás lehetőségeinek növeléséhez. Ebben az évben jelent meg a Tallinni Kézikönyv 2.0, amely a nemzetközi jog azon szabályait vizsgálja, amelyek az államok által nap, mint nap tapasztalt, de az erő alkalmazásának vagy a fegyveres konfliktusnak a küszöbértékét el nem érő kiberincidensekre vonatkoznak. A szuverenitás és az állami felelősség mellett olyan kérdésekkel is foglalkozik, mint az emberi jogok, valamint a levegő, a világűr és a tenger joga.

A 2018-as brüsszeli csúcstalálkozón a szövetséges vezetők megállapodtak abban, hogy tovább optimalizálják a NATO hírszerzési tevékenységeit, hogy elősegítsék a szövetséges döntéshozatalt és a műveletek időben történő és releváns támogatását, többek között a riasztások és a hírszerzési információk megosztásának javítása révén, különösen a terrorizmussal, a hibrid és a kibertérrel kapcsolatban. Kimondták, hogy a NATO továbbra is alkalmazkodni fog a folyamatosan változó kiber-fenyegetettségekhez, amelyeket állami és nem állami szereplők egyaránt befolyásolhatnak. A csúcsértekezleten hozott döntések alapján Belgiumban az európai műveleti parancsnokságon belül (SHAPE) létrehoztak egy kibertér-műveleti központot (Cyber Operational Center – CyOC), amely a NATO kibertéren belüli operatív tevékenységének helyzetfelismerését és koordinálását biztosítja.[14]

A 2019-es londoni csúcstalálkozón is szintén több a kibervédelmet érintő döntés született. Megállapodtak abban, hogy növelik a kibertámadásokra reagáló eszközök és képességek számát, ezáltal erősítik a biztonságot a szövetségen belül,

[13] Berki Gábor: *Kiberháborúk, kiberkonfliktusok. Műhelymunkák*. Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016, 245–284. o.

[14] Mitko Bogdanoski: Building Cyber Resilience against Hybrid Threats. *NATO Science for Peace and Security Series - D: Information and Communication Security*, 2022.

valamint felkészülnek a társadalmat veszélyeztető hibrid fellépésekre, megfelelő védelmi megoldásokat dolgoznak ki, valamint alkalmazzák az elrettentés módszerét. Elhangzott, hogy a NATO és a szövetségesek elkötelezettek amellett, hogy saját területükön megerősítsék a kommunikáció biztonságát, beleértve az 5G-t is, felismerve, hogy a feladatok végrehajtása során minden körülmények között biztonságos és rugalmas kommunikációs rendszerekre kell támaszkodni. A csúcstalálkozó másik eredménye, hogy a NATO a világűrt műveleti dimenzióvá nyilvánította, felismerve annak fontosságát biztonságunk megőrzésében és a biztonsági kihívások kezelésében, a nemzetközi jog tiszteletben tartása mellett.[15] Az NCIA még ebben az évben megkezdte a Kiberbiztonsági Együttműködési Központ (Cyber Security Collaboration Hub) létrehozását, amely a tagállamok számára egy titkos információgyűjtési, együttműködési és képzési platformot biztosít. Az NCIA korábban is szolgáltatott információkat a szövetséges nemzeti számítógépes vészhelyzeti reagáló csoportok (CERT) részére, de NATO CERT-közösség nem létezett.

Az Észak-atlanti Tanács 2020. június 3-án kiadta nyilatkozatát a rosszindulatú kibertevékenységekről (North Atlantic Council Statement on Malicious Cyber Activities 2020), amelyben elítélte a destabilizáló és rosszindulatú kibertevékenységeket a koronavírus világjárvánnyal összefüggésben. A NATO-nyilatkozat szolidaritásáról és kölcsönös támogatásáról biztosította a rosszindulatú kibertevékenységek által érintetteket, köztük az egészségügyi szolgálatokat, kórházakat és kutatóintézeteket. A nyilatkozat a nemzetközi jog és a felelős állami magatartás normáinak tiszteletben tartására szólított fel a kibertérben, miután a Kínából vagy Oroszországból irányított dezinformációs kampányok elárasztották a nyugati médiát és a közösségi hálózatokat.[16]

A 2021. júniusi brüsszeli csúcstalálkozón a szövetségesek elismerték a változó fenyegetettségi környezetet, felismerve, hogy a kibertér folyamatos támadásoknak van kitéve. A szövetségesek új, átfogó kibervédelmi irányelvet hagytak jóvá, amely támogatja a NATO három alapvető küldetését, a kollektív védelmet, a válságkezelést és az kooperatív biztonságot, valamint hozzájárul a NATO általános elrettentő és védelmi pozíciójának fenntartásához. A NATO-nak mindenkor – békeidőben, válságban és konfliktusban – politikai, katonai és technikai szinten is aktívan elrettentenie, védenie és elhárítania kell a kiberfenyegetések teljes spektrumát.

