Rémai Dániel✧

Izraeli válaszok napjaink kibervédelmi és kiberhadviselési kihívásaira

DOI 10.17047/HADTUD.2022.32.4.3

A kiberbiztonság és a kibervédelem napjainkban megkerülhetetlen tényezők, ha egy ország általános biztonságát vizsgáljuk. A tanulmány Izrael Állam vonatkozásában tekinti át a kiberbiztonság és a kibervédelem fogalmának megjelenését, változását és ennek hatását a zsidó állam nemzeti biztonsági koncepciójára. Vizsgálja továbbá a kapcsolódó intézményi struktúrát, fókuszálva a nemzetbiztonsági szolgálatok szerepére és megváltozott feladataira.

A kiberstratégia és az operatív feladatvégrehajtás a kibertérben Izrael esetében pontosan olyan, mint számos egyéb szektor az országban: egyszerre kaotikus, ugyanakkor hatékony. Az Izrael által, az elmúlt negyed évszázadban a kibervédelem és kiberhadviselés terén bejárt út példaértékű, ugyanakkor megismételhetetlen. Elemzésem ennek az útnak a bemutatására vállalkozik.

KULCSSZAVAK: kiberbizonság, kibertámadás, aszimmetrikus hadviselés, Izraeli Védelmi Erők, nemzetbiztonság

Israeli Responses to Today's Cyber Defence and Cyber Warfare Challenges

When examining the security of a country, cyber security and cyber defence are indispensable factors. The article reviews the emergence and change of the concept of cyber security and cyber defence in relation to the State of Israel and their impact on the national security concept of the Jewish State. It also analyses the related institutional structure, roles and changed tasks of national security services. Overall, cyber strategy and operational task execution in cyberspace for Israel is similar to everything else there: they are chaotic but very effective at the same time. The way Israel has taken in the last decades in cyber defence and cyber warfare is exemplary and unrepeatable. The article would like to illustrate this path.

KEYWORDS: cyber security, cyberattack, asymmetric warfare, Israeli Defence Forces, national security

✧ A Nemzeti Közszolgálati Egyetem Terrorelhárítási Tanszékének munkatársa;
NKE Hadtudományi Doktori Iskola, hallgató – *National University of Public Service (NUPS) Department of Counterterrorism, Student of the NUPS Doctoral School of Military Sciences;*
ORCID: 0000-0002-5664-0977 e-mail: remai.daniel@tek.gov.hu

„A kiberbiztonság sokkal több, mint informatikai kérdés."[1]
Stephane Nappo

Bevezetés

A hagyományos biztonságfelfogás, amely szerint a biztonság nem más, mint a fenyegetettség hiánya, a mai napig megállja a helyét.[2] A biztonságot befolyásoló tényezők rendszere az elmúlt évtizedekben jelentős változásokon esett át. A hagyományos kihívások, kockázatok és fenyegetések nem tűntek el, hanem kiegészültek új, korábban ismeretlen dimenziókkal. A lokális és globális szinten komplexebbé, zavarosabbá, nehezebben átláthatóvá váló biztonsági környezet eszkalálódása még korántsem ért el a csúcsra, hiszen a korábban már létező kihívások, kockázatok, fenyegetések folyamatosan fennállnak és transzformálódnak, míg ezzel párhuzamosan új kihívások jelennek meg.

A technológia fejlődése, az infokommunikációs eszközök széleskörű elterjedése, az IT-infrastruktúra szerteágazó expanziója alapjaiban határozza meg a modernkori biztonsági rendszereket, a globális és nemzeti biztonsági struktúrákat. A technológiai fejlődés az élet szinte minden területén változásokat indukál: a terrorizmustól, a hagyományos katonai kihívásokon keresztül, az új típusú fenyegetettségekig érezteti hatását ez a fejlődés. Szakmai szemszögből szemlélve a társadalom technológiai evolúciója mind a felderítés, mind a „támadás" (végrehajtás), mind az elhárítás területén új kihívásokat, új feladatokat, új szemléletek és módszerek megjelenését indukálta a nemzetbiztonsági szolgálatok működésében.[3] A folyamatos változás alapvető koncepcióváltásra kényszeríti az egyes országok nemzetbiztonsági szolgálatait, rendvédelmi és katonai szervezeteit, új feladatok elé állította a nemzeti biztonsági stratégiák és törvényi szabályozások tervezésével foglalkozó szakembereket, valamint magát a civil szférát is, a polgári lakosságtól egészen a gazdasági szektorok minden szereplőjéig.

A mindennapi élet számos szegmensének áthelyeződése az online térbe korábban elképzelhetetlen változásokat hozott, amelyeket a koronavírus-járvány tovább erősített. Az átlagos felhasználó szintjén az elmúlt években tendenciózus növekedésnek indult a piaci és állami szolgáltatások áthelyeződése a virtuális térbe. Az állam számos tevékenysége, az állami és piaci rendszerek és alrendszerek működésének egyre több szegmense is az online térbe tolódott, amely folyamatot a Covid19-járvány szükségszerűségei tovább erősítették. Ezek a változások legtöbb esetben megelőzték a törvényi és technológiai védelmi mechanizmusok precízen tervezett felépítését. A nemzeti és magán adatvagyonok védelme, az online térben folyó tevékenységek biztosítása kiemelt és mindennapos kérdéssé vált. A technológia forradalma, az online tér tündöklése mellett felerősödtek a már létező, és megjelentek új kihívások is, amelyek megoldása nemzeti vagy akár nemzetközi szintű együttműködést követel

1 https://medium.com/@romadantivirus/cyber-security-is-much-more-than-a-matter-of-it-a02f724618e6 (Letöltés ideje: 2021.04.12.)

2 Gazdag – Remek 2018, 282.

3 Dobák – Kovács 2014.

l világszerte. A kibervédelem kérdése az elmúlt években a nemzeti biztonsági stratégiák kiemelt elemévé vált, és megjelentek az önálló nemzeti kiberbiztonsági stratégiák is.[4]

A változások nem kerülhették el a nemzetbiztonsági szolgálatokat sem. E szervezetek számára a technológiai innovációk megjelenése és széles körben történő elterjedése egyrészt új feladatok megjelenését jelentette, hiszen a kihívások és fenyegetések megváltozott rendszerében kell helyt állniuk. Ezzel párhuzamosan számos új lehetőség számára is utat nyitott, hiszen kiaknázhatják az online tér nyújtotta információszerzési lehetőségeket, sőt napjainkban már nem hangzanak tudományos-fantasztikumnak az online térben végrehajtott katonai vagy titkosszolgálati műveletek sem.[5]

Az elmúlt évtizedekben az online tér jelentősen kibővült, és ezzel párhuzamosan bontakozott ki az ott folyó folyamatos és egyre grandiózusabb háború, ahol az egyes szereplők információt igyekeznek szerezni, befolyásolni akarnak bizonyos személyeket, eseményeket, vagy konkrét támadások végrehajtásával rendszerek működését kívánják megváltoztatni. Ez a háború azonban nyomokban sem emlékeztet a hagyományos hadviselésre, a szembenálló felek nem feltétlen viselnek egyenruhát, kilétük, szándékaik, olykor tevékenységük is rejtve marad. Mára azonban tudjuk, hogy az online térben zajló összecsapások akár nagyobb mértékű veszélyt is hordozhatnak, és jelentősebb pusztítással járhatnak, mint a hagyományos hadviselés eszközei. Az eszközök tárháza hihetetlenül széles körű, a műveleti terület pedig szinte végtelen, mondhatni egy teljesen új univerzum áll rendelkezésre ezen összecsapások végrehajtására. Az emberiség által az online térben létrehozott világ túlmutat önmagán, és a virtuális téren kívül is hatással van életünkre. Ahogy Stephane Nappo is fogalmaz – a tanulmány mottójának választott idézetben – ma már tudjuk, hogy a „kiberbiztonság sokkal több, mint informatikai kérdés".

Izraelről számos dolog juthat az olvasó eszébe, egyre azonban biztos nem asszociálna: mégpedig, hogy a zsidó állam a béke szigete. Izrael Államot alapvető társadalmi, gazdasági, vallási, etnikai, világnézeti és gondolkodásmódbeli különbségek választják el a régió többi államától.[6] Már az állam megalakítása előtt léteztek azok a törésvonalak a Palesztin Mandátum területén elő arab és zsidó közösség között, amelyek a mai napig meghatározzák Izrael régióban elfoglalt helyét és szerepét, determinálják a zsidó állam modernkori történelmét. A folyamatos konfliktusok világa ez, ahol a generációkon átívelő ellenségeskedés intenzitása nem változik, de az alkalmazott módszerek tárháza folyamatos „fejlődésen" megy keresztül. Éppen ezért nem meglepő, hogy az új típusú fenyegetések kivédése területén, valamint az új típusú védelmi és támadó rendszerek alkalmazásában Izrael élén jár biztonsága szavatolása érdekében.

Tanulmányomban Izrael Állam vonatkozásában kívánom vizsgálni a kiberbiztonság és a kibervédelem fogalmának megjelenését, változását és annak hatását

4 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx (Letöltés ideje: 2021.04.12.)

5 https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (Letöltés ideje: 2021.04.12.)

6 Rémai 2020a.

a zsidó állam nemzeti biztonsági koncepciójára. Vizsgálom továbbá a kapcsolódó intézményi struktúrát, fókuszálva a nemzetbiztonsági szolgálatok szerepére. A tanulmány keretei között a folyamatosan változó biztonsági környezetben fejlődő kibervédelmi és kiberhadviselési képességek bemutatásával az a célom, hogy ismertessem azokat a pilléreket, amelyekre építve Izrael napjaink egyik meghatározó erőközpontja a kibertérben.

Az izraeli biztonsági koncepció fejlődése

A zsidó és az arab népcsoportok közötti ellenségeskedés már az Izrael Állam megalakulása előtti időkben is alapjaiban határozta meg a Jisuv[7] területén élő közösségek védelmi tervezését. Az 1900-as évek elejétől egészen az 1948-as első arab–izraeli háborút követő időkig az izraeli védelmi tervezés fő célja a területen élő zsidó népesség túlélésének biztosítása volt. Az Izraeli Védelmi Erők (IDF) és a belbiztonsági szolgálatok fejlesztésével lassan és fokozatosan a zsidó állam stratégiai előnyre tett szert a régiós ellenfeleivel szemben. Napjainkra ez az előny olyan mértékű, hogy lehetővé vált Izrael számára a régió más országaiba történő beavatkozás, gondoljunk csak az iráni nukleáris létesítmények ellen elkövetett támadásokra, szabotázsokra[8], vagy az IDF által szinte rendszeresnek mondható, Szíriában végrehajtott – hivatalosan meg nem erősített – támadásokra[9]. Éppen ezért napjaink izraeli védelmi tervezésének „fő irányvonala, hogy Izraelnek meg kell őriznie relatív előnyét az ellenségeivel szemben, és fejlesztenie kell nemzetközi kapcsolatait. Benjamin Netanjahu felfogásában az izraeli biztonság négy fő pilléren nyugszik: (1) katonai, (2) gazdasági, (3) politikai és (4) társadalmi alapokon".[10] A Netanjahu miniszterelnök kezdeményezésre 2017-ben készített új izraeli nemzeti biztonsági stratégia a katonai pillér esetében a Ben Gurion-i hármas felosztáshoz nyúl vissza: (1) az elrettentés, (2) a korai figyelmeztetés és (3) a támadó-védekező erő mellé új elemként került be (4) a védekező erő fogalma.[11]

Az izraeli nemzeti biztonsági koncepció alapja a különböző pillérek együttműködése. Ennek egyik ékes példája a gazdasági szektor és az IDF együttműködése, amely fontos pillére volt annak, hogy évtizedek alatt az izraeli védelmi ipar a világ élvonalába emelkedett. Izraelben a rendelkezésre álló természeti és gazdasági erőforrások szűkössége jelentős mértékben hozzájárult ahhoz, hogy az 1930-as évektől kezdve, a kutatás-fejlesztési (K+F) tevékenység, és annak állami patronálása folyamatosan magas szintű volt.[12]

Izrael 2014-ben az OECD-országok között második helyen állt a kutatás-fejlesztésre fordított összeg tekintetében, az éves GDP 4,1%-át ezen a területen költötték el.[13]

---

7 A Palesztin Mandátumterület korabeli héber elnevezése.

8 Langner 2011.

9 https://www.facebook.com/syriahroe/photos/a.150495128392167/3261644330610549/ (Letöltés dátuma: 2021.04.12.)

10 Rémai 2020b.

11 Ben Gurion 1970.

12 Rémai 2021.

13 Housen-Couriel 2017.

A K+F szektor kiemelt támogatása évtizedekre nyúlik vissza és ezek a folyamatok vezettek el oda, hogy napjainkban Izraelt startup nemzetként is emlegetik: a zsidó állam élen jár az új technológiák, infokommunikációs és informatikai eszközök és rendszerek fejlesztésében.[14] Éppen ezért nem meglepő, hogy a kibervédelem és kiberbiztonság kérdésköre már viszonylag korán, az 1990-es években, a „tech-éra" hajnalán megjelent az izraeli védelmi tervezés legmagasabb szintjén is.

A kiberbiztonság helye és szerepe az izraeli biztonsági koncepcióban

Az 1973-as jom kippuri háborúban elszenvedett veszteségeket, a háborús konfliktust követően a vizsgálóbizottságok főleg a SIGINT[15] felderítés területén felmerülő hiányosságokban és hibákban látták.[16] Ezzel párhuzamosan a következő évtizedekben a biztonsági kihívások mátrixa is jelentősen megváltozott, a konvencionális fenyegetések helyét egyre inkább az aszimmetrikus fenyegetések vették át.[17] Az 1990-es években elindult közel-keleti rendezési és békefolyamatok előrevetítették a hagyományos háborúk esélyének csökkenését a térségben, azonban a Hezbollah és a Hamasz megerősödése, valamint már az első (1987–1993), de leginkább a második intifáda (2000–2005) eseményei rávilágítottak arra, hogy „ami nem béke az háború. [de] Ami a békétől eltér az még nem háború".[18] Izrael elkezdte a felkészülést az aszimmetrikus konfliktusok korszakára, és előtérbe került a hibrid hadviselés kérdése. „A hibrid műveletek alapja, hogy a támadó hatalmi eszközeit jól koordinált, szinkronizált módon a megtámadott állam alrendszereiben azonosított kritikus gyengeségek ellen fordítja. A támadás sikerének legfontosabb feltétele, hogy e gyengeségek már létezzenek a megtámadott államban: a támadó nem tudja létrehozni, legfeljebb csak felerősítheti azokat (pl. propagandával, döntéshozók megvesztegetésével). […]"[19] A hibrid hadviselés alkalmazásában vagy az ellene történő védekezésben kiemelt szerep jut az infokommunikációs területeknek, a kiberhadviselésnek vagy akár a felderítési területnek. Ahogy Kiss Álmos Péter fogalmaz: „Nélkülözhetetlen egy robusztus felderítő képesség, mely azonosítja a kritikus gyengeségeket és garantálja a műveletek tervezéséhez és vezetéséhez szükséges valós idejű helyzetismeretet".[20]

A kiberhadviselés és az ellene történő védekezés problémája az 1990-es évek eleje óta foglalkoztatta az izraeli biztonsági szférát: egyes elemzők már 1993-ban úgy vélekedtek, hogy a „kiberaktivitás a jövő egyik kiemelt csatatere lesz"[21]. Ezzel kezdetét vette az izraeli kibervédelmi és kiberhadviselési „háló" kiépülése, amely mára számos pilléren nyugszik és átszövi az összes érintett területet, szektort, integrálva

14 Singer-Senor 2017.

15 Signals Intelligence – a rádióelektronikai hírszerzés katonai rövidítése

16 https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf (Letöltés ideje: 2021.04.01.)

17 Rémai 2020b.

18 Resperger – Kiss – Somkuti 2013, 13

19 Kiss 2019.

20 Uo. 34

21 Raska 2015.

szinte minden szereplőt. A korábban már említett, kiemelt K+F tevékenységnek és az informatikai szektor 1990-es évekbeli – állami dotálással – történt fellendítésének köszönhetően 2014-ben a globális kiberbiztonsági piac izraeli részesedése nyolc százalékon állt. Ezzel párhuzamosan a lakosság általános technológiai felszereltsége is magas: 2015-ben az izraeli lakosság 78,89%-a használt internetet.[22]

A kibertérhez kapcsolódó terület egyik specifikuma a buzani szektorelméleteken[23] átívelő voltában rejlik, hiszen egyszerre jelenik meg a polgári és katonai területen, a titkosszolgálati és rendvédelmi területen, az állami és a gazdasági szereplők esetében, és érinti a biztonság összes, a szerzők által felsorolt körét.

Véleményem szerint a kibertér, a kibervédelem és kiberműveletek tekintetében az izraeli elméleti megközelítés leginkább az Egyesült Államok stratégiai dokumentumaiban is fellelhető fogalmi kerethez közelít.[24] Kibervédelem és a kiberműveletek vonatkozásában Izrael koncepciója alapvetően a kiterjesztett és komplex értelmezési keretet veszi alapul, azaz összességében a Haig Zsolt által megfogalmazott definícióval írható le a legpontosabban: „A kibertéri műveletek a kibertérben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, a kibertéri hálózatos infokommunikációs rendszereket felhasználva, a kognitív képességekkel közvetlenül, illetve a technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire".[25]

Az izraeli kibervédelmi és kiberhadviselési tevékenység fejlődése során egyértelművé vált, hogy egy szektorokon átívelő törvényi és szabályozási környezet kialakítására van szükség, amelyben a hatékonyság maximalizálása érdekében „minden érintett szereplő helyet kell, hogy kapjon az asztalnál". Azonban ehhez a koncepcióhoz egy hosszú és rögös út vezetett el.

„A startup nemzet" kiberbiztonsága, védelme és hadviselése

Az izraeli biztonsági szektor már viszonylag korán, az 1990-es évek középen felismerte, hogy a kiberbiztonság területén preventív lépések szükségesek, de ezek a kezdeményezések önmagukban „lebegtek", nem kerültek egy önálló kormányzati szerv irányítása alá.

A kiberbiztonság és kibervédelem területén végbement reformok és fejlesztések története két időszakra tagolódik, amelyben a 2010-es év jelentette a fordulópontot. A 2010-es évek előtti időszakban az izraeli szakértők és illetékes szervezetek a kritikus infrastruktúrákra és a létfontosságú rendszerekre fókuszáltak, míg 2010 után elkezdődött a magánszektor bevonása, és az izraeli nemzeti kiberbiztonsági koncepció kiszélesítése. Az izraeli kibertechnológiai szektor fejlődésének sikerét jól mutatja, hogy 2011 és 2021 között az aktív kiberbiztonsági cégek száma Izraelben 162-ről

22 Housen-Couriel 2017.

23 Buzan – Wæver – de Wilde 1998, 38

24 Kovács 2018.

25 Haig 2018, 237.

459-re nőtt.[26] Az izraeli kibertermékek exportjának értéke 2021-ben 11 milliárd dollárt ért el, és a világon minden harmadik kiberbiztonsági cég, amely tagja az unikornis klubnak, azaz amelyek értéke egy milliárd dollár felett van, izraeli.[27] Az izraeli kibertechnológiai magánszektor olyan támogató vagy önálló fejlesztéseket valósít meg, amelyek nemzetközi szinten is az innovációk élvonalába tartoznak, ezért az izraeli nemzetbiztonság szempontjából is kiemelt jelentőségűek. A szoros együttműködés az állami és a magánszektor között lehetőséget biztosít arra, hogy a folyamatosan változó kihívásokra, kockázatokra és fenyegetésekre gyors és hatékony válaszok szülessenek.

A fentiekkel párhuzamosan Izrael célul tűzte ki, hogy pár éven belül a világ vezető globális kiberhatalmainak egyikévé kíván válni.[28] Ehhez nemcsak a saját védelmi és támadó képességei fejlesztését emelte magasabb szintre, de aktívabb szerepet vállalt a nemzetközi együttműködésekben is. Ennek keretében bilaterális megállapodásokat kötött a kibervédelem területén számos országgal[29], aktívan részt vett nemzetközi[30] és globális[31] együttműködési megállapodásokban és párbeszédekben, amelyek a kibertér biztonságos használatára irányultak. Az Egyesült Államokkal való együttműködés szorosságát jól mutatja, hogy a két ország kibervédelmi struktúrája számos hasonlóságot mutat.[32]

Az 1990-es évek közepe óta tartó szabályozási és fejlesztési folyamatok általános és átfogó kérdései között első helyen jelent meg, hogy a kibertér, annak védelme és műveleti területként történő felhasználása hol foglal helyet az izraeli biztonsági koncepcióban. Kiemelt kérdésként merült fel a hosszú távú stratégiai célok és a rövid távú műveleti célok összehangolásának problematikája. Ehhez kapcsolódott a védelem három körének (belbiztonság, „közel-külföld", „távoli kötelezettségvállalás") összehangolása a kibertérben végrehajtott védekező és támadó tevékenységekkel.[33] Napjainkban Izrael szempontjából a kibertérből érkező kiemelt kihívások két fő csoportra bonthatóak:

1) A regionális ellenfelek – különösképpen Irán – folyamatos kiberműveletei.
2) A nemzetbiztonsági szektor és a kibertechnológiai szektor közötti szoros kapcsolat és integráció, amely az elemzői vélemények szerint számos eltérő jellegű kihívást foglal magába.[34]

A kockázatok, kihívások és fenyegetések mátrixának vizsgálata során olyan elemeket találunk, mint a kiberkémkedés, a kiberzsarolás, az ipari létesítményeket és a kritikus infrastruktúrát fenyegető támadások, a dezinformációs és hírszerző műveletek.

---

26 https://www.globalxetfs.com/cybersecurity-in-israel-fortifying-digital-defenses-amid-elevated-risks/ (Letöltés ideje: 2022.11.16.)

27 https://www.gov.il/en/departments/news/2021cyber_industry (Letöltés ideje: 2022.11.16.)

28 Tabansky 2013, 3.

29 pl.: Egyesült Államok, Bulgária

30 pl.: Council of Europe's Convention on Cybercrime (Council of Europe, 2019)

31 pl.: Geneva Dialogue on Responsible Behavior in Cyberspace

32 https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf 8 p. (Letöltés ideje: 2021.04.01.); Chachko 2002. 13.

33 Raska 2015.

34 https://www.huntandhackett.com/threats/israel (Letöltés ideje: 2022.11.16.)

Az alapvető koncepcionális kérdéseken túl végigkísérte az izraeli belpolitikában az elmúlt évtizedeket a kibervédelem finanszírozásának vitája, és részben ehhez kapcsolódóan a képzési és felkészítési rendszer, az oktatás kérdésköre.

Az izraeli kiber-ökoszisztéma létrehozásának lépései

Izraelben az első törvényi erejű szabályozás a nemzeti adatvagyon és az adatvédelem tekintetében 1995-ben született (ún. Computer Law), amelyet kiegészített és továbbfejlesztett az 1998-as adatbiztonsági törvény.[35]

2002-ben fogadták el a 84/B (2002) sz. kormányhatározatot a kritikus infrastruktúrák védelméről, amely a maga nemében az első ilyen kormányzati dokumentum volt a világon. A határozat felhatalmazta a belbiztonságért felelős polgári titkosszolgálat, a Shin-Bet alá tartozó National Information Security Authority-t (NISA – Nemzeti Információbiztonsági Hatóság) a létfontosságú létesítmények szektorspecifikus védelmének megtervezésére. A koncepció legnagyobb problémája az volt, hogy a Shin-Bet nem kapott megfelelő anyagi támogatást a feladat végrehajtásához, így a NISA és a Shin-Bet közötti feszültség egyre markánsabbá vált, és ez, valamint az erőforrások hiánya komolyan hátráltatta a NISA hatékony feladatellátását.

Komoly előrelépést jelentett a 2010-ben életre hívott Nemzeti Kiber Kezdeményezés[36], amelynek feladata az volt, hogy meghatározza az utat, amely által Izrael vezető kiberhatalommá válhat a jövőben. A vizsgálat eredményeit hét fő csoportba sorolta a bizottság, és azokhoz konkrét javaslatokat fogalmazott meg:

1) Javítani kell az informatikai oktatást, erősíteni kell az interdiszciplináris együttműködést.
2) Fejleszteni kell a területre vonatkozó alapvető ismereteket (tudásbázis létrehozása) és fokozottan támogatni kell a K+F tevékenységeket.
3) Létre kell hozni egy, az egész országra kiterjedő „védőpajzsot", amelynek felépítésében jelentős szerep jut az izraeli K+F szektor termékeinek, mindeközben azonban kezelni kell a felmerülő adatvédelmi aggályokat.
4) Fejleszteni kell a nemzeti operatív képességeket a kibertérben a rutinszerű működés és vészhelyzet esetén, de közben számos erkölcsi, jogi és pénzügyi kihívás fog megjelenni, amelyeket meg kell oldani a siker elérése érdekében.
5) Fejleszteni kell a védelmet technikai és nem technikai jogalkotási intézkedések ötvözésével.
6) Ösztönözni kell a helyi, hazai beszerzéseket, telepíteni kell olyan egyedi technológiákat, amelyeket az izraeli tudományos és ipari vállalatok fejlesztettek ki közösen.
7) Izraelben nem létezett nemzeti átfogó „kiberpolitikai" ügynökség, ezért az ajánlás hangsúlyozottan kiemeli egy ilyen szervezet létrehozásának szükségességét.

A Nemzeti Kiber Kezdeményezés ajánlásaira építve született meg 2011-ben a 3611 (2011) sz. kormányhatározat, az Advancing National Cyberspace Capabilities

35 https://unidir.org/cpp/en/states/israel (Letöltés ideje: 2021.04.12.)

36 Tabansky 2013.

Resolution[37]. A határozat megfogalmazta a legfontosabb célokat, mint (1) a diplomáciai együttműködések erősítése, (2) a gazdasági fejlődés fokozása, valamint (3) a globális kiberhatalmi státusz elérése és fenntartása. Ezek megvalósításához – a korábbiakhoz képest – nagyobb mértékben rendeltek erőforrásokat és eszközöket. A határozat létrehozta az Israel National Cyber Bureau (INCB – Izraeli Nemzeti Kiberiroda) nevezetű szervezetet, és a 2011–2016 közötti időszakra évi 130 millió dolláros költségvetést határozott meg számára.[38] Az INCB 27 fő feladata közül kiemelt volt az ipari fejlesztések operacionalizálása, valamint az akadémiai és a gazdasági szektor közötti kapcsolatok erősítése, továbbá egy egységes kibervédelmi hálózat alapjainak lefektetése.

Míg az INCB alapvetően kommunikációs közvetítőként határozta meg magát, addig a globális biztonsági kihívások szükségessé tették a terület operatívabb felügyeletét is. Ennek érdekében született meg a 2443 (2015) sz. kormányhatározat, amely létrehozta a National Cyber Security Authority-t (NCSA – Nemzeti Kiberbiztonsági Hatóság), mint operatív ügynökséget, hogy eljárjon az INCB mellett. A szervezet fő céljai között szerepelt (1) a hírszerzési tevékenység struktúrájának javítása, (2) az egyensúly megtalálása a nemzetbiztonsági érdekek és az alapvető szabadságjogok között, valamint (3) a humán és pénzügyi erőforráshiányban szenvedő izraeli IT-vállalatok támogatási rendszerének kidolgozása. Az NCSA-val együtt megalakult az izraeli számítógép-biztonsági incidenskezelő csoport (CERT – Computer emergency response team) és létrejöttek az ágazati CERT-ek. Az NCSA, mint operatív szerv megalakulása után átvette a Shin-Bettől a kritikus infrastruktúrák védelmének feladatát. Egyetlen szektor képez ez alól kivételt, mégpedig az izraeli telekommunikációs rendszerek.[39]

A 2444 (2015) sz. kormányhatározat „a nemzeti kibervédelmi felkészültség előmozdítása" címet viseli, amelyben megbízzák az NCSA-t a Nemzeti Kiber Doktrína kidolgozásával.

A 2015 és 2017 közötti időszakban az izraeli biztonsági szektort és az elemzőket a nemzeti kiberstratégia megfogalmazása tartotta lázban. Számos kutatóintézet és elemző készített javaslatokat, hogy melyek azok az elemek, amelyeknek mindenképpen bele kell kerülnie egy ilyen szintű és jelentőségű dokumentumba. A szektorra jellemző általános problémák mellett (finanszírozás, a humánerőforrás hiánya, az oktatás-képzés kérdései) kiemelt szempontként merült fel a túlzott interdependencia. Az izraeli kibervédelmi modellben a katonai, az állami és a gazdasági szereplők egymásra utaltsága ugyanis gyengíteni látszott a hatékony működést.[40] A védelmi jellegű tevékenység mellett egyre nagyobb szerepet kapott a támadó erő kérdése, amelynek fontosságára és kiemelt szerepére a jövőben várható konfliktusokban több elemző is felhívta a figyelmet.[41]

37 *Határozat a nemzeti kiberképesség fejlesztéséről.* https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Israel_2011_Advancing%20National%20Cyberspace%20Capabilities.pdf (Letöltés ideje: 2021.04.01.)

38 Tabansky 2013, 6.

39 https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf (Letöltés ideje: 2021.04.01.)

40 Raska 2015, 8.

41 Siboni - Assaf 2016.

A koherens izraeli kibervédelmi tevékenység megvalósításának következő lépéseként elkészült a Nemzeti Kibervédelmi Stratégia, amely egy nem nyilvános dokumentum.[42] Ennek folyományaként valósult meg az intézményrendszer átalakítása, amelynek fő eleme az NCSA és az INCB közös irányítás alá történő összevonása volt 2017-ben a 3270 (2017) sz. kormányhatározat alapján. A határozat létrehozta az Israel National Cyber Directorate-t, a Ma'arach-ot. Az Izraeli Nemzeti Kiber Igazgatóság (INCD)[43] „nemzetbiztonsági és technológiai ügynökségként Izrael kibertérének védelméért, valamint Izrael kiberhatalmának megteremtéséért és előmozdításáért felelős".[44]

Az INCD működése nagyban hasonlít a hazánkban is létező, az NBSZ égisze alatt működő Nemzeti Kibervédelmi Intézet[45] tevékenységéhez. A fő feladatai közé a kibervédelemmel foglalkozó szervezetek közötti kapcsolattartás, az állampolgárok IT-tudatosságának fejlesztése, a kibertámadások megelőzése és kezelése, valamint a vészhelyzeti reagálási képességek fejlesztése tartozik. A feladatait több pillére támaszkodva látja el: (1) a stratégiaalkotástól, (2) a humán erőforrás képzésen át, egészen (3) az innovatív megoldások és technológiák fejlesztéséig.

Az INCD fókuszában a lakossági és a gazdasági szereplők kiberbiztonságának védelme áll, az izraeli gazdaság informatikai védelmének egyik alapköve ez a szervezet. A honlapon elérhető ajánlások, elemzések és ismertetők jelentős része a vállalati szektort célozza meg.[46]

A szervezet feladatai öt fő kategóriába sorolhatók:

– a védelmi képességek fejlesztése és erősítése (észlelés – azonosítás – reagálás);
– az ellenálló képesség növelése (IT awareness);
– nemzetközi kapcsolattartás;
– a nemzeti kiberstratégia megfogalmazása, aktualizálása és tanácsadás a politikai vezetés számára;
– a K+F fejlesztések összehangolása és irányítása.

Az INCD közvetlen a miniszterelnök irányítása alatt álló szervezet, amely 2017-től jelentős befolyásra tett szert az izraeli kibertevékenység alakítása kapcsán. Mind az aktuális, operatív feladatok, mind a stratégiai tervezés területén az INCD kiemelt és erőteljes szereplővé vált, amely számos esetben okozott súrlódást más, a kibervédelem területén működő szervezetekkel, például a Moszaddal, az Izraeli Rendőrséggel vagy a Shin-Bet-tel. Az INCD koordináló szervként igyekszik a mai napig is az együttműködést biztosítani az érintett szervezetek között, kapcsolódjanak azok akár a polgári, akár a katonai vonalhoz.[47]

Összességében azt láthatjuk, hogy az INCD helyezkedik el a rendszer közepén, kiemelt szerepe van a stratégiaalkotásban és az irányok meghatározásában. Azonban

42 https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf (Letöltés ideje: 2021.04.01.)

43 https://www.gov.il/en/departments/about/newabout (Letöltés ideje: 2021.04.01.)

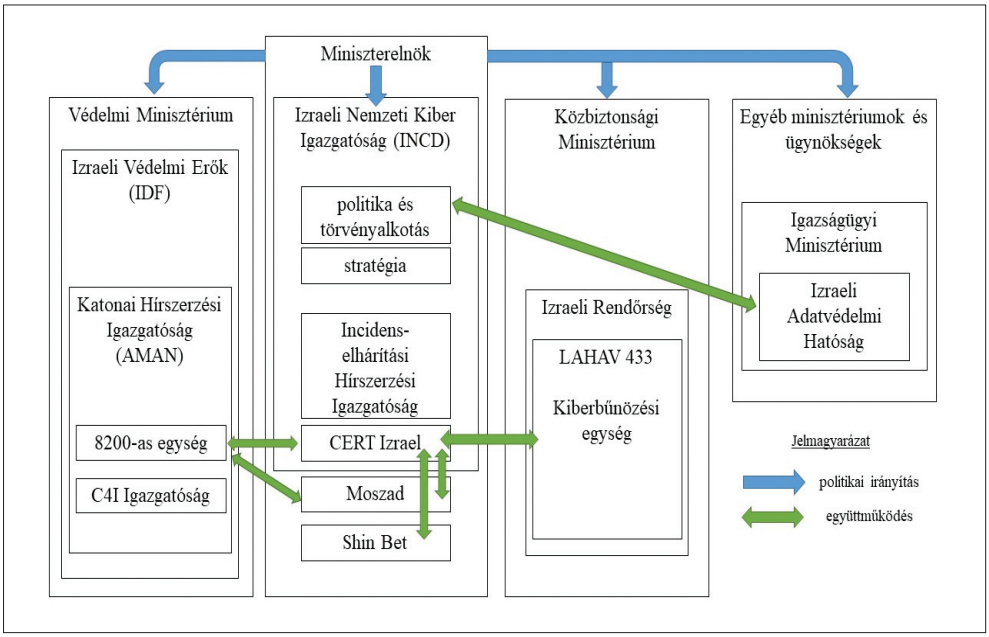
44 Housen-Couriel 2017.

45 https://nki.gov.hu/ (Letöltés ideje: 2021.04.01.)

46 https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/en/Cyber%20Defense%20Methodology%20for%20an%20Oragnization.pdf (Letöltés ideje: 2021.04.01.)

47 https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf (Letöltés ideje: 2021.04.01.) 5.

az operatív szinten számos szervezetet találunk az IDF 8200-as egységétől, a C4I Corpson át, a polgári titkosszolgálatok illetékes szervezeti elemein keresztül egészen az Izraeli Rendőrség kiberbűnözés ellenes egységéig. A végrehajtó szervek mellett jelentős szerepe van az Igazságügyi Minisztérium illetékes szervezeti egységeinek, amelyek közvetlenül együttműködnek az INCD-vel a törvényi keretek és az alapvető jogok biztosítása érdekében. (*1. ábra*)



1. ábra.
Áttekintő ábra a kibertevékenységben érintett izraeli szervezetekről
[A szerző szerkesztése az „Israel's National Cybersecurity and Cyberdefense Posture" dokumentum ábrája alapján.
Forrás: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf (Letöltés ideje: 2021.04.01.) 14.]

Az 1. táblázat (lásd következő oldalt) összefoglalja azon szervezeteket és fő feladatkörüket, amelyek az Izraeli Nemzeti Kiber Igazgatóság (INCD) mellett kiemelt jelentőséggel bírnak a kibervédelmi és kiberműveleti területeken.

Izraeli Védelmi Erők (IDF) és a polgári titkosszolgálatok (együtt)működése a kibertevékenység területén

Az izraeli kibertevékenységet alapjaiban jellemzi, hogy a képességek kettős felhasználásúak. A nemzeti *kiber-ökoszisztéma* létrehozásának egyik kiemelt szempontja volt, hogy az együttműködés eredményeit mind az állami, mind a gazdasági szektor fel tudja használni, és profitálni tudjon belőle. A konvergencia az IDF és a polgári titkosszolgálatok kiberágazataiban dolgozó munkatársak és a piaci szektor között nagyon

szoros. Gyakori jelenség, hogy az aktív szolgálat után önálló high-tech vállalatokat alapítanak a korábban a fegyveres erőknél dolgozó szakemberek.[48]

1. táblázat.
Áttekintés a kibervédelmi és kiberműveleti tevékenység főbb izraeli szereplőiről
(Forrás: saját szerkesztés)

Szervezet	**Fő feladatkör(ök)**
8200-as egység	A katonai hírszerzésen belül a technikai információk (SIGINT) gyűjtésével és elemzésével foglalkozó szervezeti egység. Nem megerősített információk szerint a támadó képességek területen is jelentős kapacitásokkal rendelkezik az egység. (vö. Stuxnet – 2010, Duqu – 2011)
C4I Igazgatóság	Az IDF harctámogató alakulata, amely a távfeldolgozás és a kommunikáció minden területéért felelős a haderőn belül.
CERT Izrael	Izrael információbiztonsági és kibereseményeivel foglalkozó civil központja. Az IL-CERT felelős a kiberbiztonsági eseményekkel kapcsolatos tevékenységek koordinálásáért, a megelőző védelmi tevékenységekért, valamint az információ megosztásáért és a nyilvánosság tájékoztatásáért az információbiztonsággal és az adatvédelmi kérdésekkel kapcsolatban.
Moszad	Az illetékességi körébe tartozó területen kibervédelem, információgyűjtés, információszerzés, információcsere, proaktív támadó műveletek végrehajtása.
Shin-Bet	Az illetékességi körébe tartozó területen kibervédelem, információgyűjtés, információszerzés, információcsere, proaktív támadó műveletek végrehajtása.
LAHAV 433 – Kiberbűnözési egység	Nemzeti szintű nyomozóhatósági jogkörrel rendelkező rendőri szerv, amelynek egyik fő feladata a kibertérben elkövetett bűncselekmények detektálása, felderítése és a lakossági kibervédelem erősítése. Kiemelten jelenik meg a kiskorúak sérelmére a kibertérben elkövetett bűncselekmények kivizsgálása, és az ilyen esetekkel kapcsolatos lakossági bejelentések kezelése.
Izraeli Adatvédelmi Hatóság	Az 5741-1981 sz. Adatvédelmi Törvény alapján a hatóság a személyes digitális információk izraeli szabályozó és végrehajtó hatósága. A hatóság felelős a digitális adatbázisokban tárolt valamennyi személyes adat védelméért.

Operatív szinten az izraeli modell *egy többrétegű védelmi és támadó stratégia szerint működik*, ahol a területek határvonalai összefolynak: aktív védekezés és magas szintű támadó képességek jelennek meg mind a polgári, mind a katonai területen.[49] Ha plasztikusan akarnánk megfogalmazni, akkor a kibervédelem kérdése a polgári titkosszolgálatok, mint a Moszad és a Shin-Bet hatáskörébe tartozik, míg a kiberhadviselés az Izraeli Védelmi Erők területe.

Részben a feladatkörökből, részben a történelmi előzményekből fakadóan a Shin-Bet aktívan részt vesz az izraeli kibervédelemben. Magától értetődően – hasonlóan

48 https://europe.autonews.com/automakers/high-techs-israeli-military-connection (Letöltés ideje: 2021.04.12.)

49 Raska 2015.

a Moszadhoz és az Izraeli Rendőrség speciális egységeihez –, a Shin-Bet is felhasználja a kiberteret információgyűjtésre, információszerzésre, információcserére más kormányzati szervekkel és – szükség esetén – proaktív módon támadó tevékenységek végrehajtására is.

Az utánpótlásképzés és az oktatás kérdése végigkíséri az izraeli kiberéra történetét. Éppen ezért nem meglepő, hogy ezen a területen is megjelennek az innovatív módszerek. A Shin-Bet volt az első titkosszolgálat, amely az informatikai szakemberek kiválasztására egy online kriptográfiai feladványsort használt, amely rejtvényként és kiválasztási eljárásként is funkcionált egyben.[50]

A minden területen felmerülő proaktív hozzáállás – amely a Netanjahu miniszterelnök által kezdeményezett 2017-es nemzetbiztonsági stratégia egyik kiemelt módszere – legfőbb célja, hogy minden erőforrást Izrael Állam védelmének és a biztonság szavatolásának rendeljenek alá.[51]

A titkosszolgálatok közötti villongások felszámolására 1994 körül létrehozott Magna Charta dokumentumok[52], a politikai nyomás és a valós fenyegetettség miatt a szervezetek az évek során belátták, hogy a „need to know" és a „need to share" klasszikus információ-kezelés elve helyett az izraeli hírszerző közösséget a „must to share" elve kell, hogy jellemezze.[53] Az információk megosztásának mára komoly hagyománya van, a szolgálatok egymást támogatva lépnek fel, de emellett megőrzik saját szervezeti, működési jellegzetességeiket és fő feladatukra koncentrálnak. Azonban, ha olyan információ merül fel, amely nemzetbiztonsági szempontból releváns lehet, de szorosan nem kapcsolódik a szervezet fő profiljához, akkor azt bejáratott csatornákon, a lehető legrövidebb időn belül továbbítják az illetékes szolgálatnak. „Az információ megosztása mellett nagyon szoros az operatív szintű kooperáció is."[54]

2013-ban Benny Gantz vezérkari főnök úgy fogalmazott, hogy „hatalmas kiberháború fog tombolni, amely nemcsak a katonai, hanem a polgári rendszereket is érinteni fogja".[55] Az Izraeli Védelmi Erők kiberterületen dolgozó egységei számára kijelentése nem okozott komoly változást. Az IDF kibertevékenységéről viszonylag keveset lehet tudni, de a kibervédelem és kibertámadások területén élen járó egységekről van szó. Mind az IDF Computer Service Directorate alá tartozó C4I Corps, amely mindenfajta katonai kommunikációért felel,[56] mind a 8200-as egység, amely eredetileg a SIGINT hírszerzésért volt felelős,[57] az IDF hatékony működésének egy-egy alapkövét jelenti.

Az Aman (Agaf Modiin – katonai hírszerzés) alá tartozó 8200-as egység azon túl, hogy folyamatos információgyűjtést hajt végre és adatokkal látja el az Aman értékelő-elemző részlegeit, az elmúlt években nem egyszer került be hírekbe. Meg nem erősített

50 https://www.israelneedsu.com/ (Letöltés ideje: 2018.11.29.)

51 Adamsky 2017.

52 Kahana 2002.

53 Best Jr. 2011.

54 Rémai 2020a, 12.

55 Raska 2015.

56 https://web.archive.org/web/20110525094701/http://dover.idf.il/IDF/English/units/forces/ground/communication/default.htm (Letöltés ideje: 2021.04.12.)

57 https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c (Letöltés ideje: 2021.04.12.)

információk és szóbeszédek szegélyezik a szervezet történetét olyan kibertámadásokról, amelyek az IDF kiberhadviselési képességének fejlettségéről adnak tanúbizonyságot. A CSIS (Center for Strategic and International Studies) összefoglaló listája alapján 2006 óta minimum 42 olyan kiemelt kibertámadást tartanak nyilván, ahol az izraeli kötődés erőteljesen igazolható.[58] Kiragadott példaként említhetjük, hogy a 2010-es év óta tartja magát az elmélet, hogy az iráni atomprogram ellen végrehajtott Stuxnet elnevezésű, rosszindulatú számítógépes féreg által okozott támadás mögött is a 8200-as egység áll.[59]

Nem véletlen, hogy az Aman hatáskörébe tartozik egyrészt az évenkénti országfenyegetettségi jelentés elkészítése, másrészt a hírszerzési tevékenység folyamatos fejlesztése.[60] Ez utóbbiból következtethetünk arra, hogy az IDF hírszerző szervezete jelenti az etalont, amely alapján a polgári titkosszolgálatok és más rendvédelmi erők kialakítják saját módszereiket.

Következtetések

A permanens fenyegetettség állapotában létező állam esetében a jövő kihívásaira történő felkészülés az elmúlt évtizedekben a fennmaradás záloga lett, így nem meglepő, hogy az izraeli védelmi tervezés már idejekorán elkezdett foglalkozni a kibertér kihívásaival, és a benne rejlő lehetőségekkel. Ez a több évtizedes felkészülés, tanulás és kísérletezés vezetett el napjainkban oda, hogy Izrael meghatározó globális kiberhatalom. A biztonsági kihívások, kockázatok és fenyegetések mátrixának alakulását látva az izraeli védelmi tervezés „jól tette meg tétjeit", amikor a kibertérben történő jelenlétet tette meg az egyik kiemelt iránynak évtizedekkel ezelőtt. A kibertér térnyerését felerősítette a koronavírus-járvány, amely által a polgári lakosság és a gazdasági szektor kitettsége a kibertérből érkező fenyegetéseknek jelentősen növekedett. Az izraeli kibervédelmi modell lényege, hogy a lehető legszélesebb kört bevonja a többszintű, rétegzett védelmi struktúrába. Ugyanakkor a védelem mellett folyamatosan fejlesztette és a gyakorlatban próbálta ki a fejlett és kifinomult hírszerzési, valamint támadó képességeit a hagyományos katonai és titkosszolgálati műveletek támogatására annak érdekében, hogy regionális pozícióját megerősítse.

Netanjahu elnök 2018-ban úgy fogalmazott, hogy a kiberbiztonságra költött összegek megtérülni látszanak, hiszen Izrael kitettsége a kibertérben folyamatosan csökken. Ugyanakkor kiemelte, hogy ehhez szükséges volt a speciális izraeli gazdasági modellre és a high-tech iparral való szoros együttműködésre, amely minden közreműködő fél számára előnyös volt, hiszen „a biztonságra való véget nem érő törekvés egy óriási üzleti lehetőség"[61].

Összefoglalva a kiberstratégia és az operatív feladat-végrehajtás a kibertérben Izrael esetében pontosan olyan, mint számos egyéb szektor az országban: egyszerre

58 https://csis-website-prod.s3.amazonaws.com/s3fs-public/210430_Significant_Cyber_Events_List.pdf?B21zjJhsoO3qkgQNyGMmZN5IhAE80S_I (Letöltés ideje: 2021.04.14.)

59 Langner 2011.

60 Rémai 2020a.

61 https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf (Letöltés ideje: 2021.04.01.) 12.

kaotikus, ugyanakkor hatékony. Az Izrael által, az elmúlt negyed évszázadban a kibervédelem és kiberhadviselés terén bejárt út példaértékű, ugyanakkor megismételhetetlen. A sikerhez szükség volt az ország speciális biztonsági helyzetére, az egyedi társadalmi, gazdasági és politikai jellemzőkre és az izraeli innovációs potenciálra.

FELHASZNÁLT IRODALOM

Advancing National Cyberspace Capabilities Resolution. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Israel_2011_Advancing%20National%20Cyberspace%20Capabilities.pdf (Letöltés dátuma: 2021.04.01.)

Cyberdefense Report: Israel's National Cybersecurity and Cyberdefense Posture. Cyber Defense Project (CDP) Center for Security Studies (CSS), ETH, 2020. Zürich https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf (Letöltés ideje: 2021.04.01.)

Ben-Gurion, David. 1970. *Memoirs.* The World Publishing Company, New York.

Best Jr., Richard A. 2011. *Intelligence Information: Need-to-Know vs. Need-to-Share.* Congressional Research Service. https://fas.org/sgp/crs/intel/R41848.pdf (Letöltés ideje: 2021.04.25.)

Buzan, Barry – Wæver, Ole – de Wilde, Jaap. Security 1998. a New Framework for Analysis. Boulder, Lynne Rienner. https://doi.org/10.1515/9781685853808

Chachko, Elena. 2002. Persistent Aggrandizement? Israel's Cyber Defense Architecture. A Hoover Institution Essay. https://www.hoover.org/sites/default/files/research/docs/chachko_webready.pdf (Letöltés ideje: 2021.04.12.) https://doi.org/10.2139/ssrn.4054071

Adamsky, Dmitry (Dima). 2017. *The Israeli Odyssey toward its National Cyber Security Strategy,* The Washington Quarterly, 40:2, 113–127, https://doi.org/10.1080/0163660X.2017.1328928

Dobák Imre – Kovács Zoltán. 2014. Új technológiák hatása a hírszerzésre. In: Dobák Imre (szerk.): A *nemzetbiztonság általános elmélete.* Nemzeti Közszolgálati Egyetem, 2014, Budapest. 206-221 p. ISBN 978-615-5305-49-8 http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/8567/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y (Letöltés ideje: 2021.04.12.)

Gazdag Ferenc – Remek Éva. 2018. A *biztonsági tanulmányok alapjai.* Dialóg Campus Kiadó, Budapest. 282 p. ISBN 978 615 5845 88 8

Haig Zsolt. 2018. *Információs műveletek a kibertérben.* Dialóg Campus Kiadó, Budapest. 237 p.

Housen-Couriel, Deborah. 2017. *National Cyber Security Organisation: ISRAEL.* NATO CCD COE, Tallin. 5 p. https://ccdcoe.org/uploads/2018/10/IL_NCSO_final.pdf (Letöltés ideje: 2021.04.12.)

Kahana, Ephraim. 2002. Reorganizing Israel's Intelligence Community *International Journal of Intelligence and Counter Intelligence,* Vol. 15, No. 3, 415–428. DOI: https://doi.org/10.1080/08850600290101686

Kiss Álmos Péter. 2019. A hibrid hadviselés természetrajza In: *Honvédségi Szemle,* 2019/4., p. 34. https://honvedelem.hu/files/files/116701/hsz_2019_4_017_037_4557.pdf (Letöltés ideje: 2020. 04. 02.)

Kovács László. 2018. *Kiberbiztonság és –stratégia.* Dialóg Campus Kiadó, Budapest. 153 p.

Langner, Ralph. 2011. *Cracking Stuxnet, a 21st-century cyber weapon* https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyber_weapon/transcript?language=en (Letöltés ideje: 2021.04.12.)

Raska, Michael. 2015. *Policy Report CONFRONTING CYBERSECURITY CHALLENGES: ISRAEL'S EVOLVING CYBER DEFENCE STRATEGY* Military Transformations Programme, Institute of Defence and Strategic Studies (IDSS), Singapore https://www.michaelraska.de/download/Israel's_Evolving%20Cyber%20Strategy_Raska.pdf (Letöltés ideje: 2021.04.01.)

Rémai Dániel. 2020 a. Az izraeli nemzetbiztonsági rendszer fejlődésének története In: *Nemzetbiztonsági Szemle (online).* 7 (4). pp. 3–19. ISSN 2064-3756 https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1802/3441 (Letöltés ideje: 2021.04.12.) https://doi.org/10.32561/nsz.2019.4.1

Rémai Dániel. 2020 b. Biztonsági kihívások hálójában, avagy az Izraeli Védelmi Erők esete az aszimmetrikus hadviseléssel
In: *Honvédségi Szemle.* 148 (6) pp. 16–31.
https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/163/155
(Letöltés ideje: 2021.04.12.) https://doi.org/10.35926/HSZ.2020.6.2

Rémai Dániel. 2021. Made in Israel, avagy hadiipari és logisztikai sajátosságok az Izraeli Védelmi Erőkben
In: *Katonai Logisztika* (szerkesztés alatt) https://doi.org/10.30583/2020.4.076

Resperger István – Kiss Álmos Péter – Somkuti Bálint. 2013. Aszimmetrikus hadviselés a modern korban
Zrínyi Kiadó, Budapest.

Siboni, Gabi – Assaf, Ofer. 2016. *Guidelines for a National Cyber Strategy*
https://www.inss.org.il/publication/guidelines-for-a-national-cyber-strategy/
(Letöltés ideje: 2021.04.01.)

Singer, Saul – Senor, Dan. 2012. *Startra kész nemzet - Izrael gazdasági csodájának története* Patmos Records.

Tabansky, Lior. 2013. *Cyberdefense Policy of Israel: Evolving Threats and Responses*
https://www.chaire-cyber.fr/IMG/pdf/article_3_12_-_chaire_cyberdefense.pdf
(Letöltés ideje: 2021.04.12.)

Internetes források

A szír ellenzék által készített adat vizualizáció az Izrael által végrehajtott légicsapásokról
https://www.facebook.com/syriahroe/photos/a.150495128392167/326164433061054 9/
(Letöltés ideje: 2021.04.12.)

CI4 Corps https://web.archive.org/web/20110525094701/http://dover.idf.il/IDF/English/units
/forces/ground/communication/default.htm (Letöltés ideje: 2021.04.12.)

Cyber-Security-Qutes
https://medium.com/@romadantivirus/cyber-security-is-much-more-than
-a-matter-of-it-a02f724618e6 (Letöltés ideje: 2021.04.12.)

Cybersecurity in Israel: Fortifying Digital Defenses Amid Elevated Risks.
https://www.globalxetfs.com/cybersecurity-in-israel-fortifying-digital-defenses-amid-elevated-risks/
(Letöltés ideje: 2022.11.16.)

CSIS - Significant Cyber Incidents
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
(Letöltés ideje: 2021.04.12.)

CSIS - Significant Cyber Incidents Since 2006.
https://csis-website-prod.s3.amazonaws.com/s3fspublic/210430_Significant_Cyber_Events_List.pdf?
B21zjJhsoO3qkgQNyGMmZN5IhAE80S_I (Letöltés ideje: 2021.04.14.)

High-tech's Israeli military connection
https://europe.autonews.com/automakers/high-techs-israeli-military-connection
(Letöltés ideje: 2021.04.12.)

INCD brosúra
https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/en
/Cyber%20Defense%20Methodology%20for%20an%20Oragnization.pdf (Letöltés ideje: 2021.04.01.)

Israeli Cyber Security Industry Continued to Grow in 2021: Record of $8.8 Billion Raised.
https://www.gov.il/en/departments/news/2021cyber_industry (Letöltés ideje: 2022.11.16.)

Israeli National Cyber Directorate https://www.gov.il/en/departments/about/newabout
(Letöltés ideje: 2021.04.01.)

National Cybersecurity Strategies Repository
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx
(Letöltés ideje: 2021.04.12.)

Nemzeti Kibervédelmi Intézet https://nki.gov.hu/ (Letöltés ideje: 2021.04.01.)

Shabak Challenge weboldal https://www.israelneedsu.com/ (Letöltés ideje: 2018.11.29.)

Threat profile Israel. https://www.huntandhackett.com/threats/israel (Letöltés ideje: 2021.04.01.)

UNIDIR Cyber Policy Portal https://unidir.org/cpp/en/states/israel (Letöltés ideje: 2021.04.12.)

Unit 8200: Israel's cyber spy agency https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c
(Letöltés ideje: 2021.04.12.)