NEMZETBIZTONSÁGI SZEMLE
10. évfolyam (2022) 4. szám 17–29. • DOI: 10.32561/nsz.2022.4.2

Szeleczki Szilveszter[1]

A kiberhírszerzés értelmezése és helye a nemzetbiztonságban[2]

Interpreting Cyber Intelligence and Its Position in National Security

A nemzetbiztonsági feladatokra világszerte meglehetősen nagy figyelem hárul a mindennapok során. A feladatokat végrehajtó szervezetek számára fontos a korszerű technológiai támogatás, valamint a kapcsolódó eljárások gyakorlati alkalmazhatósága. A kibertér megjelenésével a nemzetbiztonsági hírszerzési ágak határai kezdenek elmosódni. A kibertér sokrétű struktúrája a kiberhírszerzést és egyúttal a korábban meghatározott információsszerzési módszereket közös, interdiszciplináris területként teheti értelmezhetővé.

Kulcsszavak: *kiber, nemzetbiztonság, hírszerzés, információ, hálózatok*

National security is a major focus of attention in everyday life around the world. For the organisations that carry out these tasks, it is important to have state-of-the-art technological support and the ability to apply the relevant procedures in practice. With the emergence of cyberspace, the boundaries between the intelligence branches of national security are becoming blurred. The multifaceted structure of cyberspace can turn cyber intelligence and at the same time the previously defined methods of information gathering into a common, interdisciplinary field.

Keywords: *cyber, national security, intelligence, information, networks*

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem, e-mail: Szeleczki.Szilveszter@uni-nke.hu

[2] „Az Innovációs és Technológiai Minisztérium Kooperatív Doktori Program Doktori Hallgatói Ösztöndíj Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.”

Bevezetés a nemzetbiztonság elméleti alapjaiba

A nemzetbiztonsághoz kapcsolódó tevékenységek általános ismérve, hogy társadalmi jelentőségű érdekekből kiindulva fogalmazódnak meg közös célok és feladatok. A nemzetek kritikus infrastruktúrájának működését alapjaiban befolyásolja a nemzetbiztonság állapota.[3] A megfelelő biztonsági állapot elérése, fenntartása és fejlesztése természetesen folyamatos intézkedéseket igényel. A célok elérése érdekében nemzetbiztonsági szolgálatok végzik a rájuk szabott speciális feladatokat. Jelen dokumentumban a nemzetbiztonsággal kapcsolatos veszélyek és tevékenységek bevezetése mellett előtérbe kerül a nemzetbiztonsági szolgálatok strukturális elképzelése és a hírszerzés területének vizsgálata. E területek közé tartozik az úgynevezett kiberhírszerzés is, amely kiemelt jelentőségű. A hírszerzésnek tudományos szempontból többféle megközelítési módja létezik, mint például a jogtudomány, a hadtudomány vagy a rendészettudomány oldaláról való értelmezés. Kutatásomat hadtudományi megközelítéssel végzem, amely során releváns szakirodalmat használok fel, értve ez alatt a biztonsági stratégiákat, jogszabályokat és hadtudósok a témához kapcsolódó munkáit. A hadtudományi megközelítést indokoltnak látom, hiszen a katonai területen megjelenő hírszerzési ágakat ugyan a lehetőség szerint részletesen meghatározzák, viszont átfedések tapasztalhatók az értelmezésükben.

A vizsgálatok során kiemelten foglalkozom a kibertérrel mint új, közismerten kihívásokkal teli területtel és annak hírszerzéshez társított értelmezésével. A célom választ találni arra, miként értelmezhető a kiberhírszerzés és egyúttal annak a nemzetbiztonságban elfoglalt helyét is behatárolni. Az információs tér aspektusai rohamosan fejlődnek világunkban, és számos technológia támogatja őket. Manapság a legtöbb információ elektronikusan hozzáférhető, aminek köszönhetően a legtöbb embernek az információs tér vonatkozásában a digitális adatok, eszközök, rendszerek jutnak eszébe. A digitális rendszerek minden kétséget kizáróan sokat segítenek a polgári és a katonai infokommunikációs képességek elképzeléseinek modern megvalósításában. A nemzetbiztonsági berendezkedésben a hírszerzési eljárások, módszerek határvonalai kezdenek eltűnni, aminek a világszerte tapasztalható intenzív hálózatosítás és az ennek hatására létrejövő, nagy kiterjedésű kibertér megjelenése áll a hátterében. Egy nemzet biztonsági berendezkedése számos befolyásoló tényezőből áll, a kapcsolódó szervezetek megfelelő működtetésétől kezdve egészen az emberek biztonságtudatos napi rutinszerű tevékenységéig. Mindez kihat a kritikus infrastruktúrákra,[4] amelyeken belül például jelentős a honvédelmi célokat szolgáló katonai erők helyzete. Kulcsfontosságú a nemzetet érintő kihívások, kockázatok és fenyegetések elleni védelmi tevékenységek rendszerezése. Resperger István professzor publikációjában[5] megjelent gondolatával egyetértve elmondható, hogy a kihívások, a kockázatok és a fenyegetések a lehetséges veszélyek megnyilvánulási formáinak tekinthetők, amelyek hatással vannak egy adott régió, terület vagy nemzet hatalmi viszonyaira, befolyásolva a külső és belső nemzeti stabilitást.[6]

---

3 Várhalmi 2010: 75. e) pont.

4 Utalva itt a 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről 1-es mellékletében meghatározott ágazatokra.

5 Resperger 2016: 116–117.

6 Resperger 2018: 38.

A 21. századi információs társadalomban infokommunikációs hálózatok tömegei működnek digitális világunkban, amelyek kapcsán a funkcionális „élmény" mellett a hálózatok biztonságával is foglalkozni kell, hiszen dependens viselkedésükből kifolyólag a veszélyek globálisan jelentkezhetnek.

> „A hálózatok által átszőtt globális világ sosem volt olyan sebezhető, mint manapság. Ez a sebezhetőség a nyitottságból, a bonyolult technikai rendszerekből, az infokommunikációs rendszerektől való növekvő függésből, illetve az összefonódó és egymással összekapcsolt létfontosságú infrastruktúrákból eredeztethető. Egy olyan bonyolult, infokommunikációs rendszerekkel behálózott társadalomban és gazdaságban, ahol közel minden ügyünket a hálózaton keresztül intézzük, saját fejlettségünk csapdájába eshetünk."

– írja Haig Zsolt a biztonságtudatos szemléletmódot előtérbe helyezve, továbbá hangúlyozza, hogy

> „az információs társadalom és annak védelmi rendszere olyan számítógép-hálózatokkal átszőtt hálózatos rendszerek komplexuma, amelyben e rendszerek biztonságos működése kölcsönösen függ a többi rendszer működésétől. Ennek következtében a rendszer bármelyik súlyponti elemének információs támadása, vagy védelme nemzetbiztonsági kérdés, amely védelmi síkon kihat az egész társadalomra".[7]

A nemzetbiztonsági feladatok végrehajtásának szervezésében egyaránt fontos a katonai és polgári szolgálatok tevékenységi köreinek behatárolása és az együttműködési képességek meghatározása. A hírszerzés és különösen a kiberhírszerzés vonatkozásában aktuális és fontos e szolgálatok célirányos vizsgálata.

A nemzetbiztonsági szolgálatokról

A nemzetek a biztonságtudatos érdekeket szem előtt tartva nemzetbiztonsági szolgálatokat (működésük szerint polgári vagy katonai) hoznak létre, amelyek száma a nemzeti döntéshozók megítélésétől függően változó. A nemzetbiztonsági szolgálatok feladataikat jogi szabályok alapján végzik. Az alapvető nemzetbiztonsági tevékenységek közé a hírszerzési és az elhárítási feladatok tartoznak. Amerikában egy kifejezetten összetett szervezet, az úgynevezett Hírszerző Közösség (Intelligence Community, IC) működik, amelybe 18 szervezet tartozik. Magában foglal független (például a Központi Hírszerző Ügynökség [Central Intelligence Agency, CIA]), az Amerikai Védelmi Minisztérium alá tartozó (például Nemzetbiztonsági Ügynökség [National Security Agency, NSA]) és egyéb szervezeteket. A koalícióban részt vevő szervezetek szoros együttműködéseken alapulva végzik tevékenységüket. „Az IC küldetése, hogy időszerű, éleslátó, tárgyilagos és releváns hírszerzési információkat nyújtson a nemzetbiztonsági

[7] Haig 2007

kérdésekről és eseményekről szóló döntésekhez."[8] Az NSA a nemzeti és a NATO szövetségi követelményeknek megfelelően fejleszti képességeit.

> „A katonai műveletekhez hírszerzési támogatást nyújtunk a tevékenységeink által, amíg kiberbiztonsági személyzetünk, termékeink és szolgáltatásaink biztosítják, hogy a katonai kommunikáció és adatok biztonságban maradjanak, ne kerüljenek ellenfeleink kezébe. […] Emellett közös protokollokat és szabványokat állítunk fel, hogy a katonai erőnk biztonságosan oszthassanak meg információkat szövetségeseinkkel, a NATO-val és a koalíciós erőkkel szerte a világon. Az interoperabilitás a sikeres közös műveletek és gyakorlatok kulcsa."[9]

Hazánkban a nemzetbiztonsági szolgálatok a Magyar Kormány irányítása alatt működnek. Magyarország alaptörvénye szerint: „A nemzetbiztonsági szolgálatok alapvető feladata Magyarország függetlenségének és törvényes rendjének védelme, nemzetbiztonsági érdekeinek érvényesítése."[10] A magyar kormány a nemzetbiztonság gyakorlati céljából megalkotta két biztonságpolitikai dokumentumát, a *Nemzeti biztonsági stratégiát*[11] (NBS), valamint a *Katonai biztonsági stratégiát*[12] (KBS). Az NBS kiemelt jelentőséget tulajdonít a megfelelő döntéshozáshoz szükséges információk zavartalan, megbízható, időszerű, fuzionált szolgáltatására. „Hatékonyan kell működtetni a rendvédelmi szervek aktuális és releváns értesüléseinek koordinált felhasználása, valamint a kormányzati hírigények célirányos összehangolása érdekében kiépített információfúziós rendszert."[13] A katonai célok vezérfonalán meghatározott nemzetbiztonsági tevékenységek vonatkozásában a KBS a válságkezelő műveleteket helyezi középpontba, amelyek során különböző intenzitású fegyveres konfliktusok történhetnek. „A honvédelmi feladatok végrehajtását támogató nemzetbiztonsági tevékenység végzése során a jövőben is kiemelt hangsúlyt kell helyezni a hazai társszolgálatokkal, valamint a NATO és az EU-tagállamok hírszerző és elhárító szervezeteivel kialakított stratégiai együttműködés célzott, elsősorban az aktuális kihívások területén megvalósuló fejlesztésére."[14] A katonai és polgári szervezetek egyaránt felhívják a figyelmet a 21. században olyan aktuális kihívásokra, mint például a kibertérből érkező, új típusú támadások.

A hírszerzés szerepe a nemzetbiztonságban

Az előzőekben leírtak alapján a hírszerzés meglehetősen fontos (és szerteágazó) feladatkör a nemzetbiztonsághoz tartozó tevékenységek vonatkozásában. Először az ókorban vált fontossá, ugyan akkoriban a felderítést és a kapcsolódó híradást nem választották szét egymástól. „A felderítés vagy hírszerzés szervezett formában csak a római császárkor idején valósult meg, amikor a császári adminisztráció felismerte

8 Lásd: www.dni.gov/index.php/what-we-do
9 A szerző fordítása, lásd: www.nsa.gov/About/Mission-Combat-Support/
10 Magyarország Alaptörvénye (2011. április 25.) 46. cikk (3) bekezdés.
11 1163/2020 (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
12 1393/2021 (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról.
13 NBS 152. pont.
14 KBS 4.3. pont.

a kisebb-nagyobb rendszerességgel összegyűjtött információk taktikai és stratégiai jelentőségét."[15]

A hírszerzés fogalmi értelmezése

A hírszerzésnek sokféle meghatározása lehetséges. Mindenki számára elfogadható, hogy jelentéstartalma kapcsolatában valamilyen új adatról, új ismeretről, információról van szó. Alapvetően állami, közszolgálati tevékenységi körnek mondható, de a jelenkori információs társadalomban a technológiai lehetőségeknek köszönhetően a hírszerzés mára a kibertérben szabadon gyakorolható a jogi szabályok betartásával (lásd például ipari vagy gazdasági kémkedések). Maga a hír mint megszerzett információs tartalom gyűjthető, tárolható, feldolgozható és továbbküldhető. Érdekes, hogy a hír tartalmát tekintve bizonyos értelemben függ és nem is függ az időtől. Nem függ, hiszen a hír egyaránt szólhat a közeli és távoli múltban bekövetkezett, a jelenleg zajló vagy éppen egy, a jövőben tervezett eseményről. Továbbá függ, hiszen a hír hatásmechanizmusát előtérbe helyezve a későbbi döntések miatt nagyon is lényeges az idő, pontosabban szólva a hír megszerzésének az ideje. Mindezekből adódik, hogy így vagy úgy a hírszerzés tervezési és szervezési folyamataiban fontos szerepe van az időnek.

Na de mit is jelent a hírszerzés mint közszolgálati tevékenység? A *Hadtudományi lexikon*ban a hírszerzés „az állam egyik funkciója, amelyet az eminens nemzeti érdekek érvényre juttatása és védelme érdekében, kizárólag erre a feladatra létrehozott, közvetlen kormányzati irányítás alatt működtetett szervezetek – speciális eszközöket és módszereket alkalmazva – végeznek titkos (bizalmas) és nyílt forrású információk beszerzésével".[16] Ahogy már arról szó esett, a hírszerzés képességét meghatározza, épp ezért fontos eleme a nemzetközi kapcsolatrendszer.

> „A politikai, katonai és gazdasági információk megvédése szükségessé teszik a korszerű és hatékonyan összehangolt hírszerző és elhárító képességek alkalmazását. A nemzetbiztonsági szolgálatok alapvető feladata, hogy különleges műveleti eszközeik és módszereik hatékony felhasználásával derítsék fel és akadályozzák meg a Magyarország nemzeti érdekeit leplezett formában veszélyeztető törekvéseket, illetve azonosítsák a törekvések hátterében álló állami, illetve nem kormányzati szereplőket. Napjaink biztonsági kihívásainak jelentős része globális és regionális jellegű, ezért a magyar nemzetbiztonsági szolgálatoknak – a nemzeti érdekek érvényesítésével, elsősorban a szövetséges államok irányában – hatékony nemzetközi partnerszolgálati együttműködést kell kialakítaniuk."[17]

A hírszerzés angol megfelelője az „intelligence", a NATO-terminológiában a következő olvasható a fogalom kapcsán: „A környezettel, a szereplők képességeivel és szándékaival kapcsolatos információk irányított gyűjtéséből és feldolgozásával létrejövő termék a veszélyek azonosítása és a döntéshozók általi kiaknázási lehetőségek felkínálása érdekében."[18]

---

15 Boda–Regényi 2019: 16.
16 Krajnc 2019: 446.
17 NBS 166. pont.
18 A szerző fordítása. NATO 2021: 69.

A hírszerzés célja, típusainak jellegzetes felosztása

Az előzőekben ismertetett, a hírszerzéshez tartozó meghatározások alapján kijelenthető, hogy a hírszerzés alapvető célja az információszolgáltatás. A hírszerzési célok és azok eléréséhez kapcsolódó tevékenységek hátterében jogi szabályok vannak. Magyarországon a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény szabályozza a hírszerzéssel szemben támasztott feladatokat, felelősségi köröket s vele a hírszerzés tevékenységrendszerét. „A nemzetbiztonsági szolgálatok belső szervezetét és működésének részletes szabályait, az utasításkiadás rendjét úgy kell meghatározni, hogy az egyéni felelősség mindig megállapítható legyen."[19] Fontos megemlíteni, hogy a jogi szabályozás következtében a hírszerzést végző emberek speciális, a feladatok végrehajtásához szükséges plusz jogokkal rendelkeznek (például a hírszerzéshez felhasznált eszközök használati engedélyei). A szakirodalom[20] szerint az információszerzési tevékenységek az alábbi jellegzetes hírszerzési ágakban valósulnak meg:

- emberi erőforrásokkal folytatott hírszerzés (HUMINT[21]);
- rádióelektronikai felderítés (SIGINT[22]);
- nyílt forrású hírszerzés (OSINT[23]);
- képfelderítés (IMINT[24]);
- mérés és jelmeghatározó hírszerzés (MASINT[25]);
- kiberhírszerzés (CYBINT[26]).

A felsorolásból kiemelkedik a kiberhírszerzés, hiszen e fogalom kapcsán a legtöbb ember számára egy kevésbé megfogható, konkrét határokkal nem rendelkező terület jelenik meg. A kibertér és a kibervédelmi kihívások a jelenkori modern világunkban meglehetősen aktuális és népszerű témák. A kibertér és ezáltal a kiberhírszerzés is interdiszciplináris területnek mondható, összetett jelentéstartalommal. Ahogy már a korábbiakban arról szó volt, a nemzetbiztonsági szolgálatok alapvető feladatköre a kihívások kezelése, amely kapcsán a kibertér szerepe is jelentős. A KBS egyértelműen hangsúlyozza, hogy a nemzetbiztonsági szolgálatok számára az információk hozzáférhetősége érdekében kiemelten fontos a nemzeti és nemzetközi kapcsolatok kiépítése és fenntartása.

> „Biztonságunk katonai dimenziójának másik pillérét a NATO által biztosított kollektív védelem alkotja, amelyet az Európai Unió (a továbbiakban: EU) Közös Biztonság- és Védelempolitikája, ezen belül a kölcsönös segítségnyújtási klauzula, továbbá az Egyesült Nemzetek Szervezete (a továbbiakban: ENSZ) és az Európai Biztonsági és Együttműködési Szervezet (a továbbiakban: EBESZ) keretében működő együttműködési fórumok egészítenek ki."[27]

19 1995. törvény a nemzetbiztonsági szolgálatokról 26. §.
20 Resperger 2018: 119.
21 Human intelligence, HUMINT.
22 Signal intelligence, SIGINT.
23 Open source intelligence, OSINT.
24 Imagery intelligence, IMINT.
25 Measurement and signature intelligence, MASINT.
26 Intelligence gathered from cyberspace, CYBINT.
27 KBS Bevezető rész.

A kiberhírszerzés meglehetősen ingoványos területként értelmezhető, éppen ezért a következőkben e hírszerzési ágat részletesebben értelmezzük, megítélve egyúttal a nemzetbiztonságban elfoglalt lehetséges helyét is.

A kiberhírszerzésről mint kiemelt területről

A kiberhírszerzés egy meglehetősen tág jelentéstartalommal rendelkező fogalom. A kiberhírszerzés egyik alapvetése, hogy hasonlóan a többi hírszerzési ághoz, információ gyűjtése és későbbi feldolgozása valósul meg. A másik már specifikusabb alapvetés, hogy jelen esetben a tevékenységek a kibertérben történnek, és itt érdemes is megállni egy pillanatra. Mit is jelent ez pontosan? Számos meghatározás született már annak megértésére, hogy mi is a kibertér, amelyben jelen esetben hírszerzési tevékenységek hajtódnak végre. A kiberhírszerzés értelmezésére jelenleg nehéz pontos leírásokat találni, hiszen a kibertér értelmezése sem mondható könnyen körülhatárolt területnek. A következőkben a kiberhírszerzés elméleti megközelítésű vizsgálatához a kibertér fogalmi értelmezéséről és struktúrális felépítéséről lesz szó, amelyekből származtatva a kiberhírszerzés is könnyebben körvonalazhatóvá, érthetővé válik.

A kibertér értelmezése

Magyarország Nemzeti Kiberbiztonsági Stratégiájában a következő olvasható a kibertér Magyarországi környezete vonatkozásában:

> „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett."[28]

A megfogalmazásból egyértelműen kiragadható, hogy elektronikus információs rendszerekről esik szó, továbbá azok kapcsolódási viszonyairól. Az említett fogalmat és sok egyéb szempontot is vizsgálva Haig Zsolt a kibertér alatt a következő meghatározást írja:

> „A kibertér az ember által mesterségesen létrehozott, dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot."[29]

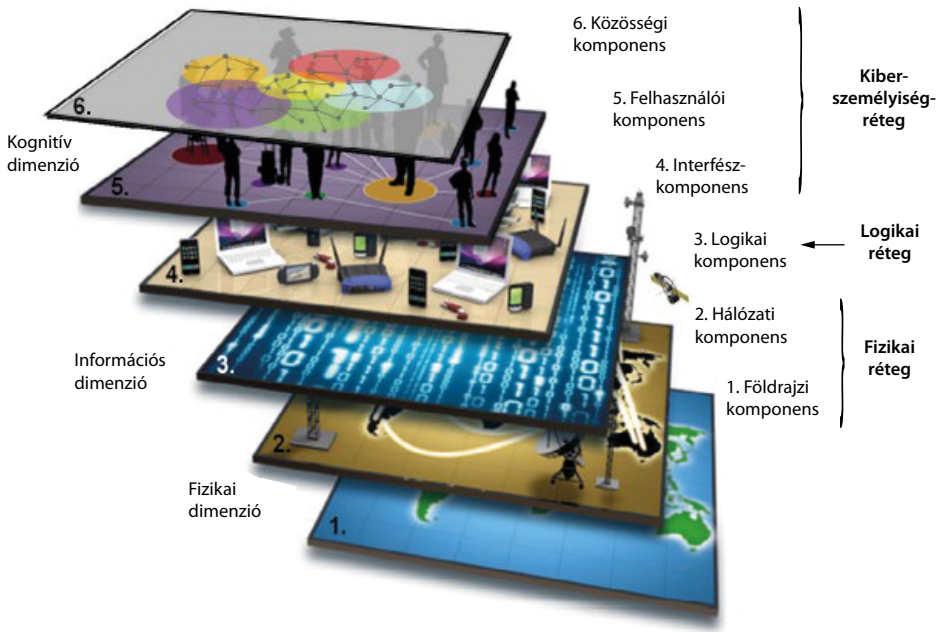
[28] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, II. pont.
[29] Haig 2018: 226–227.

Egyetértve Haig megfogalmazásával, több olyan kulcsszó is elhangzott, amely a kibertér strukturális sémáját érinti, ilyenek többek között a globális, hálózat, elektromágneses spektrum, mesterséges, dinamikusan változó tartomány, infokommunikációs rendszerek. A megfogalmazásban szó esik az információval végzett négy alapműveletről, a hálózatosított infokommunikációs rendszerekről, továbbá az elektromágneses spektrumot is felhasználó, változó környezetről.

A kiberbűnözésről, a kiberterrorizmusról a legtöbb embernek a számítógépes hálózat jut eszébe (például a hekker vagy hekkercsoport behatol egy állami információs rendszerbe), azaz valaki (általában szervezeti megbízásból) egy számára biztos helyről kapcsolódik számítógépes rendszerekre. Mindettől függetlenül a kibertér struktúrája nem csupán ezt tartalmazza. Nyilvánvalóan nehéz azt megállapítani, hogy hol a határa egy dinamikus változó környezetnek, amely számos képességet ölel fel.

Mindezek alapján vetődik fel a kérdés, hogy a korábban felsorolt hírszerzési ágak, az emberi erőforrásokkal folytatott hírszerzés, a rádióelektronikai felderítés, a nyílt forrású hírszerzés, a képfelderítés, a mérés és jelmeghatározó hírszerzés nem tartozhatna-e bele akár mind-mind a kibertéri műveletekbe, tekintettel a sokrétű kapcsolódódási pontra?

A kibertér elméleti megközelítésű struktúrája alapján különböző rétegek és dimenziók szerepelnek egy változó tartományban, amelyet az 1. ábra szemléltet. Különböző komponensek vannak három főbb, a fizikai, logikai és az úgynevezett kiberszemélyiségi rétegben meghatározva.



1. ábra: A kibertér struktúrája
Forrás: Haig 2018: 230.

A rétegek definiálása kapcsán a következő olvasható:

> „A fizikai réteg földrajzi és hálózati komponensekből áll. A földrajzi komponens a hálózat hardverelemeinek és infrastruktúrájának földrajzi elhelyezkedésére vonatkozik, ugyanis a korábbi meghatározás szerint a kibertér alapvetően a természetes földrajzi környezetben, az ember által mesterségesen létrehozott tartomány. A hálózati komponens a hálózat hardver-alkotóelemeinek és infrastruktúráinak fajtáját, típusát mutatja meg. Ezek közé tartozhatnak többek között a szenzorok, adattároló központok, szerverek, routerek, vezetékek, optikai kábelek, rádiófrekvenciás adatátviteli eszközök, mobil cellás bázisállomások, műholdas eszközök stb., de idetartozik az elektromágneses spektrum is mint a vezeték nélküli hálózati kommunikáció fizikailag definiálható tartománya. A logikai réteg a hálózat virtuális tere, amely alapvetően a kibertér fizikailag nem megfogható elemeit tartalmazza. A logikai réteg elemei lehetnek a hálózatban kezelt információk, átviteli és címzési protokollok, szoftveralkalmazások, hálózati szolgáltatók és felhasználók adatai, internetes domainnevek, információbiztonsági megoldások stb. A kiberszemélyiség rétege interfész-, felhasználói, illetve közösségi komponensekből áll. Ez jelenti a hálózat felhasználóinak digitális reprezentációját a kibertérben."[30]

A kiberhírszerzés[31] *(CYBINT) értelmezése*

A korábban említett, a *Hadtudományi lexikon* által megfogalmazott definíció alapján kiemelendő, hogy a hírszerzés kormányzati irányítás alatt van, valamint speciális eszközöket és módszereket tartalmaz. A kiberhírszerzés rendeltetése vonatkozásában a következő olvasható:

> „A CYBINT a célország vagy a célszervezet számítógépes hálózatain tárolt információk megszerzésére irányul. A CYBINT-nek alapvetően három fajtája van: a nyílt számítógépes hálózatokban védett információk megszerzése, a zárt (védett) számítógépes hálózatokban lévő információk megszerzése, valamint a számítógépes hálózatok által kisugárzott jelekből folytatott adatszerzés."[32]

Mindezek alapján a meghatározás kifejezetten a számítógépes hálózatokra összpontosuló tevékenységekre utal. Bizonyosan elfogadható, hogy ez a szemlélet tartalmazza az elektronikus információs rendszert és a kapcsolódó globális hálózatokat (a különböző országon belüli és határon túli kapcsolatokat). Ami viszont hiányolható, az az infokommunikációs rendszerek képességéből ered, amely nem csupán informatikai, hanem kommunikációs eszközökből áll (utalva például az elektromágneses spektrum széles tartományára). A kiberhírszerzést annak fogalmi tisztázásának érdekében célszerű összevetni a kibertér struktúrájával és fogalmával. A korábban bemutatott kibertérstruktúra alapján azt lehet mondani, hogy a kiberhírszerzés gyakorlatilag

30 Haig 2018: 231.

31 A szakirodalomban egyaránt találkozhatunk az angol „cyber intelligence" és a „cyber threat intelligence" kifejezésekkel. Utóbbi nevezhető a gyakrabban használtnak, amely alapvető eleme a kiberbiztonságnak.

32 Resperger 2018: 121–122.

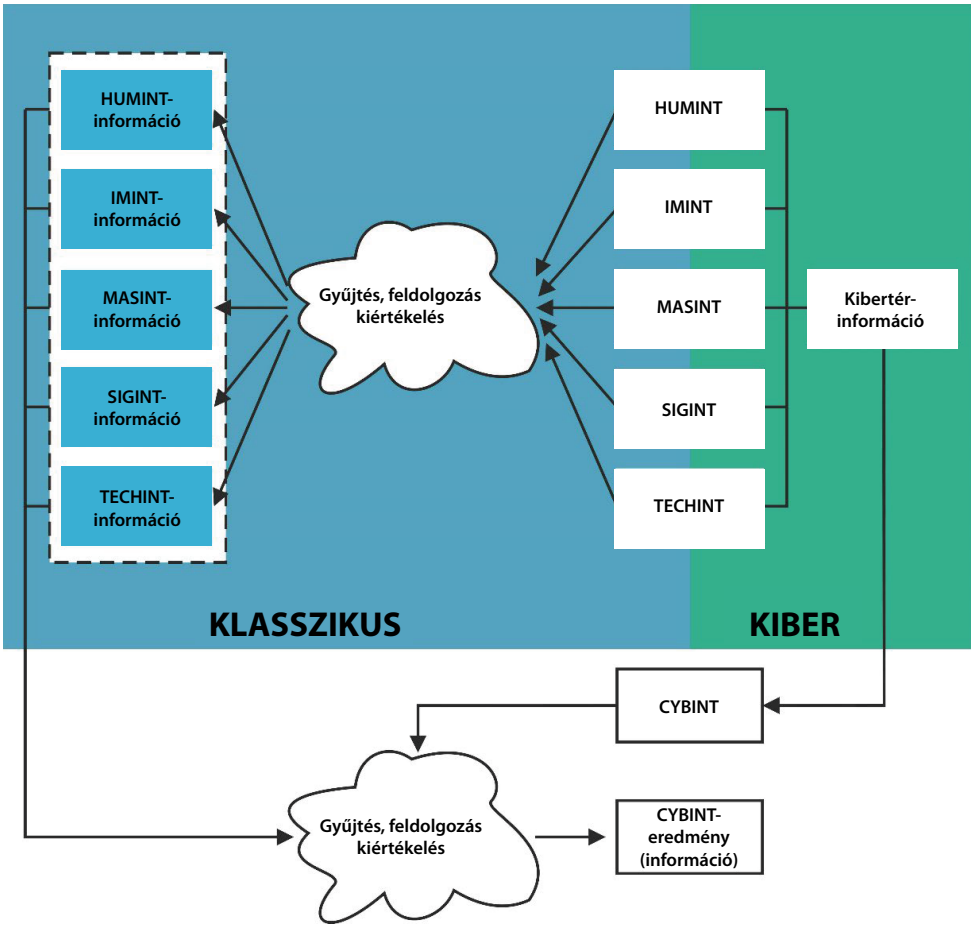
minden rétegben értelmezhető. A számítógépen alapuló hálózatoknak vannak fizikai, logikai és kiberszemélyiségi aspektusai is. A kibertér a korábban említett fogalmakból kiindulva meglehetősen összetett, globális hálózatként értelmezhető, amely sokrétű, ember és gép (hírszerzési tevékenységben gondolkodva mondhatni inkább ember és az információt tartalmazó környezet) közötti interakciókat foglal magában. A szakirodalomban a kiberhírszerzést három típusra osztják fel:

- technikai hírszerzés (például hírszerző hardverek, szoftverek vizsgálatai);
- taktikai hírszerzés (például szervezetek hírszerző tervezési eljárásai);
- műveleti hírszerzés (például szervezetek információs szolgáltatásai);
- stratégiai hírszerzés (például egy ágazat tevékenységeinek elemzése).[33]

Visszatekintve a klasszikus hírszerzési ágakra a következők mondhatók el: Az emberi erőforrásokkal végrehajtott hírszerzés esetén egyértelmű, hogy a kibertérben végzett műveleteket is emberek vagy az emberek által irányított gépek végzik. A rádióelektronikai felderítés szintén kapcsolható a kibertérhez, hiszen szó volt arról, hogy a kibertérbe az elektromágneses hullámtartományban végzett műveletek is beletartoznak. A nyílt forrású hírszerzés a kibertér azon elemeihez köthető, amelyek könnyebben hozzáférhető (például nem titkos) információkat tartalmaznak. A képfelderítéshez elektronikus információs rendszer kell, úgyhogy megint csak kapcsolódik a kibertérhez. A mérés és jelmeghatározó hírszerzés az elektromágneses spektrumot használja fel, így ez a hírszerzési ág is illeszkedik a kibertér struktúrájába. Itt tehát számos kapcsolódási pont van, épp ezért vetődik fel még egy újabb kérdés: Érdemes lenne a CYBINT-képességre globális, többkomponensű hírszerzési tevékenységből származó produktumként tekinteni mint eredményre? A következő, 2. ábra jól szemlélteti, hogy a kiberhírszerzés felfogható mondhatni „összes forrásból származó" hírszerzésként.

Ennek előnye, hogy nincs szükség arra, hogy kötelezően meg kelljen szabni a határokat (a hírszerzési ágak informális fuzionálása történik) a kibertér kapcsán, amely folyamatosan változik, fejlődő technológiai kihívásokat tartalmazva. Hátránya viszont, hogy a „minden mindennel összeér" elvén szükségtelenné válhatnak a tradicionális hírszerzési ágak meghatározásai. Ennek ellenében érdemes a kiberhírszerzésre mint kibertérből származó információszerzésre és vele kibertéri produktumra, eredményre tekinteni. Ugyanezen szemlélethez tartozhat, hogy amilyen eszközöket és rendszereket használtak az eredmény (az információ) eléréséhez, meg lehet állapítani, hogy mely klasszikus hírszerzésnek köszönhető a sikeres információszerzés. A számítógépes hálózatokon keresztüli hírszerzésnek külön ágát is célszerű definiálni (például INFINT mint informatikai hírszerzés) azzal párhuzamban, hogy a kiberhírszerzést kiemeljük. Végső eredményként a kiberhírszerzés (és vele a kiberelhárítás is) átfogó, közvetlen helyet foglalna el a nemzetbiztonság mindennapos feladataiban.

[33] Flashpoint Team 2022



2. ábra: A CYBINT mint összadatforrású hírszerzés
Forrás: a szerző szerkesztése Seedyk 2018: 4. ábra alapján

Összegzés

A nemzetbiztonságot érintő kihívások, kockázatok és fenyegetések vonatkozásában nélkülözhetetlenek a magas szintű tervezési és szervezési folyamatok, amelyek a mindennapokban megjelenő biztonságtudatos munkavégzést teszik elérhetővé. A nemzetbiztonsági szolgálatoknak lehetőség szerint a mindenkori legkorszerűbb infokommunikációs eszközökkel és rendszerekkel kell rendelkezniük annak érdekében, hogy a velük szemben támasztott követelmények megvalósuljanak, s ezzel biztosítsák a nemzeti érdekeket. A hírszerzés feladatkörét kiemelve egyértelműen azt tapasztaltam, hogy e feladatkörrel kapcsolatos értelmezések számos változáson mentek

keresztül. A hírszerzés minősége egyértelműen függ a hírszerzési tevékenységben felhasználható információs rendszerek és a működtető személyzet képességétől.

„A jó hírszerzés azt jelenti, hogy valaki a lényegtelen adatok óriási halmazában is meglátja a szándékosságot, majd pedig mindezeket a különálló információkat a várható történésekre vonatkozó koherens előrejelzésekké alakítja."[34] A hírszerzési ágak meghatározásai meglehetősen változatosak. Sokrétűsége miatt különböző elképzelések fogalmazódnak meg. A katonai klasszikus hírszerzési ágak meghatározásain alapulva a megfelelő módszerrel végrehajtott hírszerzés során az adatok, információk megszerezhetők.

> „Nem minden információigény megválaszolása követeli meg az összes adat- és információszerzési eljárás alkalmazását, mert a hírszerzés képességeinek hatékony felhasználása érdekében egy adott információigény esetén csak azokat a módszereket alkalmazzák, amelyek biztosítják a szükséges adatok, információk megszerzését. A hírszerzési ágak különböző jellegű adatok, információk begyűjtésére alkalmazhatók. Ennek következtében a hírszerzés sikerét befolyásolja, hogy a hírszerző szolgálat mely adat- és hírszerzési módo(ka)t választja ki a szükséges adatok, információk megszerzésére."35

A kiberhírszerzés meghatározása meglehetősen új kihívás, hiszen a kibertér definíciójából következően nyitott kérdések fogalmazódnak meg gondolatban. A kibertér dinamikusan változó tartomány, meglehetősen sok képességet tartalmaz, épp ezért a kiberhírszerzést is ennek megfelelően érdemes vizsgálni és értelmezni. A nemzeti szintű kiberbiztonság érdekében a kibervédelmi tevékenységeket is meghatározzák. Ahogy azt Kovács László is említi, a kiberhírszerzés önálló területként jelenik meg a nemzeti kiberbiztonsági stratégiában.[36]

Mindezek alapján kijelenthető, hogy a kiberhírszerzés beillesztése a klasszikus hírszerzési ágakba nehéz feladat. A számítógépes hálózatokon keresztül zajló hírszerzés minden bizonnyal a kibertérben zajló tevékenységek közé sorolható. A kiberhírszerzés meghatározása viszont véleményem szerint ennél magasabb szintű értelmezést kíván. A kiberhírszerzést nem feltétlenül lehet a klasszikus hírszerzési ágak közé sorolni, helyette inkább a kibertér és a kibertérből érkező információkat újfajta szemlélettel célszerű vizsgálni. A klasszikus hírszerzési ágak gyakorlatilag mindegyike érinti a kiberteret, így bármelyik módszer eredménye kibertérből érkező információként is értelmezhető. A jövőben a kiberhírszerzés és az összes forrásból származó információ jelentéstartalma összefonódhat, amivel a kibertér változó környezete is hasonul a kiberhírszerzés definíciójához. A kiberhírszerzés nemzetbiztonságban elfoglalt helye pedig egyértelműen változhat a jövőben esedékes új technológiai kihívások tükrében.

---

34 Bruce Schneier idézete (Németh Ádám fordítása). Lásd: www.citatum.hu/idezet/90234
35 Dobák 2014: 121.
36 Kovács 2018: 82.

Felhasznált irodalom

Boda József – Regényi Kund szerk. (2019): *A hírszerzés története az ókortól napjainkig.* Budapest: Dialóg Campus

Dobák Imre szerk. (2014): *A nemzetbiztonság általános elmélete.* Budapest: Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet

Flashpoint Team (2022): Guide to Cyber Threat Intelligence: Elements of an Effective Threat Intel and Cyber Risk Remediation Program. *Flashpoint.io,* 2022. február 22. Online: https://flashpoint.io/blog/guide-to-cyber-threat-intelligence/

Haig Zsolt (2007): Az információs társadalmat fenyegető információalapú veszélyforrások. *Hadtudomány,* 17(3), 37–56.

Haig Zsolt (2018): *Információs műveletek a kibertérben.* Budapest: Dialóg Campus

Kovács László (2018): *Kiberbiztonság és stratégia.* Budapest: Dialóg Campus

Krajnc Zoltán (2019): *Hadtudományi lexikon.* Budapest: Dialóg Campus

NATO (2021): *AAP-06 Edition 2021. NATO Glossary of Terms and Definitions.* NATO Standardization Office

Resperger István (2016): A biztonsági környezet, az aszimmetrikus hadviselés és a terrorizmus jellemzői. *Hadtudományi Szemle,* 9(3), 115–181. Online: https://bit.ly/3DfEC3f

Resperger István szerk. (2018): *A nemzetbiztonság elmélete a közszolgálatban.* Budapest: Dialóg Campus

Seedyk, Christopher (2018): Characterizing Cyber Intelligence as an All-Source Intelligence Product. *Defense Systems Information Analysis Center,* 2018. november 2. Online: https://dsiac.org/articles/characterizing-cyber-intelligence-as-an-all-source-intelligence-product/

Várhalmi A. Miklós (2010): *A nemzetbiztonsági szolgálatok meghatározó jelentősége a Magyar Köztársaság XXI. századi biztonsági rendszerében.* PhD-disszertáció. Budapest: ZMNE. Online: https://bit.ly/3DdyE2M

Jogi források

Magyarország Alaptörvénye (2011. április 25.)

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

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

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

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