A CCDCOE a közelmúlt kibernetikai eseményeire és konfliktusaira reflektálva 2022-ben közzétette a Kibertér stratégiai kilátások 2030 (Cyberspace Strategic Outlook 2030) című dokumentumát. A kiadvány a NATO kiberfenyegetésekre adott válaszaira összpontosít a 2022-2030-as időszakban, kitérve az új és átalakuló technológiákra, a fejlődő

[15] NATO: *London Declaration*. (2022. július 01.).
[16] Dragoș-Mihai Păunescu: NATO's encounters in the cyber domain. *Proceedings of the 17th International Scientific Conference "Strategies XXI" - Strategic Changes in Security and International Relations*, 2021/1. szám.

kiberfenyegetésekre, a kibertér szereplőinek stratégiáira és tevékenységeire, valamint a változások egyéb mozgatórugóira. Elemzi és értékeli, hogyan lehet a Szövetséget katonailag és politikailag megerősíteni a kiberfenyegetésekkel szemben.[17]

A NATO saját elemzései és dokumentumai alapján összességében úgy fogalmaz, hogy míg minden egyes szövetséges fél felelős a saját kibervédelméért, a NATO platformként szolgál a szövetségesek számára, hogy konzultáljanak kibervédelmi kérdésekről, megosszák a kiberfenyegetésekkel kapcsolatos információkat, kicseréljék a legjobb gyakorlatokat, és összehangolják a tevékenységeiket. A NATO támogatja tagjait a kibervédelem megerősítésében, például a következőkkel:

- A fenyegetésekkel kapcsolatos valós idejű információk megosztásával egy külön erre a célra létrehozott, rosszindulatú szoftverekkel kapcsolatos információmegosztó platformon (malware information sharing platform – MISP) keresztül, valamint a kiberfenyegetésekre való reagálásra vonatkozó legjobb gyakorlatok cseréjével;
- Gyorsreagálású kibervédelmi csapatok fenntartásával, amelyeket a szövetségesek segítségére lehet küldeni a kibertérben jelentkező problémák kezelése céljából;
- A szövetségesek számára célok kidolgozásával a kibervédelmi képességeik közös megközelítésének megkönnyítése érdekében;
- Az oktatásba, képzésbe és gyakorlatokba való befektetéssel, mint például a Cyber Coalition, az egyik legnagyobb kibervédelmi gyakorlat a világon.

A szövetségesek nemzeti felelősségeikkel és hatáskörükkel összhangban elkötelezettek a kritikus infrastruktúrájuk védelme, az ellenálló képesség kiépítése és a kibervédelem megerősítése mellett, többek között a NATO kibervédelmi vállalásnak teljes körű végrehajtása révén.[18]

A KIBERVÉDELEM SZAKPOLITIKAI SZINTJÉNEK HELYZETE ÉS KIHÍVÁSAI AZ EURÓPAI UNIÓBAN

A NATO kiberbiztonság stratégiájának fejlődése mellett fontos az Európai Unió ez irányú stratégiaalkotás folyamatának vizsgálta is, már csak azért is, hiszen jelentős előzményei azoknak az európai jogszabályoknak, amik az adat-, információ- és hálózatbiztonság szempontjából Magyarország normatív szabályozási környezetében is szerepet kap. A helyzetet nehezíti az Európai Unió jogalkotásának, illetve államszerkezetének sajátosságai. Visszatérő vita többek között, hogyan is kell értelmezni az EU-t, konföderációnak, föderációnak, az általa meghozott normatív szabályozók az egyes tagállamokra milyen kötelezettségeket rónak. Az EU-val kapcsolatos tanulmányok kiinduló tétele az

[17] Piret Pernik (szerk.): *Cyberspace Strategic Outlook 2030*. Tallinn, CCDCOE, 2022.

[18] NATO: *Fact Sheet – NATO Cyber Defence*. (2021. április 28.).

úgynevezett „spill over" hatás, ami nagyon leegyszerűsítve azt az elvet írja le, egy valamilyen szakpolitikára vonatkozó szabályozás gyakran más szakterületekre is „tovább gyűrűzik". Esetünkben ez azért fontos, mert a kiberbiztonság egy rendkívül összetett szakterület, ami – ahogy a Nemzeti Kiberbiztonsági Stratégia is megfogalmazza-, *„kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez*". E fogalomból következik, hogy az Európai Unió számos területen igyekszik normatív szabályokat alkotni.

Az Európai Unió már az 1990-es évek közepén felismerte, hogy az elektronikus információs rendszereinek védelme fontos feladat (elsősorban a telekommunikációs rendszerek és a személyes adatok védelme aspektusából),[19] de stratégiai szinten először 2006-ban jelent meg hivatalos dokumentum a kiberbiztonsággal kapcsolatban Biztonságos információs társadalom elnevezéssel.[20]

A 2007-ben Észtország kormányzati és pénzügyi kritikus infrastruktúráit ért túlterheléses támadások nem csupán a NATO esetében volt fontos jelzés a terület mielőbb szabályozása oán, hanem az Európai Uniónak is. A 2008-ban kitört gazdasági és pénzügyi válság, a kibertérből származó fenyegetéseknek, különösen a kiberbűnözés nagy arányú növekedése az EU döntéshozói számára is világossá tette, hogy a kibertérből származó új típusú kihívásokra erőteljes választ kell adni. Az azóta eltelt időszakban az EU számos különböző stratégiai dokumentumot fogadott el, amelyek részletes bemutatását e fejezet terjedelmi keretei nem teszik lehetővé, csupán a meghatározóbb történeti előzmények felvillantására nyílik alkalmunk. Ez a megkötés ugyanúgy érvényes a jelenleg elfogadás alatt álló stratégiákra is, ugyanis az említett komplexitásból fakadóan meglátásunk szerint nem értelmezhető önmagában a „kiberbiztonság", csak ökoszisztémában rendezve.

A történeti áttekintés alapján az első említendő dokumentum az Európa 2020 foglalkoztatási és növekedési stratégia,[21] amely a 2020-ig tartó időszak intézkedéseinek alapdokumentumának tekinthető. Ennek keretében az Európai Bizottság hét kiemelt szabályozási területet azonosított, aminek a megvalósítása érdekében elkészítette az Európai Digitális Menetrend 2014–2020 stratégiáját.[22] Az Európai Digitális Menetrend többek között az alábbi megvalósulását tűzte ki:

- *„az egységes digitális piac megteremtése,*

[19] Helena Carrapico – Andre Barrinha: European Union cyber security as an emerging research and policy field. *European Politics and Society,* 2018/3. szám, 299–303. o.

[20] E dokumentum előzményeként meg kell említenünk a Hálózat- és információbiztonság: európai politikai megközelítésre irányuló javaslatot (COM(2001) 2001-ből.

[21] Európa 2020- Az intelligens, fenntartható és inkluzív növekedés stratégiája.

[22] Európai Digitális Menetrend 2010-2020: A Bizottság akcióterve az európai jólét fellendítésére.

- *az uniós adatvédelmi szabályozási keret felülvizsgálata,*
- *a távközlési szolgáltatások egységesítése,*
- *a fokozott interoperabilitás és szabványok"*[23]

Következő lépésként az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága által 2013-ban megalkotott az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér című uniós stratégiáját nevesíthetjük. A stratégia hat stratégiai prioritást és intézkedést fogalmazott meg.[24]

2018. május 25-étől az Európai Unió tagállamaiban egységesen az Európai Általános Adatvédelmi Rendelet lépett hatályba,[25] és a GDPR rendelkezéseit kell alkalmazni tagállamokban korábban hatályos adatvédelmi szabályok helyett. A Rendelet alapjául az Európai Parlament és a Tanács 95/46/EK irányelve szolgált.[26] Bár az irányelv rögzítette a személyes adatok kezelésének elveit, azonban nem határozta meg az adatvédelmi incidensek megsértésének következményeit. Az új adatvédelmi rendelet egyrészt az a hiátust pótolja, másrészt egységes követelményrendszert fogalmaz meg a személyes adatok kezelését illetően az Európai Unió minden tagállamában, továbbá korszerű választ kíván adni a technológiai fejlődésből következő kockázatokra, hogy ennek segítségével növekedjen a felhasználók új technológiákba vetett hite, és ezáltal növekedhessen a Digitális Menetrendben megfogalmazott európai digitális tér.

A GDPR mellett fontos változást jelentett a szintén 2018 májusától érvényes hálózati és információs rendszerek biztonságáról szóló irányelv (Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, továbbiakban NIS irányelv).[27] A NIS irányelv megalkotásának előzményei az európai stratégiai fejlődésre vezethetőek vissza. Az irányelv célja, hogy az EU tagállamai képesek legyenek a kibertér jelentette fenyegetések ellen hatékonyan védekezni, ily módon pedig létrejöjjön egy egységes hálózati- és információs rendszerek biztonságára vonatkozó, általános uniós szint.

---

[23] A témáról bővebben ld: Munk Sándor: Kiberbiztonsági célok, jövőképek, szabályozók az EU-ban és kapcsolatrendszerük az interperabilitással. *Hadmérnök,* 2018/KÖFOP szám, 205–217. o.

[24] Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér", text/html; charset=UTF-8 (OPOCE).

[25] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT vonatkozású szöveg).

[26] Az Európai Parlament és a Tanács a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelve.

[27] Az Európai Parlament és a Tanács a hálózati és információs rendszereknek az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148 irányelve.

Mivel irányelvként fogadták el a jogszabályt, így a tagállami jogalkotók maguk határozhatják meg, hogy milyen módon implementálják az irányelvben megfogalmazottakat a tagállami joganyagokba. 2022 májusában a Tanács és az Európai Parlament végül elfogadta a NIS2 irányelvet,[28] ami a 2018-ban hatályba lépett irányelv újragondolása. A felülvizsgálat célja az volt, hogy A módosított irányelv célja, hogy *„megszüntesse azokat az eltéréseket, amelyek jelenleg a különböző tagállamokban mutatkoznak a kiberbiztonsági követelmények és a kiberbiztonsági intézkedések végrehajtása terén. Ennek érdekében minimumszabályokat állapít meg a szabályozási keretre vonatkozóan, és mechanizmusokat határoz meg az egyes tagállamok illetékes hatóságai közötti hatékony együttműködéshez. Aktualizálja a kiberbiztonsági kötelezettségek hatálya alá tartozó ágazatok és tevékenységek listáját, és a végrehajtás biztosítása érdekében jogorvoslatokról és szankciókról rendelkezik*."

2019 áprilisában a Tanács elfogadta a Kiberbiztonsági jogszabályt, ami bevezeti az egész Unió területén érvényes egységes kiberbiztonsági tanúsítási rendszerek keretét, illetve létrehozza az Európai Hálózat- és Információbiztonsági Ügynökség feladatainak átvételére az az Európai Uniós Kiberbiztonsági Ügynökséget. A tanúsítási keretrendszer a tervek szerint növelni fogja a bizalmat, fokozza a kiberbiztonsági piac növekedését, valamint megkönnyíti e termékek EU-n belüli kereskedelmét.[29]

2020 februárjában kezdődött meg az Európai Unió digitális jövőjének megtervezése, amely ötéves intervallumban három fő célitűzést fogalmazott meg:

- az emberek szolgálatában álló technológia;
- a méltányos és versenyképes gazdaság; valamint
- a nyílt, demokratikus és fenntartható társadalom.

E jövőkép pilléreiként az európai adatstratégiát, a kommunikációt biztosító keretrendszert, valamint a mesterséges intelligencia használatára vonatkozó fehér könyvet azonosították. A 2019. végén kitört új típusú koronavírus járvány (továbbiakban COVID-19) miatt újratervezés vált szükségessé, ami a NextGeneration EU formájában valósult meg a Bizottság 2020 májusi előterjesztése alapján[30]. A koncepció célja, hogy a COVID-19 okozta társadalmi és gazdasági nehézségeket követően a helyreállítás valamennyi tagállam számára fenntartható, méltányos, inkluzív és egyenletes legyen. Mindennek egyik eszközeként a digitalizáció erősítését nevesítették, ide értve:

- az 5G hálózatok gyors kiépítését;
- az ipari és technológiai jelenlét fokozását a stratégiai ágazatokban (nevesítve a mesterséges intelligenciát, a kvantum számítástechnikát, illetve a felhőalapú számítástechnikát);

[28] A kiberbiztonság és -reziliencia megerősítése az EU egész területén – Ideiglenes megállapodás a Tanács és az Európai Parlament között.

[29] The EU Cybersecurity Certification Framework | Shaping Europe's Digital Future.

[30] Bővebben ld: Európai helyreállítási terv, Text, Európai Bizottság – European Commission.

- az innováció és a munkahelyteremtés motorjaként szolgáló valódi adatgazdaság kiépítése, illetve a kiberrezilencia növelését.

2020. szeptemberében hirdette meg a Bizottság az EU Digitális évtizedét. A megfogalmazott ajánlásokban tovább erősödött az 5G hálózatok mielőbbi kiépítésének (kiemelve a hálózatok biztonságának és ellenállóképességének növelését, illetve az Európai Unió Kiberbiztonsági Ügynökségével együttműködve erre vonatkozó stratégia megalkotását), a kvantumszámítástechnika területén történő fejlesztések szükségessége.[31]

Szintén szeptemberben nyújtotta be a Bizottság a Digitális pénzügyi csomag javaslatát, amelynek két javaslatát végül a Tanács 2021. novemberében fogadta el. E két javaslat a kriptoeszközök piacairól szóló rendeletjavaslat (MiCA-rendelet), valamint a digitális működési rezilienciáról szóló rendeletjavaslat (DORA-rendelet). A MiCA-rendelet célja, hogy olyan szabályozási keretet hozzon létre a kriptoeszközök piaca számára, amely támogatja az innovációt és kiaknázza a kriptoeszközökben rejlő lehetőségeket, ugyanakkor biztosítja a pénzügyi stabilitás és a befektetők védelmét. A DORA-rendelet célja a digitális működési rezilienciára vonatkozó, olyan szabályozási keret létrehozása, amelynek értelmében valamennyi vállalkozás gondoskodik arról, hogy a kiberfenyegetések megelőzése és enyhítése érdekében ki tudja védeni az IKT-vonatkozású zavarokat és fenyegetéseket.[32]

2020 decembere különösen jelentős volt az Európai Unió stratégiaalkotásában. A Tanács következtetést fogadott el a csatlakoztatott eszközök kiberbiztonságáról, amely a dolgok internetéhez (IoT) kapcsolódó legmagasabb szintű reziliencia megteremtését fogalmazta meg annak céljából, hogy előrelendítse az EU IoT ágazatának globális versenyképességét.[33]

Szintén említendő a Tanács által e hónapban közzétett állásfoglalása a titkosítással kapcsolatban. Az állásfoglalás nagy vitát generált a szakemberek között, ugyanis bár kimondja, hogy a titkosítással védeni kell a kommunikáció biztonságát, ennek ellenére garantálni szükséges a biztonságot is, amely a bűnüldöző és igazságügyi hatóságok részére biztosítaná, hogy az online és offline térben gyakorolni tudják jogszerű hatásköreiket.[34]

---

[31] A Tanács végül 2021. júliusában fogadta el az európai nagy teljesítményű számítástechnikával foglalkozó közös vállalkozás (EuroHPC közös vállalkozás) létrehozásáról szóló rendeletet. Bővebben ld: Európai nagy teljesítményű számítástechnikával foglalkozó közös vállalkozás: a Tanács rendeletet fogadott el.

[32] Digitális pénzügyi csomag: a Tanács megállapodásra jutott a MiCA- és a DORA-rendeletről (https://www.consilium.europa.eu/hu/press/press-releases/2021/11/24/digital-finance-package-council-reaches-agreement-on-mica-and-dora/).

[33] A Tanács következtetéseket fogadott el a csatlakoztatott eszközök kiberbiztonságáról (https://www.consilium.europa.eu/hu/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/).

[34] Titkosítás: a Tanács állásfoglalást fogadott el (https://www.consilium.europa.eu/hu/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/).

December 15-én terjesztette be a Bizottság az egyik legjelentősebb reformcsomagját a digitális tér átfogó megújítására vonatkozóan. E csomag két jelentős jogszabályt tartalmazott, a Digitális Szolgáltatásokról szóló (Digital Service Act, DSA), illetve a Digitális Piacról szóló Jogszabályt (Digital Market Act, DMA). A DSA célja, hogy az európai értékekkel összhangban védje a felhasználókat és azok jogait az online térben, ami alapján szilárd keretet alakít ki az online platformok átláthatóságának és elszámoltathatóságának biztosítása érdekében. A digitális szolgáltatásokról szóló jogszabály értelmében uniós szintű, kötelező érvényű kötelezettségek vonatkoznak majd minden olyan digitális szolgáltatásra, amelyek árukat, szolgáltatásokat vagy tartalmakat közvetítenek a fogyasztóknak. A jogszabály többek között olyan új eljárások bevezetését javasolja, amelyeknek alapvető célja az illegális tartalmak eltávolításának felgyorsítása az online platformokról, továbbá a felhasználók alapvető online jogai általános védelmének fokozása.[35] A DMA célja, hogy a nagy technológiai cégek (az EU terminológiájában digitális kapuőrök) működését szigorúbb jogi keretek szabályozzák.[36] A jogszabály várhatóan 2023 tavaszán lép hatályba.

E két jogszabály mellett a Tanács következtetéseket is elfogadott reziliencia erősítésére, a hibrid fenyegettetésekkel szembeni ellenállóképesség növelésére, kiemelten kezelve a dezinformációt, ami a COVID-19 járvány következtében különösen relevánssá vált.[37] A globális dezinformációs kampányok mögött gyakran az Európai Unió stratégiai ellenfelei állnak azzal a céllal, hogy ily módon csökkentsék a demokratikus intézményekbe, a tudományba vetett bizalmat, illetve dezintegrálják az Uniót, megosszák az egyes tagállamokat. Ezek a tendenciák a 2022. február 24-én kitört ukrán-orosz háborút megelőzően, és azt követően, különösen a szankciók bevezetése okán még intenzívebbé váltak.

Egy nappal később a Bizottság a csomag részeként az Unió új kiberbiztonsági stratégiáját is benyújtotta. A stratégia célja kiberfenyegetésekkel szembeni rezilienciája, valamint hogy minden polgár és vállalkozás megbízható szolgáltatásokat és digitális eszközöket vehessen igénybe, és ezek előnyeit teljes mértékben ki tudja használni. Végül a 2021. március 22-én következtetéseket fogadott el a Tanács a kiberbiztonsági stratégiáról, amelyekben hangsúlyozta, hogy a kiberbiztonság

[35] A jogszabályt 2022 júliusában fogadta el az Európai Parlament, jelenleg a Tanács jóváhagyása szükséges a hatályba lépéshez. Bővebben ld: A digitális szolgáltatásokról szóló jogszabálycsomag", Text, European Commission - European Commission, elérés (https://ec.europa.eu/commission/presscorner/detail/hu/IP_22_4313).

[36] A jogszabályról bővebben lásd: A digitális piacokról szóló jogszabály: tisztességes és nyitott digitális piacok biztosítása, Text, European Commission – European Commission, (https://ec.europa.eu/commission/presscorner/detail/hu/qanda_20_2349).

[37] A Tanács a reziliencia megerősítésére és a hibrid fenyegetések, többek között a dezinformáció elleni küzdelemre szólított fel (https://www.consilium.europa.eu/hu/press/press-releases/2020/12/15/council-calls-for-strengthening-resilience-and-countering-hybrid-threats-including-disinformation-in-the-context-of-the-covid-19-pandemic/).

alapvető fontosságú ahhoz, hogy reziliens, zöld és digitális Európát építésében.[38] A Digitális Évtized új kiberbiztonsági stratégiája nagyban támaszkodik a fejezetben említett, a kiberbiztonságra vonatkozó ellenállóképesség erősítését szorgalmazó dokumentumokra, illetve a biztonsági unióra vonatkozó stratégiára. A stratégia három az alábbi területeken fogalmaz meg konkrét intézkedési javaslatokat:

- reziliencia, technológiai szuverenitás és vezető szerep;
- operatív kapacitás kiépítése: a megelőzés, elrettentés és reagálás elősegítése;
- a globális és nyitott kibertér kiépülésének és működésének támogatása.

A Tanács által elfogadott következtetések az új kiberbiztonsági stratégia kapcsán az alábbi intézkedési területeket jelölte meg:

- kiberbiztonsági műveleti központok hálózatának kiépítése a hálózatok monitorozására, és a támadások korai előrejelzésére;
- közös uniós kiberbiztonsági egység létrehozása, a kiberbiztonsági válsághelyzetek hatékony kezelésére;
- közös uniós 5G eszközkészlet kialakítása, az 5G hálózatok kiberbiztonsági védelmének biztosítására;
- közös uniós internet biztonsági szabványok bevezetése, mivel ezek kulcsfontosságúak a kibertér biztonságának elősegítésében, miközben a globális internetes hálózatok nyitottságát is szolgálják
- az erős titkosítás eljárásai kifejlesztésének támogatása az alapvető állampolgári jogok és a digitális biztonság megőrzésére
- az EU kiberdiplomáciai eszközkészletének továbbfejlesztése, a kibertámadások megelőzésének és elhárításának elősegítésére
- egy közös uniós kiberhírszerzési munkacsoport felállítása az EU általános célú hírszerző szervezetének (EU INTCENT) megerősítésére
- multilaterális együttműködések erősítése a kiberbiztonság és kibervédelem területén
- az Unió kiberbiztonsági kapacitás-építő tevékenységének kiterjesztése az EU-n kívüli területekre annak érdekében, hogy a kibertámadásokkal szembeni ellenálló képesség világszerte növekedhessen.

Fentiekhez igazodik a Bizottság 2021 márciusi előterjesztése, a 2030-as időszakig vonatkozó Digitális iránytű: A digitális évtized európai útja nevet viselő dokumentum, ami digitálisan képzett lakosság és magasan képzett digitális szakemberek, biztonságos, jól teljesítő és fenntartható digitális infrastruktúrák, a vállalkozások digitális átalakulása és a

[38] Kiberbiztonság: a Tanács következtetéseket fogadott el az uniós kiberbiztonsági stratégiáról (https://www.consilium.europa.eu/hu/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/).

közszolgáltatások digitalizálását tűzte ki céljául.

Említeni szükséges a stratégiai fejlődés tekintetében a Mesterséges Intelligencia- rendszerek fejlesztés és alkalmazása az Európai Unióban nevet viselő tervezetet, aminek elsődleges célja, hogy megóvja az Európai Uniót egy MI alapú disztópikus rendszer kialakulásától. A szabályozással egy, a kínai szociális kreditrendszerhez hasonló, totális megfigyelő állam kialakulásának lehetőségét szeretnék elérni. Az ily módon kialakítandó keretrendszer a MI-rendszerek fejlesztését és alkalmazását kockázatelemzéshez kötné, amelyben elfogadhatatlan-, magas-, korlátozott-, illetve minimális kockázatot jelentő kategóriák mentén szabályozná a kérdéskört.

A bemutatott stratégiák mellett említeni szükséges Európai Kiberbiztonsági Kutatási és Kompetenciaközpont létrehozásával kapcsolatos szakpolitikai fejlődést. A szervezet megalakítását 2020 decemberében jelentették be bukaresti székhellyel. A Központ feladata, hogy javítsa a kiberbiztonsági kutatások és innováció koordinációját az EU-ban.[39]

Ahogy a COVID-19 járvány, úgy az említett ukrán-orosz háború kitörése is új szabályozási környezet kialakításának igényét hozta el. 2022 márciusában uniós tagállamok távközlésért és digitális ügyekért felelős miniszterei a kiberbiztonság területén folytatott európai együttműködés megerősítésére és ütemének felgyorsítására szólítottak fel a szomszédban zajló háború okán. [40]

Májusban a Tanács további három évvel hosszabbította meg az Uniót és annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedések keretének érvényességét.[41] A bevezethető szankciók előzménye a 2017-ben megalkotott Kiberdiplomáciai eszköztár a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretét határozza meg. Néhány nappal később a Tanács következtetéseket fogadott el, a kiber reziliencia erősítésére vonatkozóan.[42]

A háború okán júniusban a hibrid hadjáratokra való koordinált uniós reagálásra vonatkozó keretre vonatkozó következtetéseket fogadott el a Tanács,[43]

[39] A Tanács zöld utat adott a bukaresti székhelyű Kiberbiztonsági Kompetenciaközpont létrehozásának, (https://www.consilium.europa.eu/hu/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/).

[40] Member States United in Supporting Ukraine and Strengthening the EU's Telecommunications and Cybersecurity Resilience – French Presidency of the Council of the European Union 2022, French Presidency of the Council of the European Union, (http://presidence-francaise.consilium.europa.eu/en/news/member-states-united-in-supporting-ukraine-and-strengthening-the-eu-s-telecommunications-and-cybersecurity-resilience/).

[41] Kibertámadások: a Tanács 2025. május 18-ig meghosszabbította a szankciórendszer érvényességét (https://www.consilium.europa.eu/hu/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/).

[42] Cyber posture: Council approves conclusions (https://www.consilium.europa.eu/hu/press/press-releases/2022/05/23/cyber-posture-council-approves-conclusions/).

[43] Council conclusions on a Framework for a coordinated EU response to hybrid campaigns (https://www.consilium.europa.eu/hu/press/press-

amiben ismételten hangsúlyozta, hogy bár a tagállamok felelőssége a hibrid fenyegetésekre való reagálás, azonban a koordinált Uniós fellépéseknek az alábbi keretek mentén szükséges megvalósulni:

- a demokrácia és a nemzetközi jog védelmét kell szolgálniuk;
- az Unió célkitűzéseinek elérését kell szolgálniuk;
- arányosnak kell lenniük az egyes hadjáratokkal;
- helyzetismereten kell alapulniuk;
- figyelembe kell venniük a tágabb összefüggéseket;
- tiszteletben kell tartaniuk a nemzetközi jogot, valamint védeniük kell az alapvető jogokat és szabadságokat.

Érdemes visszatekinteni e Tanács által kiadott következtetésnél az alfejezet elején említett „spill over" hatás kapcsán megfogalmazottakra: a korszellem bármikor kiterjesztheti az Európai Unió normatív szabályzóinak hatáskörét, ami a kiberbiztonság területén számos kapcsolódó terület egységes szabályzását fogja indukálni.

A globális ellátási láncok kitettségét már a COVID-19 járvány is hangsúlyossá tette, a háború ezt még inkább felerősítette. Tekintettel az uniós információs és kommunikációs technológiai (IKT) ellátási láncok biztonságára, 2022 októberében a Tanács következtetéseket fogadott el, amelyben az IKT ellátási láncok megerősítését szorgalmazta.[44]

2022 novemberében az Európai Parlament új kiberbiztonságra vonatkozó jogszabályt fogadott el,[45] amelynek célja szigorúbb követelmények támasztása a vállalatokkal, a közigazgatással és az infrastruktúrákkal szemben. A jogszabály megfogalmazza, hogy a tagállamoknak egységes szinten szükséges szabályozni a kibervédelmi képességeiket, intézkedéseiket, ugyanis az eltérőség csökkenti az Európai Unió egységes felkészültségét. Ezzel párhuzamosan az Európai Bizottság előterjesztette az uniós kibervédelmi politikáról szóló közös közleményt és a katonai mobilitásról szóló cselekvési terv új verzióját,[46] amelyek célja az Ukrajna elleni orosz agresszió következtében egyre romló biztonsági környezet kezelése, valamint a polgárok és az infrastruktúra védelmét célzó uniós képességek javítása. A koncepció négy pillérre támaszkodik:

- együttes fellépést szorgalmaz az erősebb kibervédelmi képességek kialakítására vonatkozóan;
- garantálni szükséges az uniós védelmi ökoszisztéma biztonságát;

releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/).

[44] A Tanács megállapodott az IKT-ellátási láncok biztonságának megerősítéséről (https://www.consilium.europa.eu/hu/press/press-releases/2022/10/17/the-council-agrees-to-strengthen-the-security-of-ict-supply-chains/).

[45] Európa kiberbiztonságának megerősítése: új jogszabályt fogadott el az EP | Hírek | Európai Parlament (https://www.europarl.europa.eu/news/hu/press-room/20221107IPR49608/europa-kiberbiztonsaganak-megerositese-uj-jogszabalyt-fogadott-el-az-ep).

[46] Kibervédelem: az EU erőteljesebben lép fel a kiberfenyegetésekkel szemben, Text, European Commission – European Commission (https://ec.europa.eu/commission/presscorner/detail/hu/ip_22_6642).

- a kibervédelmi képességekbe való beruházás, illetve;

a közös kihívások kezelésében való szorosabb együttműködés.

FELHASZNÁLT FORRÁSOK

[1] Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése*. Budapest, Nemzeti Közszolgálati Egyetem, 2018.
[2] 1163/2020. (IV. 21.) Korm. Határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
[3] Kovács László: *Kiberbiztonság és -stratégia*. Budapest, Dialóg Campus, 2018.
[4] Bányász Péter – Krasznay Csaba – Tóth András: A NATO kibervédelmi szakpolitikája. In: Szenes Zoltán (szerk.): *A mai NATO : A szövetség helyzete és feladatai.* Budapest, HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft., 2021, 130–149. o.
[5] Szentgáli Gergely: A NATO kibervédelmi politikájának fejlődése. *Bolyai Szemle,* 2012/2. szám, 80–85. o.
[6] Bányász Péter – Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. *Hadtudomány,* 2013/elektronikus szám, 188–209. o.
[7] NATO: *Defending the networks*. (2011. augusztus 19.).
[8] NATO: *Chicago Summit Declaration.* (2022. július 05.).
[9] NATO: *Wales Summit Declaration*. (2022. július 04.).
[10] Bányász Péter: *A közösségi média lehetőségei és kihívásai a védelmi szférában*. Doktori (PhD) értekezés, Budapest, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola 2018.
[11] Paráda István: A NATO kibervédelmi irányelveinek fejlődése. *Honvédségi Szemle*, 2018/3. szám. 3–13. o.
[12] Berki Gábor: *Kiberháborúk, kiberkonfliktusok. Műhelymunkák*. Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016, 245–284. o.
[13] Mitko Bogdanoski: Building Cyber Resilience against Hybrid Threats. *NATO Science for Peace and Security Series - D: Information and Communication Security*, 2022.
[14] NATO: *London Declaration*. (2022. július 01.).
[15] Dragoș-Mihai Păunescu: NATO's encounters in the cyber domain. *Proceedings of the 17th International Scientific Conference "Strategies XXI" - Strategic Changes in Security and International Relations*, 2021/1. szám.
[16] Piret Pernik (szerk.): *Cyberspace Strategic Outlook 2030*. Tallinn, CCDCOE, 2022.
[17] NATO: *Fact Sheet – NATO Cyber Defence*. (2021. április 28.).
[18] Helena Carrapico – Andre Barrinha: European Union cyber security as an emerging research and policy field. *European Politics and Society,* 2018/3. szám, 299–303. o.

[19] Európa 2020- Az intelligens, fenntartható és inkluzív növekedés stratégiája.
[20] Európai Digitális Menetrend 2010-2020: A Bizottság akcióterve az európai jólét fellendítésére.
[21] Munk Sándor: Kiberbiztonsági célok, jövőképek, szabályozók az EU-ban és kapcsolatrendszerük az interperabilitással. *Hadmérnök,* 2018/KÖFOP szám, 205–217. o.
[22] Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér", text/html; charset=UTF-8 (OPOCE).
[23] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT vonatkozású szöveg).
[24] Az Európai Parlament és a Tanács a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelve.
[25] Az Európai Parlament és a Tanács a hálózati és információs rendszereknek az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148 irányelve.
[26] A kiberbiztonság és -reziliencia megerősítése az EU egész területén – Ideiglenes megállapodás a Tanács és az Európai Parlament között.
[27] The EU Cybersecurity Certification Framework | Shaping Europe's Digital Future.
[28] A Tanács végül 2021. júliusában fogadta el az európai nagy teljesítményű számítástechnikával foglalkozó közös vállalkozás (EuroHPC közös vállalkozás) létrehozásáról szóló rendeletet. Bővebben ld: Európai nagy teljesítményű számítástechnikával foglalkozó közös vállalkozás: a Tanács rendeletet fogadott el.
[29] Digitális pénzügyi csomag: a Tanács megállapodásra jutott a MiCA- és a DORA-rendeletről (https://www.consilium.europa.eu/hu/press/press-releases/2021/11/24/digital-finance-package-council-reaches-agreement-on-mica-and-dora/).
[30] A Tanács következtetéseket fogadott el a csatlakoztatott eszközök kiberbiztonságáról (https://www.consilium.europa.eu/hu/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/).
[31] Titkosítás: a Tanács állásfoglalást fogadott el (https://www.consilium.europa.eu/hu/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/).

[32] A digitális szolgáltatásokról szóló jogszabálycsomag", Text, European Commission - European Commission, elérés (https://ec.europa.eu/commission/presscorner/detail/hu/IP_22_4313).
[33] A digitális piacokról szóló jogszabály: tisztességes és nyitott digitális piacok biztosítása, Text, European Commission – European Commission, (https://ec.europa.eu/commission/presscorner/detail/hu/qanda_20_2349).
[34] A Tanács a reziliencia megerősítésére és a hibrid fenyegetések, többek között a dezinformáció elleni küzdelemre szólított fel (https://www.consilium.europa.eu/hu/press/press-releases/2020/12/15/council-calls-for-strengthening-resilience-and-countering-hybrid-threats-including-disinformation-in-the-context-of-the-covid-19-pandemic/).
[35] Kiberbiztonság: a Tanács következtetéseket fogadott el az uniós kiberbiztonsági stratégiáról (https://www.consilium.europa.eu/hu/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/).
[36] A Tanács zöld utat adott a bukaresti székhelyű Kiberbiztonsági Kompetenciaközpont létrehozásának, (https://www.consilium.europa.eu/hu/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/).
[37] Member States United in Supporting Ukraine and Strengthening the EU's Telecommunications and Cybersecurity Resilience – French Presidency of the Council of the European Union 2022, French Presidency of the Council of the European Union, (http://presidence-francaise.consilium.europa.eu/en/news/member-states-united-in-supporting-ukraine-and-strengthening-the-eu-s-telecommunications-and-cybersecurity-resilience/).
[38] Kibertámadások: a Tanács 2025. május 18-ig meghosszabbította a szankciórendszer érvényességét (https://www.consilium.europa.eu/hu/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/).
[39] Cyber posture: Council approves conclusions (https://www.consilium.europa.eu/hu/press/press-releases/2022/05/23/cyber-posture-council-approves-conclusions/).
[40] Council conclusions on a Framework for a coordinated EU response to hybrid campaigns (https://www.consilium.europa.eu/hu/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/).
[41] A Tanács megállapodott az IKT-ellátási láncok biztonságának megerősítéséről (https://www.consilium.europa.eu/h

u/press/press-releases/2022/10/17/the-council-agrees-to-strengthen-the-security-of-ict-supply-chains/).

[42] Európa kiberbiztonságának megerősítése: új jogszabályt fogadott el az EP | Hírek | Európai Parlament (https://www.europarl.europa.eu/news/hu/press-room/20221107IPR49608/europa-kiberbiztonsaganak-megerositese-uj-jogszabalyt-fogadott-el-az-ep).

[43] Kibervédelem: az EU erőteljesebben lép fel a kiberfenyegetésekkel szemben, Text, European Commission – European Commission (https://ec.europa.eu/commission/presscorner/detail/hu/ip_22_6642).


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

Military and Intelligence CyberSecurity Research Paper 2022/8.

Szerző(k) / Author(s):
Dr. Bányász Péter PhD – Dr. Krasznay Csaba PhD – Dr. Tóth András PhD

Kézirat lezárásának ideje / Manuscript closing time:
2022.11.15.

Szerkesztők / Editors:
Dr. Farkas Ádám PhD
Dr. Magyar Sánor PhD

Kiadó / Publisher:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:
Prof. Dr. Resperger István PhD

Elérhetőségek /Contacts:
https://hhk.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/research-paper

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. /9-11. Hungária Blvd., Budapest, H1011

ISSN:
2786-3778

A borító https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.

The cover was created on 25. February 2021, using a free wallpaper available at https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROGRAM