NEMZETBIZTONSÁGI SZEMLE
12. évfolyam (2024) 2. szám 18–37. | DOI: 10.32561/nsz.2024.2.2

Szénási Imre[1]

Kritikus rendszerelemek jellemzői, azok kijelölése, valamint azok védelme

Characteristics of Critical Infrastuctures, their Designation and Protection

Globalizált világunkban a kritikus rendszerelemek vagy más néven a kritikus infrastruktúrák védelme egyre nagyobb figyelmet kap. A tanulmányban megvizsgálom a kritikus infrastruktúrák védelmére a 21. században létrejött szabályozást az Amerikai Egyesült Államok, az Európai Unió, az Észak-atlanti Szerződés Szervezete és Magyarország szempontjából. A kritikus rendszerelemek védelme hazánkban alapvetően a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóságának hatáskörébe tartozik, azonban lehetnek olyan esetek, amikor nem a Belügyminisztérium, hanem a Magyar Honvédség látja el ezeket a feladatokat. Az őrzés-védelmi feladat e formája egyáltalán nem könnyű. Napjainkban megjelentek néhány évtizeddel ezelőtt még egyáltalán nem létező nyílt információforrások. Segítségükkel az őrzött kritikus infrastruktúra elleni támadás viszonylag egyszerűen megtervezhető, akár amatőrök számára is. A tanulmányban az orosz–ukrán háborúból származó példákat mutatok be arra, hogy egyszerű felhasználók is milyen hatékonyan támogathatják a hadseregek harcát, hogyan igazolhatják vagy cáfolhatják a propaganda állításait kizárólag az internet felhasználásával. Megfogalmaztam egy javaslatot az aktív és tartalékos katonák információtudatosságra való felkészítésére. A kutatásom során nyílt forrásokra támaszkodtam, a témához tartozó szakirodalom, a sajtóban megjelent források, valamint a jogszabályok analízisét és elemzését végeztem el.

Kulcsszavak: *kritikus rendszerelem, orosz–ukrán háború, nyílt információ, információtudatosság*

In today's globalised world, the protection of critical system components, also known as critical infrastructure, is receiving increasing attention. In this paper I will examine the regulation of critical infrastructure protection in the 21st century

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: imre.szenasi81@gmail.com

from the perspective of the United States of America, the European Union, the North Atlantic Treaty Organisation and Hungary. In Hungary, the protection of critical system elements is basically the responsibility of the National Directorate General for Disaster Management of the Ministry of the Interior. However, there may be cases where the Hungarian Defence Forces, rather than the Ministry of the Interior, carry out these tasks. The task of guarding and protecting is not an easy one, as open sources of information have emerged that did not exist a few decades ago, making it relatively easy for even amateurs to plan an attack on such guarded critical infrastructure. In this paper, I will present examples from the Russian war in Ukraine of how ordinary users can effectively support the armies' war effort and verify or refute propaganda claims using only the Internet. I have formulated a proposal for information literacy training for active and reserve soldiers.

Keywords: *critical infrastructure, Russian-Ukrainian war, open information, information awareness*

Bevezetés

Napjaink globalizált világában a kritikus rendszerelemek vagy más néven a kritikus infrastruktúrák védelme egyre nagyobb figyelmet kap. Hazánkban sincsen ez másképp.

Tanulmányomat a kapcsolódó fogalmak ismertetésével kezdem, majd rátérek a kritikus rendszerelemek jellemzőire és azok kialakulásának rövid történetére. Megvizsgálom a kritikus infrastruktúrák védelmére a 21. században létrejött szabályozást az Amerikai Egyesült Államok, az Európai Unió, az Észak-atlanti Szerződés Szervezete és Magyarország szempontjából.

A kritikus rendszerelemek védelme hazánkban alapvetően a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóságának hatáskörébe tartozik, azonban lehetnek olyan esetek, amikor nem a Belügyminisztérium, hanem a Magyar Honvédség látja el ezeket a feladatokat. Az aktív katonák létszámuknál fogva képtelenek lennének minden kijelölt kritikus infrastruktúra védelmére. A tartalékos rendszer kiegészíti a reguláris fegyveres erők képességeit, ezért ez a tevékenység megjelenik az Önkéntes Területvédelmi Tartalékosok feladatrendszerében is, összhangban a Magyar Honvédség Magyarország Nemzeti Katonai Stratégiájában[2] megfogalmazott küldetésével.

Az egyszerűnek tűnő őrzés-védelmi feladat azonban napjainkban egyáltalán nem könnyű. Néhány évtizeddel ezelőtt még egyáltalán nem létező, nyílt forrásúnak tekinthető információforrások jelentek meg, amelyek segítségével az őrzött kritikus infrastruktúra elleni támadás viszonylag egyszerűen megtervezhető, akár amatőrök számára is, az interneten fellelhető különböző applikációk és a közösségi média használatával.

Dolgozatomban az orosz–ukrán háborúból származó példákat mutatok be arra, hogy egyszerű felhasználók is milyen hatékonyan támogathatják a hadseregek harcát, hogyan igazolhatják vagy cáfolhatják a propaganda állításait, akár saját otthonukból a karosszékükben helyet foglalva, kizárólag az internet felhasználásával. A hipotézisem

[2] A Kormány 1393/2021. (VI. 24.) Korm. határozata Magyarország Nemzeti Katonai Stratégiájáról.

az, hogy a kritikus rendszerelemek védelme érdekében az azok őrzés-védelmét ellátó katonáinkat fel kell készíteni az internet és a közösségi portálok biztonságos használatára. A tanulmány végén javaslatot fogalmazok meg az aktív és tartalékos katonák információtudatosságra való felkészítésére. A kutatásom során nyílt forrásokra támaszkodtam, a témához tartozó szakirodalom, a sajtóban megjelent források, valamint a jogszabályok analízisét és elemzését végeztem el.

Kritikus infrastruktúrák, avagy kritikus rendszerelemek és azok jellemzői

Mielőtt megkezdem a kritikus infrastruktúra vizsgálatát, meghatározom az infrastruktúra szó jelentését. Az infrastruktúra:

> „közvetett módon, a szükséges feltételek, pl. infrastrukturális létesítmények, eszközök, speciális szaktudással rendelkező személyek megteremtésével járul hozzá a gazdasági-társadalmi szféra működéséhez. Két alapvető ágazata a termelői infrastruktúra (a gazdasági jellegű feltételek biztosítója) és a szociális infrastruktúra (a társadalmi jellegű feltételek biztosítója)."[3]

Amennyiben az infrastruktúrákat a fontosságuk szempontjából vizsgáljuk meg, akkor megkülönböztethetünk kritikus és sebezhető infrastruktúrákat. Tevékenységük alapvető fontosságú a gazdasági-társadalmi szféra működéséhez. Működésképtelenné válásuk esetén, ami megtörténhet valamilyen külső vagy belső beavatkozás következtében, az adott ország biztonsága kerülhet veszélybe, és ez beláthatatlan következményekkel járhat.[4]

Az infrastruktúra rövid bemutatása után rátérek a kritikus rendszerelemek fogalmának ismertetésére. A kritikus infrastruktúra fogalma Gőcze István szerint:

> „Magyarországon található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése, e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna."[5]

Gőcze István Magyarország szemszögéből vizsgálja ezt a területet, de az Európai Unió is foglalkozik a kérdéssel. A kritikus infrastruktúra fogalma az Európai Parlament és a Tanács 2022/2557 Irányelve[6] szerint: „olyan eszköz, létesítmény, berendezés, hálózat vagy rendszer, vagy valamely eszköz, létesítmény, berendezés, hálózat vagy rendszer része, amely szükséges az alapvető szolgáltatás nyújtásához."[7]

---

3 Közszolgálati Online Lexikon: infrastruktúra.
4 Haig–Kovács 2012: 45–46.
5 Közszolgálati Online Lexikon: kritikus infrastruktúra.
6 Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről.
7 A Tanács 2008/114/EK irányelve, 3.

A fogalmak meghatározása után ismertetem a kritikus infrastruktúra kialakulásának rövid történetét. A kritikus infrastruktúra nem új fogalom. Korábban nem pont ezen a néven illették, azonban a rendelkezésünkre álló írott történeti forrásokból kiderül, hogy a történelem során minden állam megvédte a gyenge pontjait. Gondoskodott azon infrastruktúrájának védelméről, amely a működéshez elengedhetetlen volt. Napjainkban ezeket már kritikus rendszerelemeknek is nevezik. Az ókori birodalmakban és a középkori államokban ezek elsősorban közlekedési és élelmiszer-ellátási útvonalakat vagy anyagi erőforrásaikat jelentették. Mindamellett a közigazgatási központok is a kritikus infrastruktúra elemei közé tartoztak.[8] A két világháború és a hidegháború alatt jött létre az, amit ma „kritikus infrastruktúrák védelme" elnevezéssel illetünk.[9]

Az emberi fejlődés dinamikus folyamata magával hozta az infrastruktúrák változását is. A folyamatból kiemelkedik az ipari forradalmak időszaka és a világháborúk kora, amelyek hatására robbanásszerű fejlődés következett be a technológiában és az infrastruktúrában. Az elektromosság felfedezése és elterjedése, a távközlési rendszerek kialakulása, a közlekedés új formáinak (például a vasút, a gépjárművek, a polgári repülés) megjelenése, az ipar tömegtermelésre való áttérése, valamint a kémiai-fizikai-biológiai tudományos felfedezések mind-mind könnyedebbé tették az emberek hétköznapi életét és lakhatóbbá a környezetet. Az új találmányok, a nagy technikai áttörések, a napjainkban megjelenő új fizikai és virtuális infrastruktúrák – egyesével és együttesen is – a rendszerek iránti függőség, az egymásrautaltság és a komplexitás veszélyét hordozzák magukban.[10]

A fentiekben megfogalmazottak miatt meghatározó jelentőségű, hogy feltérképezzük és pontosan behatároljuk a kritikus infrastruktúrákat. A kritikus rendszerelemek Haig Zsolt szerint alapvetően három fő típusra oszthatóak. Az első típus biztosítja a nélkülözhetetlen javak előállítását, szállítását és a társadalom számára alapvető fontosságú szolgáltatások folyamatos elérhetőségét. A második típusú kritikus infrastruktúrák teszik lehetővé az egymással való összeköttetést és az együttműködés képességét. A világháló és a különböző zárt kommunikációs és számítógép-hálózatok kötik össze és gyakran azokon keresztül irányítják és hangolják össze a társadalom és a gazdaság többi infrastruktúráját; ezeket kritikus információs infrastruktúráknak nevezik. A harmadik típusú kritikus infrastruktúrák járulnak hozzá az ország köz- és külső biztonságának megteremtéséhez. A kritikus infrastruktúrák védelme és működésének fenntartása a nemzetbiztonság szempontjából minden kormányzat meghatározó és létfontosságú feladata.[11]

A kritikus infrastruktúrákat fenyegető veszélyek

Az infrastruktúrára nyomást gyakorló fenyegetések a természetes és az épített környezetre is jelentős hatást gyakorolhatnak. Milyen, az infrastruktúrára leselkedő veszélyek vannak napjainkban?

A veszélyek megkülönböztethetőek a formáik szerint. Az ártó szándékú cselekedetek alapvető formái azok a szándékos károkozás céljából végrehajtott cselekmények, amelyek

8 Babos 2007: 14.
9 Babos 2016: 6.
10 Bonnyai 2019: 29.
11 Haig–Kovács 2012: 46.

nemcsak a keletkezett anyagi kár miatt jelentősek, hanem az egész társadalomra gyakorolt pszichológiai hatásuk is rendkívüli lehet. Az ártó szándékú cselekményeknek több típusa is létezik. Ide sorolhatók a klasszikus háborús cselekmények, a fegyveres összeütközések, a hibrid támadások, a terrorcselekmények, a kibertámadások, a társadalmi eredetű események (például zavargások), fegyveres konfliktusok kirobbantása, valamint a gazdasági, politikai okkal elkövetett visszaélések.[12]

Másik formaként a katasztrófajellegű eseményeket említhetjük – természeti, ipari vagy civilizációs katasztrófák –, amelyek bekövetkezési valószínűsége és gyakorisága csak nagyon csekély mértékben jelezhető előre, azonban bekövetkezésük jelentős következményekkel járhat.

Elsőként áttekintem a természeti eredetű veszélyeket, amelyek lehetnek hidrológiai események (ár-, bel- és villámárvíz, cunami), meteorológiai események, geológiai események (földrengések, földcsuszamlások), nagy kiterjedésű vegetációs tűzesetek, napkitörések. Az ipari eredetű veszélyek lehetnek valamilyen, az alkalmazott technológiában keletkező hibák, helytelen emberi beavatkozás vagy baleset miatt az ipari létesítményekben, illetve azokkal kapcsolatosan bekövetkező veszélyhelyzetek. A következőképpen jelenhetnek meg: veszélyes anyagokkal foglalkozó üzemben vagy egyéb ipari létesítményekben bekövetkező esemény, veszélyes áru szállításakor történt közlekedési baleset, környezetkárosodással járó esemény, nukleáris létesítményben bekövetkező esemény. A civilizációs katasztrófák a korunkbeli társadalom jellegzetességein alapuló olyan események, amelyek az alkalmazott rendszerek és a társadalom működőképességére egyformán kifejthetik a hatásukat. A civilizációs katasztrófák lehetnek: informatikai, kommunikációs vagy navigációs rendszerek rongálódása, humánegészségügyi és állategészségügyi epidémiák, táplálékhiány és vízkészletekért folyó fegyveres küzdelem vagy az infrastruktúrák kapacitásának kimerülése.[13]

Korunk ipari és gazdasági fejlettsége, a társadalom rétegei között tapasztalható egyre növekvő különbségek, a radikális vallási és politikai nézeteket valló csoportok számának folyamatos emelkedése és azok időszakos megerősödése, a világ terrorveszélyeztetettségének exponenciális növekedése mind okot szolgáltatnak arra, hogy a prevenciós szemlélet erősödjön.[14]

A kritikus rendszerelemek védelmére vonatkozó szabályozás fejlesztése

Amerikai Egyesült Államok

A prevenció szükségességét az Amerikai Egyesült Államokban is felismerték 1997-ben: az elnök kérésére egy tudományos testület (Federation of American Scientists) jelentést készített, amelyben felhívták a figyelmet a kritikus infrastruktúra sebezhetőségére,

12 Bognár–Bonnyai–Vámosi 2019: 33–35.
13 Bognár–Bonnyai–Vámosi 2019: 33–35.
14 Bognár–Bonnyai–Vámosi 2019: 33–35.

valamint ajánlásokat is megfogalmaztak azok védelmére.[15] A 2001. szeptember 11-i kritikus infrastruktúra elleni terrortámadás (World Trade Center és Pentagon)[16] után alkották meg a Nemzetbiztonsági Törvényt,[17] majd 2006-ban annak kiegészítését, a Nemzeti Infrastruktúra-védelmi Programot.[18] Az Egyesült Államok 16 kritikusinfrastruktúra-ágazatot azonosított, ezek a vegyipari, kereskedelmi létesítmények, hírközlési, kritikus termelési egységek, gátak, védelemipari, sürgősségi szolgáltatások, energia-, pénzügyi szolgáltatási, élelmiszeripari és mezőgazdasági, kormányzati létesítmények, egészségügyi és közegészségügyi, informatikai, nukleáris reaktorok, anyagok és hulladékok, közlekedési rendszerek, valamint a víz- és szennyvízrendszerek ágazata.

Európai Unió

Az Európai Unió (EU) 2004-ben kezdett el mélyrehatóbban foglalkozni a kritikus infrastruktúrával, az Európai Tanács júliusban átfogó stratégia kidolgozására kérte fel a Bizottságot a kritikus infrastruktúrák védelme javításának érdekében. Az Európai Unió Bizottsága ebben az évben hozta nyilvánosságra első javaslatát, a Létfontosságú Infrastruktúrák Védelmére Vonatkozó Európai Programot.[19] Ez alapján dolgozták ki az úgynevezett Zöld könyvet.[20] Az EU jogalkotási folyamatának eredményeként hirdették ki az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló irányelvet.[21] Az irányelv csak az energia- és a közlekedési ágazatra, valamint a kritikus infrastruktúrák védelmére összpontosított. Az irányelv alkalmazásában az európai kritikus infrastruktúra[22] fogalma:

> „a tagállamokban található olyan kritikus infrastruktúra, amelynek megzavarása vagy megsemmisítése jelentős hatással lenne legalább két tagállamra. A hatás jelentőségét a horizontális kritériumok alapján kell értékelni. Ide tartoznak azok a hatások is, amelyek az egyéb típusú infrastruktúrákkal fennálló, ágazatokon átnyúló kölcsönös függőségből erednek."[23]

Meghatározta a tagállamok részére, hogy 2011. január 12-ig meghozzák azokat az intézkedéseket, amelyekkel megfelelnek az irányelvnek. A 2008/114/EK irányelv 2024. október 18-ával hatályát veszti, és helyébe az Európai Parlament és a Tanács (EU) 2022/2557 irányelve lép, amelyet 11 ágazatra[24] kell alkalmazni.[25] 2016-ban az Európai Unió elfogadta

15 *Critical Foundations* 2007: 15.
16 The White House 2003: 15.
17 The USA PATRIOT Act 2001.
18 Mógor–Földi–Solymosi 2008: 15–27.
19 European Programme for Critical Infrastructure Protection, lásd: https://eur-lex.europa.eu/legal-content/EN-HU/TXT/?from=EN&uri=LEGISSUM%3Al33260
20 Zöld könyv COM(2005) 576.
21 A Tanács 2008/114/EK irányelve.
22 European Critical Infrastructure (ECI).
23 A Tanács 2008/114/EK irányelve, 3.
24 Energia, közlekedés, banki szolgáltatások, pénzügyi piaci infrastruktúra, digitális infrastruktúra, közigazgatás, világűr, egészségügy, ivóvíz, szennyvíz, valamint élelmiszer-előállítás, -feldolgozás és -forgalmazás.
25 (EU) 2022/2557 irányelv.

az Európai Parlament és a Tanács (EU) 2016/1148 számú, hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelvét (NIS).[26] Az első olyan átfogó szabályozás volt ez az információbiztonság területén, amely hálózati és információs rendszerek magas biztonsági szintjét kívánta biztosítani a közösségen belül. Az irányelv egyformán szabályozta az alapvető szolgáltatásokat biztosító szereplőket, valamint a digitális szolgáltatókat is.[27] Az irányelv a technológia fejlődésnek köszönhetően hamarosan elavulttá vált. Helyébe az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.), az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS 2) szóló irányelv[28] lépett 2023. január 16-án, amely korszerűsítette a jogi keretet a megnövekedett digitalizációhoz és a kiberbiztonsági fenyegetések változó környezetéhez való alkalmazkodás érdekében. A NIS 2 irányelv a kiberbiztonsági szabályok hatályát új ágazatokra és szervezetekre is kiterjesztette, valamint javította az Unió egészének kiberbiztonsági rezilienciáját.

Észak-atlanti Szerződés Szervezete

A NATO[29] elsődleges feladata 1949-es megalakulása óta a szövetség területének és a tagállamok népességének védelme a szerződés 5. cikkelye alapján. A Szövetség a hidegháború alatt nem hajtott végre semmilyen e cikkely hatálya alá eső műveletet, de felkészült arra, az esetleges vészhelyzetekre vonatkozó gyakorlatok végrehajtása során. Az 5. cikkely szerinti segítségnyújtást a 2001. szeptember 11-i, az Egyesült Államok elleni terrortámadás után aktiválták először.[30]

A kritikus rendszerelemek szempontjából azonban jóval fontosabb az Észak-atlanti Szerződés 3. cikkelye, amely kimondja: „A jelen szerződésben kitűzött célok hathatósabb elérése érdekében a Felek külön-külön és együttesen, folyamatos és hathatós önsegély és kölcsönös segítség útján, fenntartják és kifejlesztik egyéni és kollektív védelmi képességüket fegyveres támadással szemben."[31] Kijelenthető, hogy a NATO védelmi struktúrájában a civil mellett a katonai képesség biztosítására helyezi a fő hangsúlyt, amely csak abban az esetben teljesül, ha a tagországok rugalmasak és ellenállóak a fentiekben már felsorolt ártó szándékú cselekményekkel és katasztrófajellegű eseményekkel szemben. Az ellenálló képesség a NATO szerint az az egyéni és kollektív képesség, amely lehetővé teszi a tagállamok számára a sokkhatásokra és a zavarokra történő felkészülést, az ellenállást, az azokkal szemben alkalmazott válaszlépéseket, valamint az azokból történő gyors helyreállítást,

26 Network and Information Systems (NIS). Az Európai Parlament és a Tanács (Eu) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

27 Mógor–Angyal 2022: 119.

28 Az 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.

29 Észak-atlanti Szerződés Szervezete.

30 NATO 2022a.

31 Az Észak-atlanti Szerződés, Washington DC, 1949. április 4.

és biztosítja a Szövetség működésének folytonosságát.[32] A fentiekben megfogalmazottak miatt a polgári védelem („olyan össztársadalmi feladat-, eszköz- és intézkedési rendszer, amelynek célja katasztrófa, illetve fegyveres összeütközés esetén a lakosság életének megóvása, az életben maradás feltételeinek biztosítása, valamint a lakosság felkészítése azok hatásainak leküzdése és a túlélés feltételeinek megteremtése érdekében")[33] a NATO nemzeti és kollektív ellenálló képességének egyik központi pillére és a kollektív védelem egyik kritikus eszköze, amely létfontosságú a társadalmak és a közös értékek védelme szempontjából.[34] A Szövetség támogatja a tagállamokat az ellenálló képesség megerősítésében. 2007-ben pedig készített egy összefoglalót a kritikus infrastruktúrák védelméről és az Európai Unióval történő együttműködésről.[35] A 2016-os varsói csúcstalálkozón a NATO tagországainak állam- és kormányfői megállapodtak abban, hogy fokozzák a Szövetség ellenálló képességét a fenyegetések teljes spektrumával szemben.[36] 2021-ben a brüsszeli csúcstalálkozón kötelezettséget vállaltak arra, hogy megerősítik a tagállamok rugalmasságát és a polgári felkészültségi intézkedéseket.[37] A NATO 2022-ben egy új bizottságot hozott létre, az Ellenálló Képesség Bizottságot,[38] amely átvette a Polgári Vészhelyzeti Tervezési Bizottság[39] feladatait és szerepét is. Az Ellenálló Képesség Bizottság felelős az Észak-atlanti Szövetségen belül a stratégiai és szakpolitikai irányvonal megalkotásáért és a NATO ellenálló képességgel kapcsolatos tevékenységeinek koordinálásáért. A Szövetség legfontosabb politikai dokumentuma a stratégiai koncepció. A 2022. évben elfogadott stratégiai koncepció szerint a NATO alapvető feladatai – az elrettentés és a védelem, a válságmegelőzés és -kezelés, valamint az együttműködő biztonság – szempontjából kritikus fontosságú az ellenálló képesség. Annak elfogadásakor a tagállamok egyetértettek abban, hogy megerősítik a nemzeti és szövetségi szintű ellenálló képességet a katonai és nem katonai fenyegetésekkel, valamint a biztonságot érintő kihívásokkal szemben is.[40] A 2023-as vilniusi csúcstalálkozón a szövetséges vezetők megismételték a Szövetség elkötelezettségét a rugalmasság megerősítése mellett. Kiemeltek továbbá több olyan területet, amely további odafigyelést igényel, beleértve a társadalmi ellenálló képességet, az egészségügyi rendszereket, a kritikus infrastruktúrát és az ellátási láncokat is.[41]

A NATO 1992 és 2023 között 23 alkalommal rendezte meg a NATO Válságkezelési Gyakorlatát (CMX),[42] ahol a polgári vezetők mellett a katonai törzsek és a NATO Parancsnokságok vesznek részt. A 2023-ban megrendezett CMX 23 gyakorlaton a fentiekben felsoroltak mellett részt vett Finnország és Svédország, valamint az Európai Külügyi Szolgálat, az Európai Bizottság, valamint az Európai Tanács és az Európai Unió Tanácsa

32 NATO 2023b.
33 Lásd: www.katasztrofavedelem.hu/265/mi-a-polgari-vedelem#Mi%20a%20polg%C3%A1ri%20v%C3%A9delem?
34 NATO 2023b.
35 NATO 2007.
36 NATO 2016.
37 NATO 2021.
38 Resilience Committee (RC) – Ellenálló Képesség Bizottság.
39 Civil Emergency Planning Committee (CEPC) – Polgári Vészhelyzeti Tervezési Bizottság.
40 NATO 2022b.
41 NATO 2023c.
42 Crisis Management Exercise (CMX) – Válságkezelési Gyakorlat

Főtitkársága is. Ezen gyakorlatok célja a NATO stratégiai, politikai és katonai szintű konzultációs és döntéshozatali eljárásainak tesztelése.[43]

Magyarország

Magyarország mint az Európai Unió egyik tagja természetesen eleget tett a 2008-as európai uniós irányelvnek. Annak kiadása előtt, 2008-ban a kormány tárcaközi szakmai munkacsoport bevonásával megalkotta a nemzeti kritikus infrastruktúrák védelméről szóló Nemzeti Zöld Könyvet,[44] majd 2012 novemberében kihirdették, és több lépcsőben hatályba lépett a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, valamint a 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.[45] A 2013. évi L. törvény[46] szabja meg az állami és önkormányzati szervek mellett a kritikus rendszerek és létesítmények információbiztonsági keretrendszerét, amelyek hatósági felügyeletét a Nemzetbiztonsági Szakszolgálat látja el.[47] 2020-ban lépett hatályba a Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Kormány határozat, amelynek számos rendelkezése a létfontosságú rendszerek védelmére vonatkozó feladatokat fogalmazott meg.

A hazai szabályozásban a kritikus infrastruktúrák védelmében érintett ágazatokat és alágazatokat az 1. táblázat tartalmazza.

1. táblázat: A kritikus infrastruktúrák védelmében érintett ágazatok és alágazatok

Ágazat	Alágazat
Energia	villamosenergia-rendszer létesítményei (kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek)
	kőolajipar
	földgázipar
	távhő
Közlekedés	közúti közlekedés
	vasúti közlekedés
	légi közlekedés
	vízi közlekedés
	logisztikai központok
Agrárgazdaság	mezőgazdaság
	élelmiszeripar
	elosztó hálózatok

43 NATO 2023a.
44 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.
45 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.
46 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
47 Lásd: www.katasztrofavedelem.hu/109/kritikus-infrastrukturak-vedelmevel-osszefuggo-hatosagi-feladatok-jogszabalyok

Ágazat	Alágazat
Egészségügy	aktív fekvőbeteg-ellátás és a működtetéséhez szükséges szolgáltatások
	mentésirányítás
	egészségügyi tartalékok és vérkészletek
	magas biztonsági szintű biológiai laboratóriumok
	gyógyszer-nagykereskedelem
Társadalom-biztosítás	társadalombiztosítási ellátások igénybevételéhez kapcsolódó informatikai rendszerek és nyilvántartások
Pénzügy	pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei
	bank- és hitelintézeti biztonság
	készpénzellátás
Infokommunikációs technológiák	internet-hozzáférési szolgáltatás és internet-infrastruktúra
	elektronikus hírközlési szolgáltatások, elektronikus hírközlő hálózatok
	műsorszórás
	postai szolgáltatások
	kormányzati elektronikus információs rendszerek
Víz	ivóvíz-szolgáltatás
	felszíni és felszín alatti vizek minőségének ellenőrzése
	szennyvízelvezetés és -tisztítás
	vízbázisok védelme
	árvízi védművek, gátak
Honvédelem	honvédelmi rendszerek és létesítmények
Közbiztonság-védelem	rendvédelmi szervek infrastruktúrái

Forrás: www.katasztrofavedelem.hu/110/erintett-agazatok-alagazatok

Az Európai Unió NIS irányelvének integrációja is megtörtént a hazai szabályozásban, aminek következtében már megjelent a kibervédelem.[48] Hazánk a NIS 2 irányelvet is bevezette 2024. január 1-jén,[49] ezzel igyekszik csökkenteni a kiberbiztonsági fenyegetések kockázatát és biztosítani a szolgáltatások folyamatosságát.

Magyarországon a NATO védelmi struktúrája is megvalósul a kritikus rendszerelemek vonatkozásában. Egyrészt a honvédelmi létfontosságú rendszerelemek tekintetében.[50] Másrészt a nemzeti szabályozás lehetőséget ad arra, hogy honvédelmi érdekből, jogszabályban meghatározott feltételek alapján kijelölhető, nem honvédelmi ágazatba tartozó elem is nemzeti létfontosságú rendszerelemmé váljon. Az üzemeltetői biztonsági terv megalkotásához a honvédelmi hatóság speciális előírásokat tehet, ahol külön rész foglalkozik a honvédelmi sajátosságokkal, a honvédelmi szervekkel történő kapcsolattartással és az együttműködés rendjével.[51]

48 Mógor–Angyal 2022: 119.
49 23/2023. (XII. 19.) Szabályozott Tevékenységek Felügyeleti Hatóság rendelet az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásáról.
50 359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről.
51 Mógor–Angyal 2022: 119.

A nemzeti ellenálló képesség megszilárdításában előrelépést jelentett a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény,[52] amely önálló fejezetben határozza meg a nemzeti ellenálló képesség rendszerének követelményeit.

A területvédelmi tartalékosok és a kritikus rendszerelemek

Magyarországon a tartalékos rendszer keretfeladatait a Nemzeti Katonai Stratégiában fogalmazták meg.[53] A politikai vezetés e dokumentumban határozta meg a haderő részére a honvédelmi kiegészítő és hátországvédelmi képességeket, valamint a tartalékosokkal szemben támasztott elvárásokat. A Magyar Honvédség folyamatosan erősíti reguláris és tartalékos haderejét egy, a kor színvonalán álló fegyveres erő kialakítása érdekében, hogy az képes legyen a jelenkor biztonsági kihívásainak és kockázatainak megfelelni. Az önkéntes tartalékos rendszernek képessé kell válnia békében és a különleges jogrend bevezetése esetén is a hivatásos és szerződéses állomány támogatására, az új típusú kihívásokat is beleértve, valamint kiegészítő erőként azzal koherens rendszert alkotni.[54]

A területvédelmi erők rendeltetése az ország függetlenségének, területi épségének és határainak katonai védelme bármely lehetséges agresszor támadásával szemben, ami összhangban van a NATO-szabványokkal. A szövetség minden tagállamának rugalmasnak kell lennie, saját védelmi képességeinek kiépítésére vonatkozóan (Észak-atlanti Szerződés 3. cikkely), a nemzetközi szerződésekből eredő közös védelmi feladatok ellátása, természeti és ipari katasztrófavédelmi tevékenységek végzése, valamint a nemzetközi jog szabályainak megfelelően humanitárius feladatok ellátásának érdekében. A tartalékos rendszer kiegészíti a reguláris fegyveres erők képességeit, azonban helyettesíteni nem képes azt.

A területvédelmi erők fő feladatai összhangban vannak a Magyar Honvédség Magyarország Nemzeti Katonai Stratégiájának megfogalmazott küldetésével.[55] A területvédelmi tartalékos erők fő feladatai az alábbiak:

- a területvédelmi rendszer folyamatos működtetése és fejlesztése;
- részvétel őrzés-védelmi feladatokban, a létfontosságú rendszerelemek vagy más néven a kritikus infrastruktúra védelmében, valamint a polgári védelmi feladatok támogatásában;
- a tartalékos állomány alapkiképzése és további kiképzések végrehajtása;
- helyi protokolláris feladatok ellátása, valamint hadisírok, katonai és hősi emlékművek fenntartása és kegyeleti tevékenységekben való részvétel;
- Magyarország területének területvédelmi biztosítása, valamint a lakosság élet- és vagyonbiztonságának védelme;
- részvétel a tömeges bevándorlás elleni védekezésben;
- különböző válságkezelési tevékenységek összehangolása és megvalósítása, valamint részvétel a katasztrófavédelmi feladatokban a nemzeti biztonsági rendszer más elemeivel együttműködve a helyi közösségek védelme és támogatása érdekében;

52 2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról.
53 1393/2021. (VI. 24.) Korm. határozat.
54 1393/2021. (VI. 24.) Korm. határozat.
55 1393/2021. (VI. 24.) Korm. határozat.

- a Befogadó Nemzeti Támogatás katonai feladatainak biztosítása és koordinálása a szövetséges erők hatékony fogadásának és Magyarországon való állomásoztatásának lehetővé tétele érdekében;
- a magyar társadalomban a hazafias értékek megőrzése, erősítése, valamint a katonai nevelési programok nemzedékeken átívelő megvalósítása.[56]

A területi elven (járásonként) szervezett önkéntes védelmi képesség, amely az Önkéntes Területvédelmi Tartalékos (ÖTT)[57] rendszert jelenti, összesen 197 ÖTT-századot alkot Budapest kerületeiben és az ország járásaiban. Az ÖTT megyénként alkot egy területvédelmi zászlóaljat (TVZ), zászlóaljanként egy aktív kiképző századdal, valamint régiónként egy, összesen hét területvédelmi ezredet (TVE).

A Magyar Honvédség Területvédelmi Erők Parancsnoksága (MH TVEP) felelős a területvédelmi feladatokat ellátó szervezeti elemeinek hadműveleti és harcászati szintű irányításáért. Az alárendeltségébe tartozik az ÖTT szolgálati forma bevezetése óta megalakított hét TVE is.

A területvédelmi tartalékosok fentiekben felsorolt feladataiból kiemelkedik a kritikus rendszerelemek védelme. Az ÖTT-katonák elsősorban a saját járásukban látnak el feladatokat, emiatt kiemelkedő helyismerettel rendelkeznek. A katasztrófajellegű események, mint a természeti, ipari vagy civilizációs katasztrófák esetében részt vehetnek a megelőzésben (például: árvízvédelem) és a katasztrófák következményeinek felszámolásában (például: földrengések utáni keresés, kutatás, romeltakarítás) is, de ezzel a feladatcsoporttal a terjedelmi korlátok miatt nem foglalkozom.

A területvédelmi tartalékosok az ártó szándékú cselekmények, mint a háborús cselekmények, a fegyveres összeütközések, a hibrid támadások és a terrorcselekmények esetében kiképzettségük és felszerelésük miatt elsősorban élőerővel megvalósított őrzés-védelmi feladatokat láthatnak el. Elsődlegesen, de nem kizárólag az energia-, a közlekedés, az infokommunikációs technológiák és a honvédelmi ágazat területén.

Az egyik legnagyobb veszély, amely a katonák által őrzött objektumokra leselkedhet, az a fegyveres támadás (terrorcselekmény, tüzérségi tűzcsapás, drónokkal vagy beszivárgott élőerővel végrehajtott támadás, szabotázs stb.). Általánosságban kijelenthető, hogy napjainkban a leggyorsabb és legegyszerűbb formája az ilyen típusú támadások előkészítéséhez szükséges információk beszerzésének a nyílt források felhasználásával a közösségi média felületeiről történhet.

A nyílt információ forrásai

Az Információs Hivatal honlapján[58] megtalálhatóak a hírszerzés forrásai, amelyek lehetnek: humán műveleti tevékenység,[59] technikai hírszerzés,[60] valamint nyílt forrású hírszerzés.[61]

---

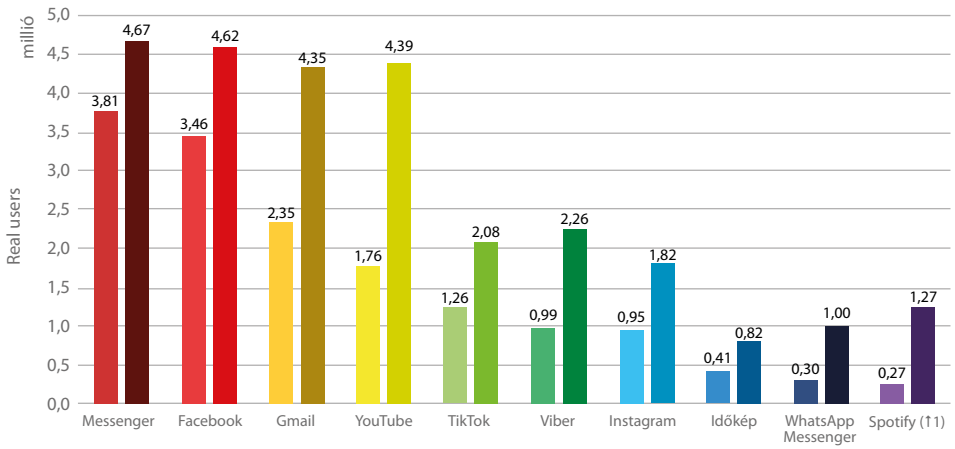
56 Magyar Honvédség Sipos Gyula 6. Területvédelmi Ezred.
57 25/2016. (XII. 22.) HM rendelet az egyes honvédelmi miniszteri rendeletek módosításáról.
58 Lásd: https://ih.gov.hu/
59 Human Intelligence – HUMINT.
60 Signals Intelligence – SIGINT.
61 Open Source Intelligence – OSINT.

A nyílt forrású hírszerzés fogalma: „bárki számára hozzáférhető, nyilvános és legális eszközökkel megszerezhető információk, melyeknek forrásai az elektronikus média, az írott sajtó, az internetes oldalak, az ingyenes és kereskedelmi adatbázisok lehetnek. Ezek szisztematikus gyűjtése és feldolgozása révén hírszerzési szempontból releváns információk keletkeznek."[62]

A nyílt információ a fent felsorolt forrásokból szabadon hozzáférhető, ebből következik, hogy nem válthatja ki az elsősorban minősített forrásokból megszerzett titkos és bizalmas információkat. Ennek ellenére olyan információkat tudhatunk meg a segítségével, amelyek elősegíthetik akár a minősített információk közti tájékozódást is. A nyílt információk felhasználásának hatalmas előnye, hogy az internet segítségével olyan adatokhoz juthatunk hozzá szabadon, akár valós időben, minimális anyagi ráfordítás mellett, amilyenekről néhány évtizeddel ezelőtt még álmodni sem lehetett. Természetesen mint mindennek, ennek is vannak hátrányai. A hátrányok közé tartozik például a rendelkezésre álló adatok gigantikus mennyisége – rendszerezésére a mesterséges intelligencia alkalmazása nyújthat segítséget. További hátránya, hogy számos, az internetre feltöltött anyag pontatlanságokat tartalmaz, vagy éppen dezinformációs céllal került fel a világhálóra, azonban ezek kiszűrésére is léteznek módszerek.[63]

Vizsgáljuk meg, hogy egy kritikus infrastruktúra elleni támadás megtervezéséhez milyen adatokhoz férhetünk hozzá nyílt forrásokat használva, vagyis az internetet és a közösségi média elemeit alkalmazva. Mindenekelőtt ki kell választanunk a célpontot, amelynek elsődleges funkciójáról, a hierarchiában elfoglalt helyéről annak hivatalos honlapjáról tájékozódhatunk. A kritikus infrastruktúra célpontként történő azonosítása során annak ellátott funkciója irreleváns. A támadás helyszínének kiválasztását követően több olyan, akár ingyenes szolgáltatást is igénybe vehetünk, amelyekkel a célterületről műholdképet, utcai nézetet (például: Google Maps, Maxar Technologies), valamint más, akár 3D-s térképet is letölthetünk, segítségükkel meghatározva a behatolási pontokat. A célpont felderítésében segítségünkre lehetnek a különböző videómegosztó portálok (YouTube, TikTok stb.), hiszen ezekre az emberek néhány like reményében rengeteg videót töltenek fel. A felvételek felbontásának minősége manapság akár a 12K-t[64] is elérheti, de egy viszonylag olcsó mobiltelefonnal is képesek 4K felbontású videók elkészítésére és feltöltésére. Amennyiben valaki célzott keresést használ, számos, addig ismeretlen adatot találhat a célpontról, amellyel megkönnyíti a gyenge pontok meghatározását. A nyílt információk egy másik nagy szeletét a hazánkban is népszerű különböző közösségi oldalak adják.

62 Információs Hivatal: A hírszerzés forrása. Lásd: https://ih.gov.hu/a-hirszerzes-forrasai.html
63 Bányász–Orbók 2013.
64 Lásd: www.youtube.com/watch?v=lFKCmnhPftM



1. ábra: A tíz legtöbb internetezőt elérő applikáció Magyarországon 2024. februárban (átlagos napi real users és havi real users)
Forrás: NMHH 2024.

Az 1. ábrából világosan kirajzolódik, hogy a közösségi médiát többen használják, mint az e-mail-szolgáltatást. Hazánkban 2024 februárjában a tíz legtöbb internetezőt elérő applikációból négy a közösségi médiához tartozott. Általánosságban véve kijelenthető, hogy a közösségi média felhasználóinak nagy többsége nem törődik a személyes adatainak védelmével, az applikációk biztonsági beállításaival vagy az általuk alkalmazott informatikai eszközök megfelelő biztonsági garanciáinak betartásával. Anyagi szempontból ugyan a közösségi média használata az esetek többségében ingyenesnek tekinthető, mégis óriási árat fizet vagy fizethet érte a felhasználó. Kiadja a személyes adatait, kapcsolati hálóját (például: LinkedIn), valamint az életének szinte minden mozzanatát. Az adatokat megszerző cégek ezeket továbbadják másoknak reklámcélra.[65] A nyílt forrású hírszerzés használatával nagyon sok érzékeny információhoz juthatunk hozzá az óvatlan felhasználók nem szándékos és sokszor nem is tudatos segítségével. A Facebook, hazánkban a jelenleg legnépszerűbb közösségi alkalmazás, például alapesetben a következő adatok hozzáféréséhez kér engedélyt a mobiltelefonon telepítve: naptár, tárhely (médiafájlok), fényképezőgép, helyadatok, hívásnaplók, mikrofon, névjegyek, telefon.[66] Az itt felsorolt adatok kiszolgáltatásáról az átlagos felhasználók többségének elképzelése sincs.[67]

A kritikus infrastruktúra védelmével megbízott katonák is emberek, akik a fenti adatok alapján nagy valószínűséggel használják a közösségi média felületeit. A katonák ilyen típusú feladatba történő bevonása előtt nagyon fontos a közösségi média használatából eredő veszélyekre figyelmeztetni és felkészíteni őket, valamint arra, hogy mire kell figyelniük. Elmagyarázni nekik az ebben az esetben az őket (is) védő rendszabályokat, ismertetni a közösségi média felületein alkalmazható biztonsági beállításokat, ahogyan ez a külszolgálatokban érintett, különösen a veszélyes területeken szolgáló katonák

65 Bányász–Orbók 2013.
66 Forrás: a szerző Facebook-applikációja.
67 Bányász–Orbók 2013.

esetében meg is történik. A kulcsszónak, véleményem szerint, a felkészítés során az információtudatosságnak kell lennie.

Most pedig tekintsük át, hogy mire kell még figyelni a katonáknak, milyen veszélyek leselkednek rájuk mint közösségimédia-felhasználókra az orosz–ukrán háború tapasztalatai alapján.

A nyílt információ amatőrök általi felhasználása hírszerzésre az orosz–ukrán háborúban

A nyílt információk megszerzésének a jelenleg is zajló orosz–ukrán háborúban is sok formáját alkalmazták és alkalmazzák. Megdöbbentő módon nemcsak a hivatalos szervek, hanem az „egyszerű" állampolgárok (az úgynevezett fotelkémek vagy Twitter-kémek) is. Ennek köszönhetően teljesen új szintre emelkedett a nyílt forrású hírszerzés.

Sokszor önkéntesen tevékenykedő állampolgárok próbálják meg kideríteni, mi igaz az orosz és ukrán oldal által is erősen befolyásolt narratívákból. A Twitter-kémek ellenőrzik a fotók, videók és beszámolók valóságtartalmát, a munkájukat pedig az ukrán és az orosz hadsereg is egyaránt felhasználja.

Hogyan lesz valaki Twitter-kém? – vetődik fel a kérdés. Az egyik választ a *Washington Post* hasábjain találhatjuk meg. Egy 29 éves férfi, Kyle Glen, aki klinikai kutatóként dolgozott Walesben, 2023-ban felfedezett egy videót a *Telegram*on. A képkockákon az volt látható, hogy feltehetően az orosz hadsereg egy ukrán civilek által használt menekülési útvonalat bombázott. Többen úgy vélték, ez ukrán dezinformáció. A férfi elemezni kezdte a felvételt, és felfedezett egy jellegzetes nevezetességet, egy olyan ortodox templomot, amelynek négy aranykupolája is volt. A Google Maps felhasználásával, valamint az Associated Press által készített fénykép segítségével meghatározta az épület pontos koordinátáit. A területtel foglalkozó Discord-, Reddit- és Twitter-bejegyzések átnézése során a robbanás szemtanúinak beszélgetéseire bukkant. Mindössze tizenkét perccel azután, hogy észrevette a felvételt, már teljesen biztos volt abban, hogy az általa felfedezett videó valódi, és közzétette az általa megalkotott elemzést a Twitter-fiókján. Létrejött új identitása: Twitter-kém lett.[68]

Természetesen nincs egyedül. Az egyik leghíresebb fotelkém az alig 20 éves Justin Peden, egy alabamai egyetemista, aki a Twitteren „The Intel Crab" néven vált híressé. Jelenleg több mint 334 500 követővel rendelkezik,[69] és több tízmillióan tekintették meg a bejegyzéseit. Az általa alkalmazott technika az, hogy ingyenes és nyíltan elérhető térképszolgáltatásokat, például a Google Earth-öt és a Yandex Maps-t használja fel, esetenként fizetős kereskedelmi műholdas adatokkal párosítja azokat, így lokalizálja az orosz légicsapásokat, tüzérségi csapásokat és egyéb érdekes pontokat. Ezt a folyamatot nevezik geolokációnak. Egy kép apró részletei alapján kideríthető, hogy pontosan hol készült. Elegendő azt térképekkel vagy kereskedelmi műholdas adatokkal összevetni, és azonnal,

[68] Verma 2022.
[69] Twitter: *IntelCrab*.

igen nagy pontossággal megerősíthető az, ami addig a pillanatig csupán megérzés vagy elmélet lett volna.[70]

A hobbikémek száma hatalmas, például a Project OWL, a nyílt forráskódú hírszerzők privát közössége az orosz–ukrán háború kirobbanását követően öt hét alatt 15 000 tagról közel 30 000-re nőtt a csoport moderátorai szerint.[71] Az idő múlásával pedig egyre ügyesebbekké is váltak. Széles körű hírszerzési adatokat képesek begyűjteni egyszerű eszközökkel. Néhányan repülőgépek és hajók követésére, mások műholdképek elemzésére, míg többen a háborús területen működő webkamerák képeinek elemzésére specializálódtak. Mások a NASA bozóttűz-adatbázisát[72] használják az ukrán „termikus anomáliák" nyomon követésére.[73]

A Twitter-kémek a geolokáció segítségével meghatározhatják az egyes ellenséges eszközök valós helyzetét is. Az így megszerzett információt felhasználva az általuk támogatott fegyveres erők könnyedén megsemmisíthetik azokat, ahogyan ez az úgynevezett „teknőstank" esetében is történt. Villámgyorsan kiderült, hogy hol rejtőzködik, ugyanis az orosz civilek fényképeket készítettek az épületben, amelyeket az internetre is feltöltöttek. Az ukrán hadsereg egy öngyilkos drónja pedig lecsapott a kínálkozó lehetőségre.[74]

A másik meglepő forrása az információknak egy meglehetősen sajátos tevékenység, nem más, mint a társkeresés. Minden embernek, így a katonáknak is megvannak a szükségleteik; mint Maslow kifejtette, az emberi szükségletek piramisának első szintjén a fiziológiai szükségletek között vannak a szexuális szükségletek.[75] Ezt természetesen a hírszerzésben dolgozók is kihasználják. A Tinderre, napjaink egyik legelterjedtebb társkereső alkalmazására, sok orosz katona is regisztrált, amit észlelve ukrán nők vették fel velük a kapcsolatot és szedtek ki szenzitív információkat belőlük,[76] amelyeket valószínűleg továbbítottak az ukrán hatóságoknak.

Az ukrán kormány állampolgárait is bevonta a nyílt forrású hírszerzésbe, a Diia nevű e-kormányzati applikációval. A program eredetileg az állampolgárok számára készült e-ügyintézési felületként a bürokrácia csökkentésére. Az ukrán kormány az orosz inváziót követően elindította az erre épülő, E-Enemy nevű funkciót. Az applikáción keresztül az állampolgárok az orosz csapatmozgásokról és háborús bűncselekményekről tájékoztathatják az ukrán hadsereget.[77] Az ide képeket vagy videókat feltöltő személyek azonosíthatóságuk esetén veszélybe kerülhettek, amennyiben a képek megjelentek a médiában, és orosz kézbe jutottak.

Nem feledkezhetünk meg a nyílt információkat elemzők másik nagy csoportjáról, a hivatásos újságírókról és a digitális oknyomozó riporterekről sem. A Bellingcat kutatók, nyomozók és polgári újságírók független oknyomozó kollektívája. Az itt dolgozó személyeket a nyílt forráskódú kutatás iránti szenvedély fogta össze.[78]

---

70 Mahadevan 2022.
71 Verma 2022.
72 NASA FIRMS.
73 Nagy 2022.
74 Portfolio 2024.
75 Maslow 1943: 370–396.
76 Parker 2022.
77 Technokrata 2022.
78 Bellingcat: Who We Are. Lásd: www.bellingcat.com/about/who-we-are/

A fentiekben láthattuk, hogy a sokszor önkéntesen tevékenykedő „fotelkémek” milyen hatékonyan tevékenykednek. Feltételezhetjük azt, hogy a profi, a különböző hírszerző szolgálatok által ki- és továbbképzett szakemberek ennél is hatékonyabbak. Valószínűleg néhány apró adatmorzsa felhasználásával is össze tudnak rakni rólunk és az általunk őrzött objektumról egy használható képet. Elképzelhető, hogy komolyabb dolgokra is tudnak következtetni.

Összegzés

Tanulmányomban áttekintettem a kritikus rendszerelemek legfőbb jellemzőit, kialakulásuk rövid történetét. A kritikus infrastruktúrák alapvetően három fő típusra oszthatóak: az első típus biztosítja a nélkülözhetetlen javak előállítását, szállítását és a társadalom számára alapvető fontosságú szolgáltatások folyamatos elérhetőségét. A második típusú kritikus infrastruktúrák teszik lehetővé az egymással való összeköttetést és az együttműködés képességét. A harmadik típusú kritikus infrastruktúrák járulnak hozzá az ország köz- és külső biztonságának megteremtéséhez. Foglalkoztam az ezekre leselkedő fenyegetések fajtáival, amelyek lehetnek katasztrófajellegű események és ártó szándékú cselekmények. Rámutattam arra, hogy a kritikus infrastruktúrák védelme és működésének fenntartása a nemzetbiztonság szempontjából minden kormányzat meghatározó és létfontosságú feladata.

Megvizsgáltam a kritikus infrastruktúrák védelmére a 21. században létrejött szabályozást az Amerikai Egyesült Államok, az Európai Unió, az Észak-atlanti Szerződés Szervezete és Magyarország szempontjából.

Rámutattam arra, hogy a kritikus rendszerelemek védelmét esetenként a Magyar Honvédség is elláthatja. Ez a tevékenység megjelenik az Önkéntes Területvédelmi Tartalékosok feladatrendszerében is, összhangban a Magyar Honvédség Magyarország Nemzeti Katonai Stratégiájában megfogalmazott küldetésével. Az őrzés-védelmi feladat napjainkban egyáltalán nem egyszerű a néhány évtizeddel ezelőtt még egyáltalán nem létező nyílt információk elemzésével megvalósított hírszerzés miatt. Az így beszerzett adatok segítségével egy jól őrzött kritikus infrastruktúra elleni támadás is viszonylag egyszerűen megtervezhető, akár amatőrök számára is az interneten fellelhető különböző applikációk és a közösségi média használatával. Tanulmányomban az orosz–ukrán háborúból származó információk alapján rámutattam arra, hogy „egyszerű” civilek milyen hatékonyan támogathatják a hadseregek harcát, valamint hogyan igazolhatják vagy cáfolhatják a propaganda állításait az internet felhasználásával.

Felhívtam a figyelmet arra, hogy a kritikus infrastruktúra védelmével megbízott katonák is emberek, akiknek többsége minden bizonnyal használja a közösségi média felületeit. A katonák feladatba történő bevonása előtt fontos a közösségi média használatából eredő veszélyekre figyelmeztetni, és felkészíteni őket arra, hogy mire kell figyelniük. Elmagyarázni nekik az ebben az esetben őket (is) védő rendszabályokat, ismertetni a közösségi média felületein alkalmazható biztonsági beállításokat, ahogyan ez a külszolgálatokban érintett, különösen a veszélyes területeken szolgáló katonák esetében meg is történik.

Tehát a katonáink felkészítése során törekedni kell az információtudatosságra, mert az internetalapú nyílt forrású hírszerzési módokat csak így lehet kivédeni.

Sajnos az eddigiekben nem fordítottunk erre túl sok figyelmet. Valószínűleg nehéz lesz a katonák digitális lábnyomát olyan szintre hozni, ahol már nem túl nagy, de mégis használhatják a közösségi médiát önmaguk és az általuk védett objektumok veszélyeztetése nélkül. Mindezt elérni kizárólag csak oktatással és az internethasználat tudatos központi és önkorlátozásával lehet. A tanulmány bevezetőjében megfogalmazott hipotézisem, amely szerint a kritikus rendszerelemek védelme érdekében az azok őrzés-védelmét ellátó katonáinkat fel kell készíteni az internet és a közösségi portálok biztonságos használatára, igaznak bizonyult.

Felhasznált irodalom

A Kormány 1393/2021. (VI. 24.) Korm. határozata Magyarország Nemzeti Katonai Stratégiájáról

A Tanács 2008/114/EK irányelve (2008. december 08.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32008L0114&from=HR

Az Európai Parlament és a Tanács (Eu) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016L1148

Az 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

Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről

Az Észak-atlanti Szerződés. Online: www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=hu

Babos Tibor (2007): *The Five Central Pillars of European Security*. Brussels: NATO Public Diplomacy Division. Online: www.files.ethz.ch/isn/56271/07_Babos.pdf

Babos Tibor (2016): The First Critical Infrastructure Protection Research Project in Hungary. In Nádai László – Padányi József (szerk.): *Critical Infrastructure Protection Research*. Switzerland: Springer International Publishing, 1–22. Online: https://doi.org/10.1007/978-3-319-28091-2

Bányász Péter – Orbók Ákos (2013): A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. *Hadtudomány,* 23(e-szám), 188–209. Online: http://hdl.handle.net/20.500.12944/1371

Bognár Balázs – Bonnyai Tünde – Vámosi Zoltán (2019): *Kritikus infrastruktúrák védelme I.* Budapest: Dialóg Campus.

Bonnyai Tünde (2019): Történeti áttekintés. In Bognár Balázs – Bonnyai Tünde (szerk.): *Kritikus infrastruktúrák védelme I.* Jegyzet. Budapest: Dialóg Campus, 29–46. Online: http://hdl.handle.net/20.500.12944/12450

Critical Foundations – Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection. Washington DC, 1997. október 13. Online: www.fas.org/sgp/library/pccip.pdf

European Programme for Critical Infrastructure Protection. Online: https://eur-lex.europa.eu/legal-content/EN-HU/TXT/?from=EN&uri=LEGISSUM%3Al33260

Haig Zsolt – Kovács László (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. Budapest: NKE. Online: www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf

Magyar Honvédség Sipos Gyula 6. Területvédelmi Ezred. Online: https://honvedelem.hu/alakulat/magyar-honvedseg-sipos-gyula-6-teruletvedelmi-ezred.html

Mahadevan, Alex (2022): This College 'Nerd' Investigates the Ukraine War from the Digital Front Lines. *Poynter,* 2022. május 24. Online: www.poynter.org/reporting-editing/2022/the-intel-crab-twitter-ukraine-russia-war-osint-justin-peden/

Maslow, Abraham H. (1943): A Theory of Human Motivation. *Psychological Review,* 50(4), 370–396. Online: https://doi.org/10.1037/h0054346

Mógor Judit – Angyal István (2022): A létfontosságú rendszerek védelmére vonatkozó szabályozás fejlesztése. *Scientia et Securitas,* 3(2), 118–125. Online: https://doi.org/10.1556/112.2022.00102

Mógor Judit – Földi László – Solymosi József (2008) Lépések a kritikus infrastruktúra védelmének magyarországi szabályozása felé. *Hadmérnök,* 3(4), 15–27. Online: http://hadmernok.hu/archivum/2008/4/2008_4_mogor.pdf

Nagy Nikoletta (2022): Fotelkémek ezreit nevelte ki az orosz–ukrán konfliktus. *24.hu,* 2022. június 8. Online: https://24.hu/tech/2022/06/08/osint-nyilt-forrasu-megfigyeles-kemek-orosz-ukran-haboru-kozossegi-media/

NASA FIRMS: https://firms.modaps.eosdis.nasa.gov/map/#d:24hrs;@0.0,0.0,3.0z

NATO (2016): *Warsaw Summit Communiqué*. Online: www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

NATO (2021): *Brussels Summit Communiqué*. Online: www.nato.int/cps/en/natolive/news_185000.htm?selectedLocale=en

NATO (2022a): *Crisis management*. Online: www.nato.int/cps/en/natohq/topics_49192.htm

NATO (2022b): *NATO 2022 Strategic Concept*. Online: www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO (2023a): *NATO Crisis Management Exercise 2023 (CMX23)*. Online: www.nato.int/cps/en/natohq/news_212527.htm

NATO (2023b): *Resilience, Civil Preparedness and Article 3*. Online: www.nato.int/cps/en/natohq/topics_132722.htm

NATO (2023c): *Vilnius Summit Communiqué*. Online: www.nato.int/cps/en/natohq/official_texts_217320.htm

NATO Parliamentary Assembly (2007): *The Protection of Critical Infrastructures*. Online: www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/270/270907/270907jopling_en.pdf

NMHH (2024): https://nmhh.hu/cikk/245667/Az_online_mediater_kozonsege_2024_februar

Parker, Nick (2022): RUDE ARMY Randy Russian Soldiers Bombard Ukrainian Girls With Flirty Tinder Requests. *The U.S. Sun,* 2022. február 23. Online: www.the-sun.com/news/4757640/russian-soldiers-tinder-ukraine/

Portfolio (2024): Túl nagy sztárrá vált az oroszok új páncélos szörnyszülöttje, meg is lett az eredménye. *Portfolio,* 2024. április 10. Online: www.portfolio.hu/global/20240410/tul-nagy-sztarra-valt-az-oroszok-uj-pancelos-szornyszulottje-meg-is-lett-az-eredmenye-679615

Technokrata (2022): Az ukránok e-kormányzati appot is bevetnek az orosz hadsereg ellen. *Technokrata,* 2022. április 21. Online: www.technokrata.hu/app/2022/04/21/diia-e-kormanyzati-app-ukrajna/

The USA PATRIOT Act: Preserving Life and Liberty. Washington DC, 2001. október 26. Online: www.justice.gov/archive/ll/what_is_the_patriot_act.pdf

The White House (2003): *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*. Washington DC. Online: www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

Twitter: *IntelCrab*. Online: https://twitter.com/IntelCrab

Verma, Pranshu (2022): The Rise of the Twitter Spies. *The Washington Post,* 2022. március 23. Online: www.washingtonpost.com/technology/2022/03/23/twitter-open-source-intelligence-ukraine/

Zöld Könyv A Létfontosságú Infrastruktúrák Védelmére Vonatkozó Európai Programról. Brüsszel, 17.11.2005, COM(2005) 576 végleges.

Jogi források

23/2023. (XII. 19.) Szabályozott Tevékenységek Felügyeleti Hatóság rendelet az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásáról

25/2016. (XII. 22.) HM rendelet az egyes honvédelmi miniszteri rendeletek módosításáról

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról

2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról