Kovács László✧, Krasznay Csaba❖

# Digitális Mohács 3.0*

DOI 10.17047/HADTUD.2024.34.3.40

Mennyire kitett Magyarország egy kibertéri műveletnek? Vajon egy másik nemzetállam békeidőben is indíthat ilyen műveletet Magyarország ellen? Ezek a kérdések jól mutatják a kiberbiztonsági kihívások fokozódását, melyekre a szakértőknek a nyilvánosság előtt is válaszokat kell adniuk. Nem véletlen, hogy ezek a kérdések felmerülnek, hiszen évtizedek óta tapasztaljuk, hogy társadalmunk és gazdaságunk egyre jobban függ a digitális ökoszisztémától, miközben a nagyhatalmi vetélkedés egyik fókuszpontja épp az információs infrastruktúrán van. A 2020-as években a mesterséges intelligencia és a digitális ökoszisztéma gyors fejlődése, valamint a biztonságpolitikai kihívások (például orosz–ukrán háború) alapvetően alakították át a kiberbiztonság helyzetét. Néhány évvel a szerzők *Digitális Mohács* címmel megjelent kétrészes tanulmánya után ez a dolgozat a hazai kiberbiztonság főbb területeit és stratégiai fenyegetéseit elemzi, javaslatokat téve a kritikus infrastruktúrák védelmére és a nemzeti kiberstratégia megerősítésére.

KULCSSZAVAK: kiberbiztonság, Digitális Mohács, kibertér,
kritikus információs infrastruktúrák

## *Digital Mohács 3.0*

*How exposed is Hungary to a cyberspace operation? Is it even conceivable that Hungary could be attacked by another nation state through cyberspace in peacetime? These are just two of a huge range of questions that regularly emerge among representatives of Hungarian cybersecurity, and which increasingly need to be answered in public. It is no coincidence that such questions are being raised, as for decades we have been experiencing that our society and economy are increasingly dependent on the digital ecosystem, while one of the main focal points of the great-power competition is exactly on the information infrastructure. And in the*

✧ Nemzeti Közszolgálati Egyetem, egyetemi tanár –
*Ludovika University of Public Service, Ludovika University of Public Service, professor;*
e-mail: kovacs.laszlo@uni-nke.hu; https://orcid.org/0000-0002-6403-0650

❖ Nemzeti Közszolgálati Egyetem, egyetemi docens –
*Ludovika University of Public Service, associate professor,*
e-mail: krasznay.csaba@uni-nke.hu; https://orcid.org/0000-0003-3216-2592

* A publikáció a Kulturális és Innovációs Minisztérium ÚNKP-23-5-NKE-129 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült. Kézirat lezárva 2024. augusztus 23.

*third decade of the century, revolutionary changes took place that, while not without portents for experts, have the power of novelty for the general public. Disruptive technologies such as artificial intelligence, security challenges that are reshaping the international order, such as the Russia-Ukraine war or the tension between the US and China, or the widespread digital inclusion caused by the COVID-19 pandemic, which has brought digitalisation at a breakneck speed to a wide range of societies and businesses are worth mentioning here. A few years after the authors' two-part study entitled Digital Mohács, this paper focuses on the domestic cybersecurity situation, analysing the most important cyberspace areas.*

*KEYWORDS: cybersecurity, Digital Mohács, cyberspace, critical information infrastructures*

***Bevezetés***

Annak ellenére, hogy napjainkra a kibertéri kihívások kézzel foghatók, a kiberbiztonsági incidensek hatásait pedig rendszeresen érzékeljük, a Magyarországot érintő kibertéri kitettséggel kapcsolatban nagyon kevés objektív adatunk van. A legalaposabb áttekintést Legárd Ildikó[1] publikációja tartalmazza, melyben a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) adatai alapján mutatja be a 2020-as évek incidenseinek trendjeit, de konkrét számadatok ebben nem szerepelnek. A szerző ezt ezzel indokolja: „Az NKI az incidensekre vonatkozó átadott adatokat számszerűen – hónaponként, szektoronként és incidenstípusonként – bocsátotta a rendelkezésemre. Tekintettel arra, hogy az Ibtv. 22. § (4) bekezdése szerint az NBSZ NKI eljárásai során keletkezett adatok nem nyilvánosak, továbbá a konkrét számadatok tükrében olyan – a kapacitásaikra és képességeikre vonatkozó – következtetések is levonhatók, amelyek megnehezíthetnék a szolgáltatások ellátását, a konkrét számadatok nem publikálhatók. Az adatok feldolgozása során kizárólag a számadatokból levont következtetéseket, a számadatokban való változás százalékos mértékét vagy egymáshoz viszonyított arányát lehet bemutatni."

További igazodási pontot jelenthet a Nemzeti Adatvédelmi és Információszabadság Hatóság éves jelentése,[2] melyben a GDPR szerinti adatvédelmi incidensek számát publikálják, hiszen az adatvédelmi incidensek nagy valószínűséggel kiberbiztonsági incidensre is visszavezethetők. A 2023-as évben a közlés szerint 533 új incidensbejelentés érkezett, mely kevesebb, mint a korábbi években. Szintén hasznos kiindulópontot jelent a Magyar Nemzeti Bank által publikált A *magyar pénzügyi szektor kiberfenyegetettségi térképe 2022*[3] című kiadvány. Ebben az MNB 2022. február–július közötti incidens-statisztikája olvasható, mely a magyar pénzintézetektől érkező jelentések objektív lenyomatát tartalmazza. Eszerint a féléves időszakban összesen 765 incidenst jelentettek ebből a szektorból. Valószínűleg a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézetéhez beérkező incidensbejelentések száma is korrelál ehhez a nagyságrendhez, azaz Magyarországon az egy évben bekövetkező, jelentésköteles incidensek száma néhány ezres nagyságrendű lehet.

A különböző nemzetközi elemzések alapján is arra a következtetésre juthatunk, hogy a magyar kibertér viszonylag békés része a globális hálózatnak. A teljesség

1 Legárd 2023.

2 NAIH 2024.

3 MNB 2022.

igénye nélkül csak néhány példa, amely alátámasztja ezt a megállapítást. Az Oxford University kutatóinak vezetésével, több más egyetem együttműködésével készült el a World Cybercrime Index[4] jelentés, mely azt a célt tűzte ki, hogy szakértői interjúk segítségével mutassa be, mely országok a legfőbb forrásai a kiberbűnözésnek. Magyarország ezen a listán a 81. helyen szerepel, közvetlenül Egyenlítői-Guinea mögött, ami azt jelenti, hogy a nemzetközi szakértők szerint gyakorlatilag nem létezik magyar forrású kiberbűnözés. A Rendőrség híradásait böngészve is az a benyomása támadhat az embernek, hogy a magyar kibercsalások jelentős részéért oroszországi és ukrajnai illetőségű bűnbandák felelősek, a magyar állampolgároknak ebben csak epizódszerep jut. A magyar Bűnügyi Statisztikai Rendszer[5] adatai alapján ugyan nyomon követhető, hogy a csalások, ezen belül is az online csalások száma folyamatosan emelkedik (2022-ben az esetszám 16 747; 2023-ban 19 704, 2024 első félévében 10 239), de ez még mindig nem számít kiugrónak a régióban. Kim-McLeod[6] kutatásában azt vizsgálta, hogy az orosz–ukrán háborúban érintett hacktivista csoportok mely országokat támadták 2023-ban. Magyarországnak ezen a listán Írország után a második legkevesebb ilyen támadással kellett szembesülnie. A kutatás szerint mindössze öt ilyen támadás történt hazánk ellen, míg a lista élén álló Csehországnak ebben az időszakban 300 hacktivista akcióval kellett szembenéznie. Összességében tehát, bár a kiberincidensek magas látenciájával számolni kell, mind a kevés objektív, mind pedig a számos szubjektív jel alapján arra kell következtetnünk, hogy Magyarország kevésbé kitett a kibertámadásoknak, mint a legtöbb Európai Unió- és NATO-tagállam.

A Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar Kiberbiztonsági Kutatóintézete folyamatos és rendszeres kapcsolatban áll a már említett Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézetével, amely szervezet az új nemzeti kiberbiztonsági stratégia kidolgozásának felelőse. Mivel a Kutatóintézet is részt vesz a nemzeti kiberbiztonsági stratégia kidolgozásában, ezért az intézet vezetése 2022 őszén úgy döntött, hogy tudományos kutatási módszereken nyugvó, objektív tényeken alapuló információkkal segíti a stratégiaalkotást, kiküszöbölve a tényadatok hiányosságát. A kutatási projekt a „Digitális Mohács 3.0" nevet kapta. A kutatás első fázisában a Kutatóintézet szervezésében megkezdődött egy olyan tudományos diskurzussorozat, melynek célja a Magyarországra vonatkozó kibertéri fenyegetések feltárása volt. Ezen tudományos viták eredményeképpen a kutatóközösség több előadást tartott a szakmai közönség részére. Ezek vitaindító és tudományos ismeretterjesztő előadások voltak; abban segítettek, hogy megfogalmazódhassanak azok a hipotézisek, melyek tudományos módszertannal alátámasztott igazolása a 2023/2024-es tanévben történt meg. A tanulmány előzetes eredményei szerint Magyarország alacsony kitettségű kibertérként jellemezhető, de a fenyegetések növekvő diverzitása miatt elengedhetetlen a nemzeti kiberstratégia mielőbbi aktualizálása.

4 Bruce et al. 2024.

5 BM 2024.

6 Kim-McLeod 2024.

### *Stratégiai alapok*

A tudományos módszertanra épülő kutatás és az abból származó következtetések levonása már csak azért is észszerű, mivel a korábban már említett kibertéri alacsonyabb szintű kitettség nem jelenti azt, hogy nem kellene már most is hatalmas erőforrásokat fordítani az egyébként egyre romló kiberbiztonsági trendek fenntartására. Ezt támasztja alá az a szakértői vélekedés is, amely szerint bármikor egy olyan fordulat állhat be a hazai kibertérben is, mely radikálisan megváltoztathatja a magyar kibertér fenyegetettségét. A szűkös erőforrások megfelelő elosztásának és a gondos tervezésnek tehát fontos előfeltétele, hogy a lehető legobjektívebben lássuk, hogy mit tartogat a közeljövő Magyarország kibertéri biztonságával kapcsolatban! A „jövőbelátás" feladatát minden ország a nemzeti kiberbiztonsági stratégiák rendszeres kiadásával oldja meg. Ez Magyarország esetében is igaz, vagy igaznak kellene lennie. Az első magyar kiberbiztonsági stratégia 2013-ban jelent meg. A 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról[7] még 2024-ben is hatályos, holott számos helyen elavult, nem számol például az olyan, kibertérre is hatással levő konfliktusokkal, mint a 2014-ben, a Krím-félsziget megszállásával kezdődő orosz–ukrán háború. Ezt egészítette ki a 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról,[8] mely 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,[9] röviden a NIS irányelv követelményeként került kiadásra. Ez a 2018-as stratégia már jobban illeszkedik a 2010-es évek közepének újszerű kihívásaihoz, de törvényszerűen nem számolhat a 2020-as évek korábban említett radikális változásaival, melyeket a 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról[10] már tartalmaz, igaz csak nagy vonalakban és némileg általánosságok szintjén. A stratégia elsődleges célja a kibertérre vonatkozóan a nemzeti kiberbiztonsági képességek folyamatos fejlesztése, különösen a kritikus infrastruktúrák és a nemzeti adatvagyon védelme érdekében. Ennek kapcsán említést tesz az offenzív katonai kiberképességek fejlesztéséről is. A stratégia hangsúlyozza a kiberfenyegetések elleni védelem fontosságát, különösen az állami és gazdasági szektorban, valamint a lakosság kiberbiztonsági tudatosságának növelését. A nemzetközi együttműködés erősítése kiemelt jelentőséggel szerepel a dokumentumban, különösen az EU- és a NATO-tagállamaival való közös fellépés terén. A stratégia célul tűzi ki a megfelelő jogszabályi környezet kialakítását és folyamatos fejlesztését. A leírás szerint a kiberbiztonsági intézmények és szervezetek támogatása szintén prioritást élvez. A stratégia ösztönzi a kiberbiztonsággal kapcsolatos kutatásokat és fejlesztéseket, innovatív megoldások keresése érdekében.

7 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

8 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról.

9 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.

10 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

Nem utolsó sorban pedig nevesíti azokat a nem állami, fenyegető aktorokat, melyekkel a magyar kibervédelemnek szembe kell néznie. Ezek a szervezett bűnözői körök, nemzetközi terrorszervezetek, kiberbűnözői csoportok, szélsőséges vallási közösségek, magán biztonsági cégek, egyes nem kormányzati szervezetek és egyéb transznacionális hálózatok. A dokumentum végül előírja egy új nemzeti kiberbiztonsági stratégia megalkotását is.

Bár a 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről[11] szerint működő Kiberbiztonsági Fórumon régebb óta napirenden van ennek az új nemzeti kiberbiztonsági stratégiának a megvitatása, különböző okok miatt az új kibertérre vonatkozó biztonsági stratégia 2024 augusztusáig, azaz jelen tanulmány írásának időpontjáig, még nem jelent meg. A megjelenés azonban nem várathat sokáig, hiszen az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről, azaz az ún. NIS2 irányelv (2022. december 14.) 7. cikke egyértelmű tagállami előírásként fogalmazza meg, hogy „A magas szintű kiberbiztonság elérése és fenntartása céljából minden tagállam nemzeti kiberbiztonsági stratégiát fogad el, amely előírja a stratégiai célokat, az e célok eléréséhez szükséges erőforrásokat, valamint a megfelelő szakpolitikai és szabályozási intézkedéseket."

Ráadásul az is elvárásként jelenik meg, hogy „A tagállamok a fő teljesítménymutatók alapján rendszeresen, de legalább ötévente értékelik nemzeti kiberbiztonsági stratégiájukat, és szükség esetén aktualizálják azt."[12]

Mivel a NIS2 irányelv legkésőbb 2024. október 18-tól hatályossá válik minden EU-tagországban, így Magyarországnak sem sok ideje maradt egy jövőálló, a kibertéri fenyegetésekre megfelelően reflektáló stratégia megalkotására.

### *Digitális Mohács: korábbi kutatások*

A Digitális Mohács cikksorozat korábbi részei megfelelő keretet adnak a fentiekben vázolt kutatásnak. A *Digitális Mohács*[13] című, 2010-ben megjelent tanulmányban jelen cikk szerzői a digitális világ fenyegetéseit és a védekezési lehetőségeket elemzik, a mohácsi csata katasztrófáját szimbolikus párhuzamként használva. A szerzők rávilágítanak a kritikus infrastruktúrák, például az energetikai és kommunikációs rendszerek sebezhetőségére és a kiberháború veszélyeire. A tanulmány hangsúlyozza a kiberbiztonsági intézkedések fontosságát és konkrét javaslatokat tesz a védelem

11 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről.

12 Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről.

13 Kovács, Krasznay 2010.

erősítésére, beleértve a technológiai fejlesztéseket, a szakemberképzést és a nemzetközi együttműködést, több évvel megelőzve a 2013-ban megjelent Nemzeti Kiberbiztonsági Stratégiát. A szerzők részletesen tárgyalják a kiberbűnözés és a kiberterrorizmus fenyegetéseit, valamint a társadalom és a gazdaság működésére gyakorolt potenciális hatásokat. Az írás célja, hogy a 2007-ben történt, Észtországot ért orosz kibertámadás apropóján felhívja a figyelmet a digitális térben rejlő veszélyekre és ösztönözze a társadalmi és politikai döntéshozókat a proaktív kiberbiztonsági stratégiák kidolgozására és megvalósítására. Az elemzés rávilágít arra, hogy a digitális infrastruktúra védelme nemzeti biztonsági kérdéssé vált, és a megfelelő intézkedések hiánya akár a mohácsi csatához hasonló katasztrófához is vezethet a digitális világban. A cikk a következő években jelentős hivatkozási alappá vált, magyar és angol változatára több tucat mű hivatkozik a Magyar Tudományos Művek Tára nyilvántartása szerint.

A *Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint*[14] című cikk 2017-ben jelent meg, mely részletesen elemzi a kibertámadások jellegét és a kiberbiztonság aktuális kihívásait, jellemzően az Ukrajnával szemben kifejtett orosz hibrid műveletek tapasztalatai alapján. A szerzők kiemelik a modern technológiák és globális kapcsolatok hatásait, bemutatják a kibertámadások típusait, célpontjait és a védekezés leghatékonyabb módszereit. A cikk hangsúlyozza a nemzetközi együttműködés, a folyamatos technológiai fejlődés és a szakértők képzésének fontosságát. Míg az első cikk, a *Digitális Mohács* a mohácsi csata történelmi jelentőségét használja metaforaként a digitális világban bekövetkező lehetséges katasztrófák illusztrálására, a második cikk főleg a kritikus infrastruktúrák sebezhetőségére és a kiberháború veszélyeire fókuszál, általános javaslatokat téve a technológiai védelem, szakemberképzés és nemzetközi együttműködés fontosságáról. A *Digitális Mohács 2.0* cikk konkrétabb és részletesebb szakértői elemzést nyújt a kibertámadások és a védekezés módszereiről, míg az első cikk inkább figyelemfelkeltő megközelítést alkalmaz. A 2017-es cikket szintén számos tudományos mű idézi.

Mindkét publikációban a kérdőívezés módszerét használták a szerzők a hipotéziseik alátámasztására vagy azok elvetésére. Míg a *Digitális Mohács* cikk célja az volt, hogy a Hacktivity hackerkonferencia résztvevőinek attitűdjét mérje fel személyes részvételükkel kapcsolatban Magyarország defenzív és offenzív kibervédelmében, a *Digitális Mohács 2.0* esetében a Hétpecsét Információbiztonsági Egyesület konferenciájának résztvevőit kérdezték meg a szerzők arról, hogyan vélekednek a felvázolt kibertámadási forgatókönyv megvalósíthatóságáról.

### *Magyarország kiberbiztonsági helyzete*

Jelen tanulmány az előző két publikáció kutatási módszertanát viszi tovább. A szerzők a kutatás első fázisában a már említett módon workshopokat tartottak a Nemzeti Közszolgálati Egyetem kiberbiztonsággal foglalkozó kutatóinak, oktatóinak és doktoranduszainak bevonásával. A workshopok célja az volt, hogy a résztvevők felvázolják azokat a kibertéri fenyegetéseket, melyekkel szemben a magyar kibervédelem intézményrendszerének fel kell lépnie. A kutatás első hipotéziseként az fogalmazódott

14 Kovács, Krasznay 2017.

meg, hogy a későbbiekben felsorolt kihívások teljeskörűen lefedik azt a fenyegetéshalmazt, melyekkel a Nemzeti Kiberbiztonsági Stratégiának foglalkoznia kell. A kutatás második fázisában mélyinterjúk készültek, amelyek során a magyar kibervédelem vezető szakértői (állami és kritikus infrastruktúrák képviselői) a következő kérdésekre adtak választ: Milyen fenyegetésekkel szembesül Magyarország? Hogyan értékelik az ország kibervédelmi felkészültségét? Ezek az interjúk részletes képet nyújtanak a stratégiai szintű kiberfenyegetések kezelésének hazai gyakorlatáról. A mélyinterjúk célja elsősorban az volt, hogy a workshopon meghatározott fenyegetéshalmazt validálja és pontosítsa. Másodsorban viszont a szerzők azt kívánták felmérni, hogy az interjú során milyen fenyegetéseket emelnek ki maguktól a válaszadók, illetve hogyan értékelik Magyarország kibertéri kitettségét, a magyar kibervédelem felkészültségét, és látják-e egyáltalán realitását annak, hogy Magyarországot egy másik nemzetállam részéről összehangolt kibertéri művelet éri. A kutatás harmadik fázisában, a korábbi Digitális Mohács kutatásokhoz hasonlóan, egy olyan kérdőív került összeállításra, melyet a kibervédelemben dolgozó szakértők között tettek elérhetővé, kihasználva a különböző közösségi média-felületeket. A tömeges kérdőív azt a cél szolgálta, hogy felmérje, mit gondol a szakértői közösség a mélyinterjúk során finomhangolt fenyegetéshalmazról, illetve hogyan látják Magyarország kiberfenyegetettségét a kibervédelem felelős vezetőihez képest. A második hipotézis ugyanis az volt, hogy a szakértői közösség és a mélyinterjúban részt vevő vezetők hasonlóképp vélekednek a stratégiai kiberfenyegetésekről, visszajelzéseikben szignifikáns eltérések nem lesznek.

Az első hipotézishez kapcsolódóan az alábbi fenyegetéshalmazt állapította meg a kutatóközösség, amelyet a mélyinterjúban részt vevő szakértői csoport tovább részletezett és specifikált:

1. ***Érzékeny információk megszerzése nyílt forrásból származó adatok alapján:*** Rosszindulatú szereplők a nyílt forrású hírszerzés módszerével olyan adatokat gyűjtenek, melyek segítségével a személyre vagy a szervezetre vonatkozó érzékeny információkhoz jutnak hozzá, ezáltal pedig célzott kibertámadásokat tudnak indítani.
2. ***Tömeges és célzott adathalászat:*** Támadók megtévesztő e-maileket küldenek tömegeknek vagy jól megválasztott célszemélyeknek, melyek segítségével hozzáférési adatokat (például felhasználónév, jelszó) szereznek meg.
3. ***Nagy mennyiségű érzékeny adat kiszivárgása:*** Egy sor érzékeny adatot (például személyes adatokat) tartalmazó adatbázis tartalma nem megfelelő üzemeltetés vagy kibertámadás eredményeként nyilvánosan elérhetővé válik.
4. ***Célzott, állami hátterű kiberhírszerzési művelet:*** Egy állami hátterű hírszerző csoport olyan komplex műveletet hajt végre Magyarország ellen, melynek célja a magyar és a szövetségesi rendszert érintő minősített információk megszerzése.
5. ***Elosztott túlterheléses támadások*** (DDoS: *D*enial-of-Service attack) ***kritikus szolgáltatások ellen:*** Olyan logikai támadás, amely az informatikai rendszer egy (vagy több) kiszolgálóját tömeges szolgáltatás igényével túlterheli, ami a felhasználók hozzáférését nehezíti, vagy akár a kiszolgáló teljes leállásához is vezethet.

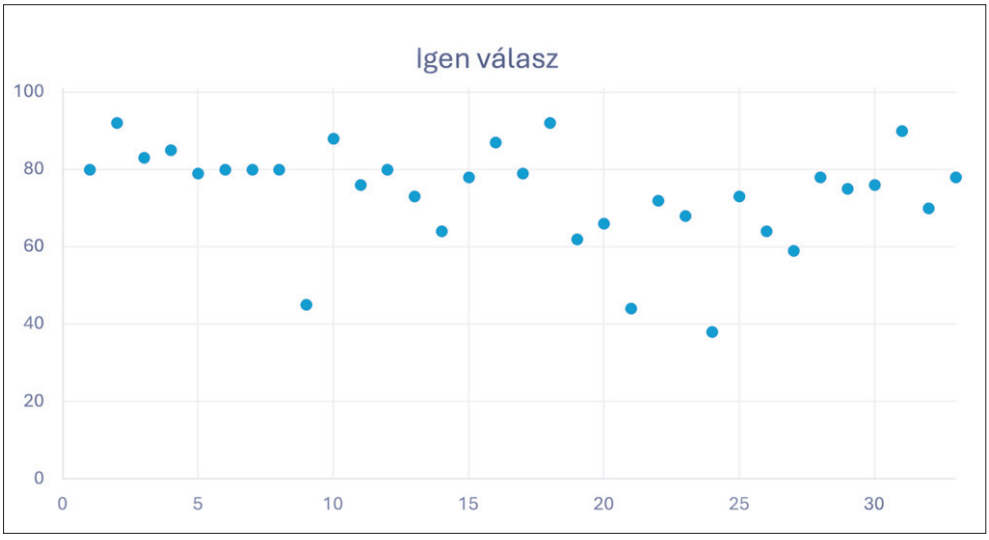
6. ***Közműszolgálatások rendelkezésre állásának sérülése:*** A közműszolgáltatásokban (például internet- vagy villamosenergia-szolgáltatás stb.) bekövetkező részleges vagy teljes leállás miatt, az egymástól való függőség (interdependencia) következtében más kulcsfontosságú szolgáltatások digitális rendszerei válnak elérhetetlenné.
7. ***Támogatás nélküli infrastruktúra jelenléte kritikus szolgáltatásokban:*** Kritikus szolgáltatásokban olyan szoftverrendszereket használnak, melyekhez gyártójuk már nem biztosít biztonsági frissítéseket, így ezek életciklusuk végéig sérülékenyek maradnak az ismert sebezhetőségekkel szemben.
8. ***Kormányzati rendszerek „átfertőzöttsége":*** A magyar kormányzati IT-rendszerekben olyan kártékony kódok, kémprogramok kerülnek telepítésre, melyek technológiájukból adódóan csak akkor távolíthatók el teljesen, ha a teljes infrastruktúrát újra telepítik.
9. ***Titkosított kommunikációs csatornák túlhasználata vagy használatának hiánya:*** A titkosított kommunikációs csatornák széles körű használata, például a csevegőalkalmazásokban jelentősen megnehezíti a rendvédelmi szervek nyomozati munkáját, eközben viszont az érzékeny adatok megosztásánál a kommunikáló felek sokszor nem használják ki a mindenki számára rendelkezésre álló titkosítási megoldásokban rejlő lehetőségeket, és ezzel sértik az adatcsere bizalmasságát.
10. ***Kritikus infrastruktúrákat érintő kibertámadások:*** Egy nemzetállami szereplő vagy kiberbűnözői csoport olyan kibertéri műveletet indít egy magyar kritikus infrastruktúra ellen, mely az adott infrastruktúra sértetlenségét vagy rendelkezésre állását befolyásolja negatívan.
11. ***A kibervédelmi technológiával kapcsolatos lemaradásból eredő kitettség:*** A magyarországi szervezetek anyagi vagy képességbeli hiányosságok miatt nem tudják a legújabb kibervédelmi megoldásokat felhasználni, így kitettségük nagyobb, mint azoké a szervezeteké, ahol ezen technológiák felhasználása megtörténik.
12. ***Ipari informatikai rendszerek sebezhetőségének kihasználása:*** Támadók kihasználják a speciális ipari informatikai rendszerekben található szoftveres sebezhetőségeket, ezáltal veszélyeztetik a kritikus infrastruktúrák működését.
13. ***IoT*** *(Internet of Things, dolgok internete)* ***és IIoT*** (*Industrial Internet of Things,* ipari dolgok internete) ***sebezhetőségek kihasználása:*** Támadók a Magyarország területén található otthoni és ipari okoseszközöket tömegesen fertőzik meg kártékony kódokkal a bennük található szoftveres vagy konfigurációs sebezhetőségek kihasználásával, ezáltal megsértve ezen eszközök és a rajtuk tárolt adatok bizalmasságát, sértetlenségét és rendelkezésre állását.
14. ***IoT alapú botnetek létrehozása:*** A megfertőzött okoseszközöket a támadók nagyobb hálózatokba szervezik, melyeket utána komolyabb kibertámadásokra, például elosztott túlterheléses támadásokra használnak, ezáltal forrásországként bevonva Magyarországot a más országok elleni kibertámadásokba.

15. ***0. napi sebezhetőségek jelenléte kritikus rendszerekben:*** Olyan szoftverhibák vannak jelen az elektronikus információs rendszerekben, melyekre nem létezik hibajavítás, és sokszor a gyártó előtt sem ismertek ezek a hibák, viszont van olyan kihasználási módjuk, melyen keresztül jogosulatlan felhasználók szerezhetnek hozzáférést a rendszerben.
16. ***Emberi ráhatással történő támadások (social engineering):*** A támadó nem technológiai sebezhetőségeket használ ki, hanem arra törekszik, hogy megtévesszen egy felhasználót. A megtévesztés eredményeként a jogosultsággal rendelkező felhasználó a jogosulatlan személy számára bizalmas adatokat ad át, vagy lehetőséget biztosít számára a saját vagy szervezete egy vagy több rendszerébe történő belépésre, kimondottan a pszichológiai befolyásolást végző személy megtévesztő viselkedése miatt.
17. ***Online csalások tömeges elkövetése:*** A gazdasági célú csalások tömegesen tevődnek át az online felületekre, kereskedelmi oldalakra, ezáltal egyre több magyar állampolgár válik csalás áldozatává.
18. ***Digitális írástudás és kiberbiztonsági tudatosság hiánya:*** A magyar állampolgárok általában kevéssé tudják biztonságosan használni az informatikai eszközöket, és nincsenek tisztában a kiberhigiénia alapjaival, így tömegesen válnak kitetté a kibertámadásoknak magánéletükben és munkájuk során is.
19. ***A szervezett kiberbűnözés megjelenése, „társadalmasítása":*** Magyar állampolgárok könnyen csatlakozhatnak a külföldi szervezett kiberbűnözői csoportokhoz, használhatják azok támadó infrastruktúráját, cserébe nyelv- és helyismeretet adnak, ezáltal a magyar szervezetek és állampolgárok még kitettebbé válnak a kiberbűncselekményeknek.
20. ***Tömeges kártékonykód-fertőzések:*** Olyan rosszindulatú programok tömeges telepítése, melyek jelentős hatást váltanak ki a nemzeti kibertérben a megfertőzött végpontok és azon tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megsértésével. Ide tartoznak a zsarolóvírusok is.
21. ***Kiberönkéntesek (hacktivisták) által elkövetett támadások:*** Hacktivista az, aki egy politikai ideológia mentén szervezett kibertéri akcióban vesz részt, melynek hatása van a fizikai világra is. Tipikusan csoportosan követik el a cselekményt, sokszor egymást nem is ismerve, akár nagyon eltérő földrajzi helyekről is. Egy hacktivista cselekmény jellemzően az elosztott túlterheléses támadásokra (DDoS), a weboldalak átírására (*defacement*) és az adatlopásra korlátozódik.
22. ***Hazai és európai kibervédelmi ipar hiánya:*** Magyarország a legkritikusabb kibervédelmi rendszereit is kénytelen Európán kívüli gyártóktól beszerezni, így nem garantálható például az, hogy az adott termék nem tartalmaz hátsókaput (*backdoor*), illetve nem lehetséges a nemzeti kibervédelem egyedi igényeire szabni az adott megoldást.
23. ***A geopolitikai feszültségek kibertéri hatásainak megjelenése:*** Magyarország „járulékos áldozatként" szenved el olyan kibertámadásokat, melyek olyan konfliktusokat kísérnek, mint például az Izrael-Irán vagy az USA–Kína közötti feszültségek.

24. ***Kriptovaluták és más innovatív fizetési megoldások elterjedése a monetáris rendszerben:*** A kriptovaluták és más innovatív fizetési megoldások (például Wise, Revolut stb.) széles körű elterjedése miatt a kiberbűncselekmények során ellopott anyagi javak visszaszerzése nagyon nehézzé válik.
25. ***Korlátozott információmegosztás a hazai érdekelt felek között:*** A nem megfelelő jogszabályi felhatalmazás és a hatáskörök tisztázatlansága következtében kulcsfontosságú információk nem kerülnek átadásra a hazai kulcsfontosságú szereplők között, így az érintett magyar szervezetek nem mindig értesülnek időben egy őket fenyegető kibertámadásról és a bekövetkezett incidensek részleteiről. Működő információmegosztó és -elemző központ hiányában a kölcsönös érdeken és bizalmon alapuló, meghatározott körön belüli információmegosztásnak még a kerete is hiányzik.
26. ***Korlátozott információmegosztás a nemzetközi érdekelt felek között:*** A nem megfelelő bizalmi szint következtében kulcsfontosságú információk nem kerülnek átadásra a NATO- és EU-szövetségen belül, így Magyarország és az érintett magyar szervezetek nem értesülnek időben egy őket fenyegető kibertámadásról.
27. ***Bizalmi elemek kompromittálódása:*** Olyan bizalmi hardver- vagy szoftverelemek biztonsága sérül (például CPU, TPM-chipek, digitális személyazonosítók stb.), melyek cseréje bonyolult vagy lehetetlen, így a rájuk épülő rendszerek biztonsága sem fenntartható.
28. ***Ellenérdekelt országok beépülése az ellátási láncba:*** A Magyarországgal és szövetségeseivel ellenérdekelt országok olyan módon befolyásolják a kulcsfontosságú digitális szolgáltatásokat, szoftvereket és hardvereket, például a saját országuk területén működő vállalatokra érvényes jogszabályokkal vagy látszólag semleges vállalatokba történő bújtatott felvásárlásokkal, hogy az ezek segítségével kezelt adatok bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet.
29. ***A hazai hardver/szoftver ellátási láncok egyenszilárdságú védelmének hiánya:*** A hardver/szoftver ellátási láncok sérülékenységeinek kihasználása világszerte növekvő, Magyarországot sem elkerülő tendenciát mutat. A külföldi jó gyakorlatok ismeretének és hazai implementációjának változó – alapvetően elégtelen – szintje a növekvő fenyegetések közepette egyre kevéssé vállalható kockázatot jelent.
30. ***A digitális ellátási láncok támadása:*** Olyan kulcsfontosságú technológiák támadása, mint például a felhőszolgáltatások, melynek következtében az elektronikus információs rendszerek széles körének sértetlensége vagy rendelkezésre állása sérül.
31. ***A mesterséges intelligencia (MI) felhasználása kibertámadások során:*** A széles körben rendelkezésre álló MI-alapú megoldások, például deepfake-ek előállítása és széles körű használata az állami hátterű kibertámadások során és a kiberbűnözés eszköztárában.

32. ***Célzott pszichológiai műveletek Magyarországgal szemben:*** Olyan, állami szereplő által tervezett módszer, mely szelektált információkat és indikátorokat közvetít egy meghatározott célcsoport részére, annak érdekében, hogy befolyásolja érzelmeiket, motivációikat, tárgyi szemléletmódjukat.
33. ***Általános dezinformáció:*** Olyan, nem állami szereplő által szándékosan létrehozott, megtévesztő, félrevezető információt értünk alatta, amit nyereségvágyból vagy szándékos károkozás céljából igaz információként próbálnak elfogadtatni, elsősorban a közösségi médián keresztül.[15]

A kérdőívben a következő kérdés szerepelt a fenyegetésekhez kapcsolódóan: „A következőkben olyan fenyegetéseket fogunk felsorolni, melyek a Nemzeti Közszolgálati Egyetem kiberbiztonsági kutatócsoportja által végzett előzetes kutatások alapján reális kihívást jelentenek Magyarország kiberbiztonságára nézve. Kérjük, hogy alaposan olvassa el a megadott fogalmat! Kérjük, jelölje meg a fogalmat akkor, ha véleménye szerint az adott fenyegetés Magyarországra nézve valós és szerepelnie kell Magyarország új nemzeti kiberbiztonsági stratégiájában!" A válasz lehetett „Igen", „Nem" és „Nem tudom". A kérdésre összesen 101 értékelhető válasz érkezett, ezek közül az Igen válaszok arányát az alábbi ábra tartalmazza.




*1. ábra.*
***A stratégiai kiberbiztonsági fenyegetésekre adott Igen válaszok a Digitális Mohács 3.0 kérdőívben***

15 A szakértői interjúk során a 32. és 33. fenyegetéseket a válaszadók kettéválasztották, ezzel megkülönböztetve az információs műveleteket és a nyereségvágyból végrehajtott kiberbűncselekményeket. Meg kell azonban jegyezni, hogy a gyakorlatban ez a két fenyegetés összemosódhat.

Jól látható módon három olyan fenyegetés volt, melyet a válaszadók biztosan nem tartanak olyannak, melynek a magyar kiberbiztonsági stratégiában szerepelnie kell. Ezek a 9. (Titkosított kommunikációs csatornák túlhasználata vagy használatának hiánya), a 21. (Kiberönkéntesek [hacktivisták] által elkövetett támadások) és a 24. (Kriptovaluták és más innovatív fizetési megoldások elterjedése a monetáris rendszerben) számúak. További négy olyan fenyegetés volt, mely nem érte el a válaszadók 2/3-ának támogatását, ezek a 14. (IoT alapú botnetek létrehozása), a 19. (A szervezett kiberbűnözés megjelenése, „társadalmasítása"), a 26. (Korlátozott információmegosztás a nemzetközi érdekelt felek között) és a 27. (Bizalmi elemek kompromittálódása) számú fenyegetések voltak. Az öt legnagyobb támogatást kapó fenyegetés sorrendben a 2. (Tömeges és célzott adathalászat), 18. (Digitális írástudás és kiberbiztonsági tudatosság hiánya), 31. (A mesterséges intelligencia felhasználása kibertámadások során), 10. (Kritikus infrastruktúrákat érintő kibertámadások) és 16. (Emberi ráhatással történő támadások (social engineering) számú volt, 87 és 92 közötti Igen szavazattal. Ezek a válaszok részben egybevágnak a szakértőkkel készített mélyinterjúkon tapasztaltakkal, akik szintén egyetértettek abban, hogy a felsorolt fenyegetések túlnyomó többsége olyan, melynek helye van egy nemzeti kiberbiztonsági stratégiában, viszont a lekevesebb szavazatot kapó 7 fenyegetés kivétel nélkül szerepelt egy vagy több szakértő válaszában, mint olyan fenyegetés, mely nem stratégiai jelentőségű. Ezek tehát kivehetők a listáról, mert bár fontos fenyegetésekre mutatnak rá, jelenleg nem olyan mértékűek, hogy azzal egy nemzeti kiberbiztonsági stratégiában foglalkozni kelljen a szakértők szerint.

Az első hipotézis validálása során a mélyinterjú és a kérdőív arra is kitért, hogy mely fenyegetések hiányoznak a kutatócsoport által meghatározott listáról. A kérdés így szólt: „Véleménye szerint mely egyéb kibertéri fenyegetések vannak, és melyik kategóriába tartoznak, melyek nem szerepelnek a listában, de stratégiai szintűek Magyarországra nézve?", illetve „Amennyiben van még olyan kibertéri fenyegetés, melyet véleménye szerint szerepeltetni kell Magyarország új nemzeti kiberbiztonsági stratégiájában, de nem szerepelt a felsorolásban, kérjük, írja le az alábbi mezőben!". A saját szavas válaszok jellemzően olyan területekre utaltak, melyeket az eredeti fenyegetéshalmaz lefedett, ám több válaszadónál is szignifikánsan megjelent két fenyegetés, melyet a kutatócsoport eredetileg nem vett figyelembe. Egyrészt a kiberbiztonsági szakemberhiány – idézet egy válaszból „Szakemberek hiánya a kiberbiztonság területén, vagy jelenős verseny ezen szakemberekért, így a forráshiányos szervezeteknél hiányos ismeretekkel és tapasztalattal rendelkező »szakemberek« megléte)" –, másrészt a vezetőség elköteleződésének hiánya jelent meg számos válaszban – idézet egy válaszból: „Az, hogy az általam megismert vezetők mind, kivétel nélkül úgy gondolják, hogy az információbiztonság és az adatvédelem csak akadályozza a munkát és nincs rájuk semmi szükség, csak egy újabb jelmondat, amivel pénzt lehet lehúzni." A válaszok elemzéséből kiderül, hogy az irányítás hiányát szervezeti és nemzeti szinten is megemlítették a szakértők. Összességében tehát az első hipotézist részben alátámasztották a válaszok, a 33 felsorolt fenyegetésből 26 mindkét kérdőívtípuson legalább 2/3-os támogatottságra talált, és mindössze két olyan fenyegetést jelzett a válaszadói közösség, mely az eredeti listán nem szerepelt.

A második hipotézis igazolására a következő kérdés hangzott el a mélyinterjúkban és a kérdőívben: „Zárókérdésként arról szeretnénk kikérni a véleményét, hogy összességében van-e és ha igen, mekkora a kockázata egy Magyarországot érő, stratégiai hatást kiváltó kibertéri műveletnek? Kérem, hogy először válaszoljon az alábbi kérdésre! Véleménye szerint van-e annak reális esélye, hogy Magyarország ellen állami hátterű kibertámadás indul?". A kérdőívre adott válaszokból kiderült: a 101 válaszadó közül 89 gondolja úgy, hogy ez egy reálisan bekövetkezhető forgatókönyv, ami azt jelenti, hogy a válaszadók 88%-a válaszolt Igennel. A szakértőkkel készített mélyinterjúk során 13 válaszadóból 11 válaszolt Igennel, ami 84,6%-ot jelent, tehát közel ugyanakkora volt az Igenek aránya, mint ami a tömeges kérdőív során volt tapasztalható.

Nagyon eltérő válaszok születtek azonban arra, hogy egy ilyen hipotetikus kibertámadás mekkora valószínűséggel történhet meg és mekkora hatást váltana ki Magyarországra nézve. Mindkét válaszadói csoport számára a következő kérdéseket tettük fel: „Amennyiben Igennel válaszolt, először azt szeretnénk kérdezni, hogy 1-5-ig terjedő skálán mekkorának ítéli meg ennek valószínűségét?", illetve „Most azt szeretnénk megkérdezni, hogy 1-5-ig terjedő skálán mekkora hatása lehet egy Magyarország elleni összehangolt kibertámadásnak?" A mélyinterjún részt vevő szakértők a valószínűséget átlagosan 2,54-re, a várható kár mértékét átlagosan 4,18-ra tették, míg a tömeges kérdőív válaszadói a bekövetkezési valószínűséget 4,1-re, a várható kár mértékét 3,66-ra becsülték. A mély rálátással rendelkező kiberbiztonsági vezetők tehát lényegesen kisebb bekövetkezési valószínűséget, de szignifikánsan magasabb kárértéket várnak, mint a kiberbiztonságban dolgozó szakértők, akik nem feltétlenül rendelkeznek azzal a stratégiai ismerettel, mint a mélyinterjú résztvevői. Az alábbi ábrán az látható, hogy egy, a szakterületen használt általános kockázati mátrixban hol helyezkednek el a két csoporttól származó válaszok. A táblázatban a színek az alábbiak szerint értendőek: zöld – alacsony kockázat, sárga – mérsékelt kockázat, narancssárga – jelentős kockázat, piros – magas kockázat.

*2. ábra.*
***A Magyarországot érő összehangolt kiberművelet kockázati mátrixa***

| | **1: Ritka, valószínűtlen** | **2: Nem valószínű** | **3: Lehetséges** | **4: Valószínű** | **5: Szinte biztos** |
|---|---|---|---|---|---|
| **5: Katasztrofális** | | | | | |
| **4: Jelentős** | | Mélyinterjú válaszadói | | | |
| **3: Mérsékelt** | | | | Kérdőív válaszadói | |
| **2: Kicsi** | | | | | |
| **1: Elhanyagolható** | | | | | |

A kérdőívben meghatározott pontos definíciók a következők voltak a bekövetkezés valószínűségére vonatkozóan:

1. Az összehangolt kibertámadás esélye nagyon kicsi, szinte biztos, hogy nem következik be.
2. Az összehangolt kibertámadás valószínűleg nem fog bekövetkezni ebben az évtizedben, de esélye idővel egyre nagyobb lesz.
3. Az összehangolt kibertámadás valószínűleg ebben az évtizedben bekövetkezik, de egyelőre nem kell tőle tartani.
4. Az összehangolt kibertámadás bekövetkezte a következő 3–5 évben várható.
5. Az összehangolt kibertámadás bármikor bekövetkezhet a közeli jövőben.

A várható kár mértékére vonatkozóan pedig az alábbi definíciókkal találkoztak a kitöltők:

1. Elhanyagolható hatása lesz, az állampolgárok szinte észre sem fogják venni.
2. Kis hatása lesz, egyes szolgáltatások rövid ideig leállnak, a közvélemény foglalkozni fog vele, de komolyabb gazdasági és politikai hatás nem várható.
3. Közepes hatása lesz, bizonyos szolgáltatások több napra leállnak, a közvélemény kiemelt helyen kezeli a kibertámadást, egyes szervezetek számára komoly gazdasági problémát okoz a jelenség, a politika pedig kénytelen reagálni a helyzetre.
4. Komoly hatása lesz, a támadás miatt kritikus szolgáltatások állnak le rövidebb ideig, ez az elsődleges téma a közvélemény körében, a helyzet gazdasági értelemben súlyosan érint számos szervezetet, a kormány kiemelten kezeli a helyzetet.
5. Kritikus hatása lesz, a támadás következtében létfontosságú rendszerek állnak le hosszabb ideig, akár emberek is meghalnak, a lakosság részéről pánikreakciókat lehet észlelni, a gazdasági kár nemzetgazdasági szinten is mérhető, a kormány a szövetségi rendszerből kér segítséget.

A második hipotézis tehát szintén igazolásra került, de csak részben. A kiberbiztonsági szakmában dolgozók és a kibervédelemért felelős vezetők közel ugyanakkora arányban gondolják úgy, hogy egy Magyarországgal szembeni, összehangolt kibertámadás bekövetkezhet, ennek bekövetkezési valószínűségét és a várható kár mértékét azonban szignifikánsan máshogy látják, így a kockázati mátrix alapján általánosságban a kockázatot – mely egyszerűsítve a bekövetkezési valószínűség és a várható kár mértékének szorzata – is eltérően értékelik. A mélyinterjú során megszólított szakértők közepes (10,61), a kérdőívvel elért szakértők pedig magas kockázatot (15) állapítottak meg. Érdemes ezt összevetni a két csoportnak feltett első kérdéssel is, mely így szólt: „Hogyan értékeli Magyarország általános kibertéri kitettségét 1–5 skálán?". A mélyinterjú során megkérdezett szakértők átlagosan 3,19-re, míg a kérdőívvel elért szakértők 3,63-ra becsülték ezt a szintet, még mielőtt a részletes kérdéseket megkapták volna.

### *Összegzés, következtetések*

Összességében a „Digitális Mohács 3.0" kutatás célja az volt, hogy meg lehessen állapítani, milyen attitűddel rendelkeznek a magyar kibervédelemben ma aktív szerepet játszó szakértők. A vizsgálat fő fókusza Magyarország kibertéri kitettségére irányult. A kérdés elemzése során egy stratégiai szintű kibertámadás került felvázolásra, majd ez lett összevetve a kiberbiztonsági szakmában dolgozó szakértők erre a támadásra adott lehetséges válaszaival. A mélyinterjúk során 13 vezetővel készült interjú, akik átlagosan 18,3 éve dolgoznak a szakterületen döntéshozóként, döntéselőkészítőként vagy senior szakértőként. Kiválasztásuk és felkérésük a Nemzeti Közszolgálati Egyetem Kiberbiztonsági Kutatóintézetén keresztül történt oly módon, hogy a workshopokon részt vevő kutatók egybehangzóan állították össze a kulcsfontosságú személyek listáját. A 2023 decembere és 2024 márciusa között elkészített interjúk során kiderült azonban, hogy azok a személyek, akiket egybehangzóan kulcsfontosságú személyeknek tartott a kutatói közösség, jellemzően nincsenek döntéshozó pozícióban. Ez egyrészt érthető, hiszen a végső döntéshozatal a nemzeti kibervédelemben és a kritikus infrastruktúráknál a szakértői szintnél magasabb szinten van, másrészt rávilágít arra is, hogy hiába látják tisztán a Magyarországot fenyegető kibertéri veszélyeket ezek a kulcsfontosságú személyek, ha a teljes körű védelemhez szükséges vezetői támogatást nem tudják megszerezni vagy a szükséges és elégséges védelmi intézkedéseket nem lehet – például erőforrás hiányában – megvalósítani. Ez a csoport arra a kérdésre, hogy „Hogyan értékeli Magyarország kibervédelmi képességeit 1–5 skálán?", átlagosan 2,88-as választ adott. A válaszadók arra a kérdésre, hogy miért az adott pontszámot adták, szinte egyöntetűen azt válaszolták, hogy a vezetői szinten nincsen kellő megértés és szükséges támogatás. A magyar kibervédelem megerősítéséhez elengedhetetlen a társadalmi összefogás, valamint a szakpolitikai és gazdasági döntéshozók szoros együttműködése a kiberbiztonsági szakértőkkel.

FELHASZNÁLT IRODALOM

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról biztonságára vonatkozó Stratégiájáról.

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek.

484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről.

Belügyminisztérium 2024. BSR - Bűnügyi Statisztikai Rendszer. https://bsr.bm.hu/Document/Index

Bruce M., Lusthaus J., Kashyap R., Phair N., Varese F. 2024. Mapping the global geography of cybercrime with the World Cybercrime Index. *PLoS ONE* 19 (4): e0297312. https://doi.org/10.1371/journal.pone.0297312

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.

Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről.

Kim-McLeod, Riam 2024. *Russia-Ukraine war: Telegram-based hacktivism in 2023.* https://www.secalliance.com/blog/russia-ukraine-war-telegram-based-hacktivism-in-2023

Kovács László, Krasznay Csaba 2010. Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság: Biztonságpolitikai Szemle,* 2010 (1): 44–56.

Kovács László, Krasznay Csaba 2017. Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság: Biztonságpolitikai Szemle,* 2017 (1): 3–16.

Legárd Ildikó 2023. Információbiztonsági incidenstrendek a közigazgatásban. *Nemzetbiztonsági Szemle*, 11. (1): 78–107. https://doi.org/10.32561/nsz.2023.1.6

Magyar Nemzeti Bank 2022. A magyar pénzügyi szektor kiberfenyegetettségi térképe 2022. https://www.mnb.hu/letoltes/kiberfenyegetettsegi-terkep-2022.pdf

Nemzeti Adatvédelmi és Információszabadság Hatóság 2024. A Nemzeti Adatvédelmi és Információszabadság Hatóság 2023. évi beszámolója. https://www.naih.hu/eves-beszamolok?download=908:naih-beszamolo-a-2023-evi-tevekenysegrol