SZOLNOKI SZABOLCS

KIBERDIPLOMÁCIA, TECHNOLÓGIA-TRANSZFER, DIGITÁLIS TÉR – IZRAEL AKTUÁLIS KIHÍVÁSAINAK ÁTTEKINTÉSE A 2020-AS ÉVEK KEZDETÉN

Pécsi Tudományegyetem, PhD hallgató

Absztrakt

Izraelre, a „kibernemzetre”, hűen becenevéhez számos ország egyfajta példaképként tekint hírszerzési és védelmi képességei ismeretében. Jelen tanulmány egy átfogó, de terjedelmi korlátok miatt közel sem teljes képet igyekszik bemutatni a kibervédelmi-ökoszisztémáról, amely több mint 430 startuppal, dollár-milliárdos cégértékű vállalatokkal, egészen fiatal kortól elérhető oktatási programokkal büszkélkedhet. A szerző a sikerek és erősségek mellett az elmúlt időszak jelentősebb incidenseit és az aktuális kihívásokat is felvázolja, célja jó gyakorlatok, együttműködési lehetőségek feltárása.

Kulcsszavak: kibernemzet, kritikus infrastruktúrák, STEM oktatás, technológia-transzfer, kiberdiplomácia

CYBER DIPLOMACY, TECHNOLOGY TRANSFER, DIGITAL SPACE – OVERVIEW OF ISRAEL'S CURRENT CHALLENGES IN THE EARLY 2020S

Abstract

True to its nickname Israel, the “cyber nation,” is seen as a kind of role model in terms of intelligence and defense capabilities by many countries. Present study aims to provide a comprehensive but far from complete picture of the cyber defense ecosystem of Israel, the country with around 430 startups and billion-dollar value unicorns in this industry. Author outlines the major incidents of the recent period as well as the current challenges and threats. Purpose of the article is to introduce good practices and cooperation opportunities to policymakers and Hungarian cyber security experts.

Keywords: cyber nation, critical infrastructures, STEM education, technology transfer, cyber diplomacy

Bevezetés – Izrael, a „kibernemzet”

A modern, önálló Izrael 2018-ban ünnepelte kikiáltásának hetvenedik évfordulóját. A jeles jubileum mellett az is okot adhatott az ünneplésre, hogy az ország imázsa az elmúlt évtizedben jelentősen javult. Ma már világszerte sokak számára Izrael hallatán a startup nemzet, az innováció és kutatás-fejlesztés, a kockázati-tőkebefektetések fellegvára és a kiemelkedő kutatók hazája jut eszébe.

Izraelre egyre többször „Cyber Nation”-ként hivatkoznak, mivel az ország már nem csak saját kiberterének védelmében jeleskedik, hanem „exportálja” is képességeit. A márkanév mögött tudatos országimázsépítés áll, amely nem meglepő, hiszen annak céljai elsősorban gazdaságiak, a versenyképesség javítását szolgálják, például az export fejlesztésén keresztül. *(Papp-Váry 2019)* A kiberbiztonsági iparnak nyújtott kormányzati támogatás kezdettől fogva jelen van olyan programokkal, mint a Kidma[26] és a Masad[27], amelyek segítik az ágazat startupjait és egészséges versenyt teremtenek közöttük. Ezen kívül a kormány partnerséget kötött a hadsereggel, az egyetemekkel és a versenyszféra szereplőivel. (*Israel Cyber Alliance, 2021*)

A kiber-ökoszisztéma több mint 430 céggel büszkélkedhet, a tőzsdén bejegyzett nagyvállalatoktól kezdve az országszerte működő induló garázscégekig. Összértékük meghaladja a 3.5 milliárd dollárt, a globális kiberbiztonsági piac körülbelül 5 százalékát képviselve. (*Israel Cyber Alliance, 2021)*

Az aktuális kihívások között elsőként említhetjük a csúcstechnológiai iparágban jelentkező, így a kiberbiztonság állami, akadémiai és vállalati szereplőnél is nehézségeket okozó munkaerőhiányt. A piaci szereplők körében ráadásul a leggyorsabban fejlődő, innovatív startup cégekre veszélyt jelentenek a multinacionális vállalatok helyi kutatási, fejlesztési és innovációs fejlesztő központjai azáltal, hogy jelentősen magasabb fizetésekkel és rendkívül vonzó béren kívüli juttatási csomagokkal csábítják a programozókat, mérnököket. A szektorban az éves átlagfizetés 275.714 NIS[28] (megközelítőleg 25 millió forint). (*Payscale*

[26] Elnevezése angolul: Advancement of Cyber Defense R&D, 2013-ban elindított program, amely 80 millió új izraeli sékellel támogatta az iparáig KFI projektjeit; a sikereitől vezérelve pedig 2015-ben a Kidma 2.0 még nagyobb, 100 millió sékeles költségvetéssel rendelkezett.
[27] Elnevezése angolul: Dual Cyber R&D, a nemzeti és a védelmi kiber technológiák támogatásának 10 millió sékel költségvetésű 2012-2013 között megvalósított programja.
[28] Új izraeli sékel.

2021) Az IVC Kutatóközpont 2019-es felmérése szerint a vizsgálat idején legalább 800 magasan képzett munkavállalóra volt szüksége a megközelítőleg 20.500 főt foglalkoztató szektornak. (*Solomon 2019*)

További elem a kihívások sorában a folyamatos és intenzív fenyegetettség - a fizikai tér mellett - a kibertérben is. Az ország hírneve nem rettenti el az offenzív szándékú politikai vagy gazdasági riválisokat, éppen ellenkezőleg. A közel egy évtizede folyamatosan élesedő és egyre látványosabb kiber-hidegháború Izrael és Irán között 2020-ban újabb támadásokkal került a világsajtó címlapjaira. Az amerikai F5 Labs adatvédelmi vállalat friss jelentése szerint 2020. július és október között Izrael vált a hackerek első számú célpontjává, ezzel megelőzve az Egyesült Államokat, Indiát, Oroszországot, Törökországot és Csehországot. (*Nocamels 2020*)

A kiberbűnözés természetesen Izraelben sem korlátozódik a kritikus és kormányzati infrastruktúrák elleni, a külföldről indított incidensekre. Az állampolgárok éberségét honfitárs digitális banditák is rendszeresen próbára teszik – a figyelmetlenségnek pedig nagy ára van. A social engineering – magyarul pszichológiai manipulálás és megtévesztés során kihasználják, hogy sok esetben az ember a leggyengébb láncszem, és nem éri meg közvetlenül az informatikai rendszereket támadni, annál inkább a felhasználóktól kicsalni a belépési azonosítókat és jelszavakat. Az URL (Uniform Resource Locator, magyarul egységes erőforrás-helymeghatározó)[29] rövidítéseken alapuló becsapós SMS üzenetek Izraelben rendkívül elterjedtek. A módszert Fehér Krisztián könyvéből részletesen megismerhetjük – lényege, hogy félrevezető szöveggel ráveszik a címzettet, hogy kattintsanak a ránézésre beazonosíthatatlan weboldalra mutató hivatkozásra. (*Fehér 2018*) 2020. novemberében több ezer SMS üzenetet kaptak mobiltelefon előfizetők a következő üzenettel: "A fiókját letiltottuk, kérjük, erősítse meg személyazonosságát ezen a linken keresztül". A rendőrség kiberbiztonsági egysége és az Izraeli Nemzeti Kiber Igazgatóság (INCD) közös művelete két bűnöző letartóztatásához vezetett, akik ezres nagyságrendben, bankok és hitelkártya-társaságok nevében kiküldött SMS üzeneteikkel több százezer sékelt tulajdonítottak el a becsapott állampolgároktól az internetbankos jelszavak és kétfaktoros azonosításhoz kapott kulcsok megszerzésével. *(Israel National Cyber Directorate 2020/3)*

A rendőrség beszámolója szerint 2020-ban 8.377 kiberincidenst vizsgáltak, amelyek többsége személyazonosság-lopással és okmányhamisítással kapcsolatos. Az Israel Hayom

[29] Az interneten megtalálható bizonyos erőforrások (például szövegek, képek) szabványosított címe.

újság birtokába jutott jelentés szerint csupán 75 személy - 50 tiszt, továbbá 25 önkéntes nemzeti szolgálatos és katona teljesít szolgálatot az izraeli FBI-nak is hívott Lahav 433 elnevezésű, öt különböző bűnügyi nyomozó egység kombinációjával létrehozott Nemzeti Bűnügyi Osztálynál.[30] Ez a létszám a kritikusok szerint rendkívül alacsony ennyi ügy eredményes kivizsgálásához. *(The Jerusalem Post 2020/2)* Ennek ellenére a szerző nem állna be a bírálók táborába, ismerve a Lahav 433 és társszervei szoros együttműködését, illetve a kiemelkedő folyamat-automatizálási és technológiai képességét a dark web – magyarul sötét internet[31], a közösségi média, az azonnali üzenetküldő alkalmazások, az internetes fórumok és más platformokon végzett felderítésekben.

Számos vitát és kritikát eredményezett, hogy a 2010-ben útjára indított nemzeti kibervédelmi stratégia végrehajtása még nem tudott kiteljesedni a kibertörvény elfogadtatási folyamatának két évvel ezelőtti befagyása miatt. Az állami hatóságok, elsősorban az Izraeli Nemzeti Kiber Igazgatóság (INCD) a jogszabály hatályba lépéséig, és ezáltal az eredményes működéséhez szükséges felhatalmazásokkal történő felruházásig arra kényszerül, hogy a kormány által 2015-ben jóváhagyott „hibrid intervencionista-kooperatív" kiberpolitika keretében folytassa tevékenységét.

Szintén a szabályozási, szakpolitikai kihívások közé sorolható a Nemzeti Kibervédelmi Koncepció 2.0 c. dokumentum várható véglegesítésének, és a végrehajtáshoz szükséges költségvetés rendelkezésre bocsátásának bizonytalansága. Ugyan csak nemrégiben, 2020. decemberben tették közzé a koncepció vázlatát társadalmi egyeztetésre, 2021. márciusban két éven belül negyedik alkalommal tartanak parlamenti választásokat, a politikai válság pedig pont egy olyan területen is késlekedést okoz, ahol folyamatosan naprakészen kell tartani mind a szabályozási környezetet, mind pedig az infrastruktúrát – ehhez pedig felhatalmazással rendelkező döntéshozók és költségvetés szükségeltetik.

[30] Egységek angol elnevezései: Serious and International Crime Unit, National Economic Crimes Unit, National Car Theft Unit, National Fraud Squad, Gidonim Unit for intelligence gathering and special operations.
[31] Az internet nem indexelt, nem kereshető rétege, ahol a kapcsolat titkosított, és az adatforgalom a világ különböző pontjain lévő átjátszókon keresztül halad át, így a felhasználó anonim maradhat.

Kritikus infrastruktúrák fenyegetettsége – nyilvánosságra hozott támadások a közelmúltból

Bár természeti adottságai nem kifejezetten kedvezők, Izraelt az egyik legfejlettebb országnak tartják a Közel-Keleten gazdasági és ipari tekintetben. Tim Marshall könyvében kiválóan levezeti, hogy a gazdasági és politikai viszonyokat megalapozó fizikai realitások a földrajz fogságában tartják az államokat, a technológia fejlődésével viszont megnyílt a kitörés lehetősége. *(Marshall 2016)* Ezt a zsidó állam vezetése már nagyon korán felismerte, így a kormányzati programoknak köszönhetően szinte minden ágazat termelékenységét és fejlődését átjárja, és előre mozdítja az innováció, a tudomány és technológia. A nagyarányú digitalizáció ugyanakkor veszélyeket, támadási felületet is biztosít ellenségeik számára, az intenzív kutatási és fejlesztési tevékenységek pedig az ipari kémkedést élénkítik. A 2019-ben azonosított 8.500 gyanús incidens kétharmada a kritikus infrastruktúrák ellen irányuló - sikertelen kísérlet volt a Nemzeti Kiber Igazgatóság vezetőjének elmondása alapján.

Vízgazdálkodás elleni támadások

A kritikus infrastruktúrák védelmét már korán magas prioritású feladatként határozták meg. Kiemelkedik közülük a víz, hiszen a csapadékszegény éghajlat következtében a nagy mennyiségű lakossági, ipari és mezőgazdasági édesvíz felhasználás fedezésére újszerű megoldások segítségét kellett igénybe venniük. A keletkezett szennyvíz 86 százalékát újrahasznosítják, főként mezőgazdasági öntözésre, továbbá a tengervizet több üzemben is sótlanító eljárással kezelik. A „Sorek” elnevezésű, Tel-Aviv közelében található létesítmény a legnagyobb kapacitású vízsótlanító telep a világon, évente 151.4 milliárd literes teljesítményével. Ezen üzemek segítségével sikerült elérni, hogy a vízhiánnyal küzdő ország ivóvíz exportőrré váljon.

2020. áprilisban az Izrael és Irán közötti kiber-hidegháború keretében a perzsa állam a vízellátást vette célba – vidéki szivattyúk, tározók és vízvezetékek irányítóközpontjait. Hozzáfértek a szennyvízkezeléshez, valamint a klór és más vegyszerek hozzáadását szabályozó rendszerekhez. A művelet szelepek és vezérlőrendszerek kisebb mértékű károsodásán kívül jelentős mértékű műszaki, üzemeltetési meghibásodást és ellátási kimaradást nem okozott, mivel a behatolást korán észlelték és képesek voltak annak elfojtására. Az iráni Forradalmi Gárda kiber alakulatába tartozónak gondolt hackerek az

Egyesült Államokban és Európában működő szerverekről indították a támadást. Szakértői vélemények szerint a Stuxnet kódjának átalakításával vitték véghez az izraeli eszközök manipulálását. A károkozás valószínűsíthetően szándékosan csak korlátozott mértékű volt, ugyanis a két ország közötti viadalokat a virtuális térben egyfajta kiber-hidegháborúként, sokszor az erőviszonyok felméréseként, erődemonstrációként is lehet értelmezni. Rendkívül könnyű, akár véletlenül is olyan károkozást előidézni, amely casus belli-ként szolgálhat, és hagyományos válaszcsapást válthat ki, ez pedig egyik félnek sem érdeke – egyelőre.

Energiaszektor fenyegetettsége

A vízellátás mellett a villamosenergia-hálózat is állandóan célkeresztben van. 2020. januárban tett nyilatkozatában Yuval Steinitz energiaügyi miniszter elmondta, hogy Izrael energiainfrastruktúrájának számos komoly kiber-roham ellen kellett megvédenie magát a közelmúltban. Példaként említette az egyik erőmű megbénítására és átvételére tett időben észlelt és semlegesített kísérletet. *(Ackerman 2020)* Yosi Shneck az állami tulajdonban lévő közüzemi vállalat, az Israel Electric Corp (IEC) képviselője sajtóközleményben a minisztert megerősítve elismerte, hogy észlelték ugyan az incidenst, azonban nem az IEC üzeme ellen irányult. Az IEC az ország villamos energiájának mintegy 70 százalékát biztosítja, a fennmaradó 30 százalék pedig kisebb magánversenytársaktól származik. Yiftah Ron-Tal IEC elnök arról számolt be, hogy az állami közmű átlagosan 11.000 feltételezett kibertámadással néz szembe másodpercenként, ami a világ egyik legcélzottabb vállalatává teszi. *(Reuters 2020)* 2018-ban a vállalat vezetője a mostanihoz hasonlóan megdöbbentő számokról számolt be – nemzetközi konferencián elhangzott előadásában elmondta, hogy 2017-ben 191 millió IEC elleni támadást regisztráltak, havonta átlagosan 15 milliót. *(Arkin 2018)*

A januári bejelentéssel hozható összefüggésbe az IBM közleménye, amelyben iráni, az állam által támogatott hackerek rosszindulatú programfejlesztéseiről írnak. A ZeroCleare adatmegsemmisítő malware-t az xHunt és APT34 csoportok hozták létre és a közel-keleti térség energiavállalatai elleni kibertámadásokban használták azokat. Az IBM jelentése *(IBM Security 2020)* nem nevezte meg pontosan azon vállalatokat, amelyeket a ZeroCleare támadott. Szaúd-Arábia Nemzeti Kibervédelmi Hatósága már a ZeroCleare fejlettebb verzióját is azonosította. A Dustman elnevezésű adatmegsemmisítő malware Bahrein olajvállalatát, a BAPCO-t támadta részleges sikereket elérve 2019. december 29-én.

Egészségügyi intézmények és vakcinafejlesztő kutatóintézetek információbiztonsági kihívásai

A koronavírus világjárványt kihasználva világszerte az egyik kiemelt célponttá az egészségügyi szektor vált. A Check Point kiberbiztonsági vállalat adatai szerint Izraelben példátlan számú támadás érte az egészségügyi intézményeket 2020. november és 2021. január között. Ez az előző évi adatok alapján 25 százalékos emelkedést jelent, míg világszinten 45 százalékos növekmény tapasztalható. Globálisan átlagosan heti 620 kibertámadás éri az egészségügyi intézményeket, míg a zsidó államban átlagosan heti 813.

Az Izraeli Egészségügyi Minisztérium képviselője 2020. májusi bejelentésében egy egészségügyi szektorban bevezetni tervezett "kibervédelmi pajzs" rövid időn belül felavatásáról beszélt, amelyen a FireEye vállalattal közösen dolgoznak. *(Margit 2020)* A rendszer üzembehelyezéséről még nem tettek közzé híreket, azonban kétségeket, és további kérdéseket vet fel, hogy 2020. decemberben a FireEye-t szofisztikált kibertámadás érte. A cég által használt, a megbízók informatikai rendszerének biztonságát tesztelő ún. Red Team Tools[32] megoldásokat tulajdonítottak el. Az akció mögött közleményük szerint *(Koi 2020)* állami támogatású szervezett kiberbűnözők csoportja, az ún. APT csoport[33] állhat.

A vakcinafejlesztést és engedélyeztetést végző szervezetek, ahogyan bárhol a világon, Izraelben is célponttá váltak. A 2020. májusi támadást követően egy televíziós csatorna forrásmegjelölés nélkül arról számolt be, hogy a hackerek nem információszerzésre, hanem a kutatási folyamatok szabotálására törekedtek. *(The Times of Israel 2020)* A BriLife elnevezésű izraeli COVID-19 vakcinát az 1952-ben alapított kormányzati, a Védelmi Minisztérium irányítása alatt álló Izraeli Biológiai Kutatási Intézetben (IIBR) fejlesztik. *(The Israel Institute of Biological Research)*

Biztosítási ágazat – zsarolás és ügyféladatok kiszivárogtatása

2020. decemberben hatalmas visszhangot kiváltó eseményként érte a Black Shadow hackercsoport támadása a Shirbit biztosítótársaságot. A kiberbűnözők azt követelték, hogy a cég 24 órán belül küldjön 50 bitcoint – az incidens idején 961 110 amerikai dollár értékű

[32] Ezekkel az eszközökkel azt szimulálják, mintha támadók próbálnának behatolni megbízóik rendszereibe – így fedezik fel a sérülékeny, gyenge pontokat, réseket a pajzson.
[33] Angolul: Advanced Persistent Threat, magyarul fejlett, folyamatos fenyegetés.

váltságdíjat, így, ha a pénzt megkapják, akkor nem hozzák nyilvánosságra az ellopott adatokat, és nem értékesítik azokat. A Black Shadow figyelmeztette a Shirbit-et: amennyiben nem fizetnek, a váltságdíj 100 bitcoin-ra emelkedik, újabb 24 óra elteltével pedig 200 bitcoinra, ezt követően viszont már áruba bocsátják a megszerzett bizalmas információkat, megkezdve a fokozatos kiszivárogtatást. Röviddel az üzenet közzététele után fenyegető bizonyítékként a biztosítótársaság ügyfeleinek személyazonosító igazolványait és más érzékeny adatokat tartalmazó fájlokat tett közzé a hackercsoport. A Shirbit ugyan felbérelt egy tárgyalási szakértőt, mégis számos tárgyalási kör és nagy mennyiségű, szakaszosan kiszivárogatott vállalati és ügyféladat után a károsult vállalat bejelentette, hogy nem enged a zsarolásnak, nem szándékozik eleget tenni a Black Shadow fizetési igényének. Az eset után az Izraeli Nemzeti Kiber Igazgatóság (INCD) felszólította a Shirbit ügyfeleit, hogy cseréljék le személyazonosító igazolványukat és vezetői engedélyüket, mivel a kiszivárgott okmányokkal kiberbűnözők visszaéléseket követhetnek el a károkra. *(Bob 2020/1)*

A biztosítótársaság elleni incidens nem volt egyedi, viszont a többivel ellentétben komoly károkat okozott. Izraelben csak novemberben összesen 141 vállalatot ért zsarolóvírus-támadás, októberben pedig 137-et. A megcélzott vállalatok 14 százaléka a csúcstechnológiai ágazatban, 7 százalékuk pedig a biztosítási ágazatban van. A támadások további 11.5 százaléka kormányzati hivatalokat, 5.6 százaléka pedig az egészségügyi szektort érintette. *(Bob 2020/1)*

Logisztika, importszektor, gyártás – az ellátási lánc elleni támadások és védekezés

2020. decemberben az Amital Data szoftvercég szervereinek feltörése mintegy 40 ügyfele elleni támadást tett lehetővé, az ország logisztikai és importszektorának legnagyobb vállalatait érintve. A hackereknek sikerült több tucat vállalat szervereire behatolniuk, ezáltal Izrael ellátási láncába. A megtámadott vállalatok a legnagyobbak közé tartoznak, és egy ilyen támadás súlyosan megzavarhatja az ország alapvető árucikkeinek ellátását. Az ellopott információk stratégiai értéket is jelenthetnek az ellenséges államok számára. Annak ellenére, hogy sikeres volt a behatolás, nem kértek a támadók váltságdíjat, ami felveti annak gyanúját, hogy a cél stratégiai jelleggel az izraeli kritikus infrastruktúra felderítése volt. Az Amital hackelése során kiderült, hogy további 15-20 támadás történt olyan logisztikai cégek ellen, amelyek nem tartoztak az ügyfeleik közé, de a logisztikai, ellátási ágazat szereplői. A támadók módszeres tervet dolgoztak ki a vállalatok feltérképezésére, adataik megszerzésére.

Az érintettek teljes listája még mindig nem ismert, de az Amital ügyfelei között vannak olyanok, amelyek bizalmasan értékesített termékek, köztük katonai felszerelések kereskedelmében érdekeltek. *(Orbach-Hazani 2020)*

A jelentős fenyegetettség miatt 2021. januárban az Izraeli Gyártók Szövetsége (MAI) bejelentette, hogy létrehoz egy irányítása alatt működő, önálló kiberbiztonsági központot a tagjait ellen irányuló, és őket ért támadások kezelésére. A MAI az ágazat szereplőinek ernyőszervezete a jövőben tájékoztató, ismeretterjesztő kampányokkal és olyan szolgáltatásokkal igyekszik védelmet nyújtani az izraeli ipari és üzleti ágazatoknak, mint a valós idejű informatikai támogatás a kibertámadások kezelésében. A megalakulóban lévő védelmi egységhez történő csatlakozásra az izraeli high-tech és kibervédelem elismert és nagymúltú szakértői kaptak felkérést, köztük Refael Franco, az Izraeli Nemzeti Kiber Igazgatóság (INCD) korábbi helyettes vezetője, aki a központ első embere lesz. *(Big News Network 2021)*

Felsőoktatás, a szellemi tulajdon informatikai védelme

Izrael egyetemeihez is számos olyan funkció kapcsolódik, amelyek a létfontosságú infrastruktúrák közé tartoznak. Olyan fizikai és információs-technológiai berendezések – hálózatok, szolgáltatások és eszközök, amelyek összeomlása vagy megsemmisítése súlyos következményekkel járhat a polgárok egészsége, védelme, biztonsága és gazdasági jóléte, illetve a kormányok hatékony működése szempontjából. *(Országos Katasztrófavédelmi Főigazgatóság)* Ilyenek például az egyetemi kórházak, de a haderő és az akadémia együttműködésének köszönhetően érzékeny információk, bizalmas kutatási eredmények is megjelennek az egyetemi informatikai rendszerekben, ezáltal vonzó célponttá teszik azokat.

A legfrissebb, sajtóban is megjelent kiberincidens 2021. januári, a dél-izraeli Ben-Gurion Egyetem szervereibe történő behatolásról szól. Az esetet az Egyetem és az Izraeli Nemzeti Kiber Igazgatóság (INCD) közösen végzett rutinvizsgálatának keretében fedezték fel. Különösen érdekessé teszi, hogy a Ben-Gurion Egyetem Beer-Sheva városában található, amely a haderő és kiberképességek fejlesztésének központja, a felsőoktatási intézmény tevékenysége pedig számos ponton kapcsolódik a védelmi iparhoz. *(Dombe 2021)*

Az izraeli oktatási- és tudásközpontok fenyegetettsége olyan mértékű, hogy önálló ún. CERT[34]-et, azaz számítógép-biztonsági incidenskezelő csoportot hoztak létre a felsőoktatási intézmények és a kutatóhelyek, szoros együttműködésben a kormányzati CERT-el és az iparág piaci szereplőivel. Az Egyetemközi Számítógép Központ[35] az izraeli felsőoktatási intézmények adatbiztonságának javítására irányuló erőfeszítései részeként megalkotott továbbá egy kísérleti környezetet is National Cyber Testbed elnevezéssel, bevonva feltörekvő és veterán információbiztonsági vállalatokat. (*Inter-University Computation Center Cyber & Data Security Services)*

Védelmi ipar fenyegetettsége

Az Iránnal kapcsolatba hozott Pay2Key csoport hackerei 2020. december végén közzétettek egy adatbázist, amellyel azt akarták bizonyítani, hogy behatoltak az Israel Aerospace Industries (IAI) leányvállalata, az ELTA Systems szervereibe. A Pay2Key olyan személyekhez kapcsolódó jogosulatlan adatszerzéssel büszkélkedett, mint Camila Edry, az ELTA kiberprojekt-fejlesztési vezetője, vagy Esti Peshin, kiber-divízió vezérigazgató személyes adatainak közzététele. *(Shmulan 2020)*

Az IAI az ország legnagyobb repüléstechnikai és védelmi vállalata, amely csúcstechnológiát képviselő fegyverek és védelmi rendszerek fejlesztésére és gyártására specializálódott a hadsereg minden ága, valamint a kiber- és a belbiztonság számára. Leányvállalata, az ELTA az egyik vezető védelmi elektronikai szereplőként radarokat, korai előrejelző rendszereket, kommunikációs és hírszerzési technológiákat, elektronikus hadviselési technológiákat és kiberbiztonsági termékeket fejleszt, gyárt és értékesít hazai, illetve nemzetközi, döntően kormányzati ügyfeleknek.

A Pay2Key rosszindulatú szoftvereit több izraeli vállalat elleni zsarolótámadásokra használták fel az elmúlt év végén, érintettek voltak például az Intel tulajdonában lévő Habana Labs szerverei is. Egyelőre nem tisztázott, hogy a perzsa állam támogatta-e az akciót. Bizonyos izraeli kiberbiztonsági szakértők szerint a Pay2Key hivatalosan nem kapcsolódik az iráni rezsimhez, de Iránban található, vagy perzsa nyelvet használó hackerek működtetik. Egyesek úgy gondolják, hogy tetteik kizárólag pénzügyileg motiváltak, és nem kémkedési

[34] Angol megnevezése: Computer Security Incident Response Team.
[35] Angol megnevezése: IUUC – Inter-University Computation Center.

vagy stratégiai célokat szolgálnak. A támadók felderítése közben a zsarolások útján kicsalt bitcion-ok útját követve Iránban található váltókig jutottak el. *(Kahan 2020)* Mások, köztük a ClearSky izraeli kiberbiztonsági vállalat szerint a Pay2Key az iráni Fox Kitten APT csoporthoz köthető, erről részletes jelentést adtak ki még az ELTA Systems elleni incidens előtt. A ClearSky szerint az Amital Data és jelentős izraeli logisztikai cégek elleni támadás is a Pay2Key akciója volt. (*Clearsky Cyber Security Ltd. 2020.)*

Kiber-hidegháború a zsidó és a perzsa állam között

Közel egy évtizede folyamatosan élesedik és egyre látványosabb a kiber-hidegháború Izrael és Irán között. Május 9-én újabb incidenssel került a világsajtó címlapjaira – a dél-iráni Shahid Rajaee kikötő terminálját megbénították, a behatolás következményeként a teherszállítás tíz napig szünetelt. Izraeli válaszcsapásnak tulajdonítják a perzsa állam fentiekben már említett áprilisi akcióját, amelynek keretében az izraeli kritikus infrastruktúra megzavarásának jegyében a vízellátást vették célba – vidéki vízközmű hálózatok szivattyúinak, tározóinak és vízvezetékeinek irányítóközpontjait támadva. *(Haaretz 2020/1)*

A támadás-visszatámadás a két fél között nem ritka jelenség. Amael Cattaruza idézi fel könyvében, hogy a kiberműveletek már szervesen beépültek a katonai doktrínába, és ugyan egyelőre a magánszektorban még nem hallhattunk sok esetről, de Donald Trump kormányának már voltak olyan nagy port kavart elképzelései, mint a „hack back", azaz visszahackelés gyakorlatának alkalmazása. A visszaheckelésre a jogos önvédelem jogosítaná fel a vállalatokat, ellentámadást indíthatnának azok ellen, akiket az őket ért incidenssel gyanúsítanak. *(Cattaruza 2020)*

Ugyan balesetként jelentették a május 10-én az Ómáni Öbölben megtartott iráni gyakorlat során 19 katona életébe kerülő, és 15 főnek sérülést okozó „friendly fire" – azaz baráti tűz rakétatalálatot, egyesek mégis az indítóegészség kompromittálását, és a kiberháború újabb eseményét látják mögötte. *(Marcus 2020)*

Május 21-én a magát Hacking Saviours-nak nevező iráni hátterű csoport a Upress, Izrael egyik legnagyobb tárhelyszolgáltatója elleni sikeres támadásának keretében több ezer honlap tartalmát megváltoztatta. Egyéb beavatkozások mellett a kezdőoldalakat a zsidó állam bukását héberül és angolul hirdető üzenetekre cserélték,[36] és a látogatóktól a böngészőkön

[36] Például: „The countdown of Israel destruction has begun since a long time ago".

keresztül kamerahozzáférési engedélyt kértek. Egyelőre nem tisztázott, hogy a tárhelyszolgáltató adatbázisait törték-e fel. A sérülékenységet egy WordPress (nyílt forráskódú és ingyenes tartalomkezelő rendszer) bővítménye okozta. Szakértők szerint a támadást megelőzően iráni közösségi média oldalakon már felfedték és elemezték ezeket a biztonsági réseket, ezt pedig a kiváltó előzmények, a felkészülés részeként értelmezik. *(Paganini 2020)*

Izrael és az Egyesült Arab Emirátusok normalizált kapcsolatának hatása a kiber-együttműködésekben

Az Egyesült Arab Emirátusok és Izrael közötti kapcsolatok normalizálódásával egyidőben a tudományos- és technológiai együttműködések robbanásszerű bővülését jelzik előre iparági szakértők és gazdasági elemzők. Ugyanakkor a közeledés kibertámadások hadát zúdította az Arab-öbölbeli államra Mohamed Hamad al-Kuwaiti kormányzati kiberbiztonsági vezető nyilatkozata szerint, aki kiemelte a pénzügyi szektorban különösen látványossá vált rosszindulatú incidenseket. *(Haaretz 2020/2)*

Közvetlenül a békeegyezmény bejelentése után számos új közös projekt elindítását kezdeményezték, kiemelten, de nem kizárólag a COVID-19 koronavírus világjárvánnyal való küzdelem jegyében. Várható együttműködési területek: infokommunikáció, biztosítás- és pénzügyi technológiák, agrárinnováció, orvosi technológiák, kockázati tőkebefektetések, élelmiszeripar, sótalanítás és vízgazdálkodás. *(Lyngaas 2020)*

Természetesen nem minden friss bejelentés kapcsolódik előzmények nélküli partnerségekhez. A kapcsolatok normalizálódása előtt is számos példát láttunk a sikeres együttműködésre. Jelentős az izraeli kiberbiztonsági vállalatok dominanciája, akik képviselettel vagy disztribútorral rendelkeznek az arab országban, például a Cybereason, CheckPoint, CyberArk, és az InSights. Az emírségekben más high-tech vállalatok is sikeresek voltak a múltban (is), így a Cato Networks felhőszolgáltatásokat nyújtó izraeli cég, amely szerverfarmot működtet Dubaiban. Ezen vállalatok békeegyezmény előtti beengedése az arab állam piacára is alátámasztja az Izrael iránti bizalom és együttműködési hajlandóság meglétét. *(Alexander 2020)*

Az Izrael elleni bojkott eltörlése lehetővé teszi a két állam vállalatai számára, hogy nyíltan építsenek kapcsolatokat az üzleti, pénzügyi, idegenforgalmi, technológiai, kutatási, energetikai és tudományos szcénában. A technológiai befektetésekhez is hozzájárul az üzleti

tranzakciók könnyítése érdekében aláírt egyetértési szándéknyilatkozat. Keretében vegyesbizottság jön létre, feladata a pénzügyi és beruházási együttműködés támogatása, az akadályok csökkentése és ösztönzők kialakítása. Az Egyesült Államok bevonásával megkötendő háromoldalú megállapodás egyik nevesített célja a kutatás és fejlesztés terén folytatott együttműködés előmozdítása, valamint egy közös innovációs alap létrehozása. Izrael az arab országra elsősorban tehetős, új technológiákra éhes célpiacként tekint. *(Kabir 2020)*

Magyarország és Izrael

Hazánk és Izrael között a nemzetközi szervezetekben sokoldalú együttműködési megállapodásokon keresztül, és kétoldalú alapon is szerveződnek különböző projektek.

Benjámin Netanjahu izraeli miniszterelnök, valamint a visegrádi országok államfői 2017. július 19-én megrendezett budapesti csúcstalálkozóján két munkacsoport létrehozásáról is döntöttek. Ezek egyike a biztonsági együttműködést, a másik pedig a közös kutatási, fejlesztési és innovációs törekvéseket koordinálja. Kiemelt témák voltak a védelmi ipar, a kiberbiztonság, a hibrid fenyegetések, a tömegpusztító fegyverek elterjedésének megakadályozása, valamint az információ és a „know-how” megosztása. *(Israel Ministry of Foreign Affairs 2017)*

Magyarország és Izrael kétoldalú kiberbiztonsági együttműködésének középpontjában a tapasztalatcsere, a szakértői tanácskozások és a technológia-transzfer áll. A vállalati közös fejlesztéseket ipari kutatásfejlesztési együttműködési pályázat szolgálja, amelynek keretösszege 3+3 millió euró, a kiberbiztonság pedig az egyik kiemelt fókuszterület. *(NKFI Hivatal 2019)*

A következő időszakban a pályázati forrás lehetőséget biztosíthat innovatív cégek együttműködésére, de izraeli kockázati tőkebefektetők is érdeklődést mutatnak a magyar ökoszisztéma induló cégei iránt. Szakpolitikai szintéren a szakmai és ernyőszervezetek közeledése, kapcsolatok formalizálása, és megkezdett közös fórumok folytatása várható a közeljövőben.

Kihívások a 2020-as évek kezdetén - parlamenti választások

Az Egyesült Államokban a választási rendszerek már bekerültek a kritikus infrastruktúra felsorolásába, ezzel szemben Izraelben a lebonyolító szervezetek ugyan különleges segítséget kapnak a nemzeti kibervédelmi hatóságtól, de nem azonos típusú felügyelet alatt állnak, mint más kritikus infrastruktúrák. *(Bob 2020/2)*

Mivel Izraelben két éven belül rövidesen negyedik alkalommal is parlamenti választásokat tartanak, Matanyahu Englman államellenőr és ombudsman *(The State Comptroller and Ombudsman of Israel 2019)* bejelentette, hogy hivatala átfogóan áttekinti a Központi Választási Bizottság (CEC) képességét egy potenciális kibertámadás veszélyével való szembenézésre. Englman hivatala azon dolgozik, hogy áttekintse a CEC számítógépes rendszereit, annak tevékenységét az elmúlt három választási fordulóban, és felmérje egy külső kibertámadás kezelésének képességét azzal a szándékkal, hogy lehetővé tegyék a demokratikus szavazás megfelelő lefolytatását, illetve kizárják a külső beavatkozás lehetőségét. *(Joffre 2020)*

A Kibertörvény hiánya

A Miniszterelnöki Hivatal 2018. június 20-án tette közzé a Kiberbiztonságról és Nemzeti Kiber Igazgatóságról (Israel National Cyber Directorate – INCD) szóló törvény tervezetét az Igazságügyminisztérium honlapján. Elfogadásának fontosságában egyetértés volt ugyan, viszont a tervezet szövegezése számos kritikát kapott, a politikai válságnak köszönhetően befagyott a folyamat. A jogszabály hatályba lépése a 2010-ben megkezdett kiberbiztonsági stratégia végrehajtásának utolsó lépése lenne a nemzeti szintű hatóság létrehozásával és a teljes körű működéséhez szükséges jogkörök megadásával. Néhány példa a teljesség igénye nélkül:

- az INCD munkatársai bármilyen kiberbiztonsághoz, a feladataik ellátásához kapcsolódó információ és dokumentum megszerzéséhez, valamint gyűjtéséhez felhatalmazást kaphatnának,
- behatolhatnának nem lakóépületekbe és eszközöket foglalhatnának le,
- lakóingatlanok esetében bírósági végzéssel, vagy a tulajdonos hozzájárulásával léphetnének be,

- kötelező érvényű utasításokat adhatnának állami- és magánszolgáltatóknak a kibertámadások megelőzése, észlelése és az azokra adott válaszok küldésének lehetővé tétele érdekében,
- bírósági végzéseket kérelmezhetnének mintavételi célokhoz, számítógépes műveletek elvégzéséhez – vészhelyzet esetében azonban az INCD vezetője bírósági végzés nélkül is 24 órát meg nem haladó ideig (utólagosan lezajlik a bírósági felülvizsgálati folyamat),
- a magas kockázatú, nemzetbiztonsági és nemzetgazdasági szempontból kiemelt szervezetek az INCD közvetlen irányítása alá kerülhetnek információbiztonsági szempontból, míg az alacsonyabb kockázatúakat rendszeres jelentéstételre kötelezhetik, továbbá puha eszközökkel, például képzésekkel és ajánlásokkal segíthetik. *(Cahane 2018)*

Az Izraeli Nemzeti Kiber Igazgatóságot (INCD) a 2018. december 27-én elfogadott, az állami szervek biztonságának szabályozásáról szóló törvény módosítása hozta létre. *(Levush 2019)* Egyesítette a Nemzeti Kiber Irodát és a Nemzeti Kibervédelmi Hatóságot, továbbá ideiglenes feladatellátást tett lehetővé a Kiberbiztonságról és Nemzeti Kiber Igazgatóságról szóló törvény elfogadásáig. Az INCD küldetését, feladatait és hatásköreit tehát önálló, törvényerejű jogszabály még nem tartalmazza.

Éppen ezért az ország kiber-sebezhetőségével kapcsolatban a szakmai és politikai vitákban gyakran felmerülő téma a fentnevezett törvény hiánya, amely felhatalmazást adna a magánszektor által betartandó kiberbiztonsági szabványok meghatározására, bizonyos esetekben kikényszerítésére, továbbá incidenskezeléskor az állami hatóság azonnali, akár bírósági végzés nélküli beavatkozására.

2019. májusban Joseph Shapira akkori államellenőr és ombudsman[37] jelentésében elmarasztalta a kormányt, amiért befagyott a kibervédelemi sztenderdek magánszektorbeli szabályozásának kezelésére kezdeményezett törvény elfogadásának folyamata. A jelentés szerint a törvény hiánya egyértelműen akadályozza az INCD és más állami kiberbiztonsági szereplők cselekvőképességét, megnehezítve az ország kritikus infrastruktúrájának védelmét. A Miniszterelnöki Hivatal irányítása alatt álló INCD ugyan egyetértett a törvény mielőbbi

[37] Ellenőrzéseket végez és jelentést tesz a minisztériumok, az önkormányzatok és a közszféra különböző szervezeteinek tevékenységeiről annak biztosítása érdekében, hogy azok működése megfeleljen a jogszabályoknak, a jó kormányzás, valamint az integritás és a hatékonyság elvének.

elfogadásának fontosságával, azonban védelmébe vette a kormányzatot, és kiemelte azon innovatív gyakorlatokat, amelyek a törvény elfogadásáig tartó időszakban helyettesítik a jogszabályt. Maga az INCD és azzal együttműködésben a szaktárcák is megalkottak ilyeneket, például a Környezetvédelmi Minisztérium, amely kibervédelmi előírásokat határozott meg a veszélyes hulladékot kezelő vállalatok számára. *(Bob 2020/3)*

Kritikákat a törvénytervezettel kapcsolatban is megfogalmaztak, nem csupán elfogadásának megkésettségével. Ilyenek például a bűnüldöző hatóságokkal való lehetséges hatáskörben, feladatellátásban történő ütközések, a transzparenciához kötődő folyamatok parlament és állampolgárok általi megismerhetőségének hiánya, alkotmányossági aggályok és az állami szervek biztonságának szabályozásáról szóló törvényhez való rendezetlen viszony.

A törvény elfogadása már második éve nem mozdul előre befagyott állapotából, amelyen nem segít, hogy 2020. december 23-án feloszlott a Knesszet, és két éven belül negyedik alkalommal tartanak választást 2021. márciusában. A 2018. óta tartó átmeneti időszakban a kormány által 2015-ben jóváhagyott „hibrid intervencionista-kooperatív" kiberpolitikát folytatják. Ez a megközelítés lehetővé teszi az INCD számára, hogy az ország hatékonyabb védelme érdekében kreatív módon, közvetlenül bevonja a magánszektort a védelmi intézkedésekbe. A főügyész beleegyezésével folytatott gyakorlat keretében nem gyűjtenek személyes információkat egészen addig, amíg nincsen rá konkrét jogalapjuk, továbbá nem rendelkeznek az érintett személy beleegyezésével. Bizonyos esetekben egy szervezet is hozzájárulását adhatja egy egyén képviseletében. Az INCD vezető jogtanácsosának elmondása szerint olyan szerződésmintákat sikerült kidolgozniuk, amelyeket az eseti megállapodások során minden alkalommal elfogadott a másik fél, akinek az informatikai rendszeréhez való hatósági hozzáférést ilyen keretek között biztosították.

A vitákban számos kérdés merül fel azzal kapcsolatban, hogy mi történik akkor, ha egy szervezet nem mutat együttműködési hajlandóságot. Talán az egyik legbonyolultabb kérdés, hogy hol van az a pont, és létezik-e egyáltalán, ahol beleegyezés nélkül beavatkozhat a hatóság egy - akár országos kiterjedtségben megjelenő - veszély elhárítása esetén. A második vitás felvetés a felelősségre vonhatóság kérdésköre. Kihallgatható, és akár büntetőjogi felelősségre vonható-e adott szervezet képviselője, amennyiben elutasítja az együttműködést, ezáltal az ország kiber-ökoszisztémáját veszélyezteti?

A törvény elfogadása után az INCD terve a magánszszférával való kapcsolatainak két szintre bontása. Első körben információkat kérnek be a szervezetektől és útmutatást adnak a kiber események kezelésére. Mivel egy incidens elhárítása akár néhány óra vagy perc

megkésett beavatkozás miatt is veszélybe kerülhet, az INCD vezető jogtanácsosa szerint a legitim beavatkozás egy speciális szaktudással rendelkező és bármikor elérhető bírói testület felállításával biztosítható lenne.

A jogszabály megalkotása, amely felhatalmazást ad egy nagykiterjedésű, nemzetgazdaság egészére vesztélyt jelentő incidens esetén az állami kibervédelmi szervezetek számára az azonnali beavatkozásra, olyan kísérleti projekteket is előmozdíthatna, mint a "világítótorony" elnevezésű digitális vakcinázás. Ennek keretében a kormányzati hatóságok együttműködve a távközlési és a vezető technológiai vállalatokkal azon dolgoznak, hogy "virtuális védőoltásokkal" képesek legyenek a lakosságot immunizálni, továbbá segítsék a már fertőzött eszközök hatékony elszigetelését, megakadályozva a további terjedést. *(The Jerusalem Post 2020/1)*

Ajánlások és Nemzeti Kibervédelmi Koncepció 2.0

A kötelező erejű törvények mellett a puha eszközöket, így az ajánlásokat is folyamatosan fejlesztik Izraelben. 2020. december 15-én a Nemzeti Kiber Igazgatóság (INCD) kiadta a Védekezéselmélet 2.0 elnevezésű koncepció vázlatát, amelyet véleményezhetnek az érintett szereplők írásban, de több videókonferenciát is terveznek a konzultáció keretében. A dokumentum a 2017. évben publikált 1.0-ás verziót jelentősen meghaladja, és a gazdaság szereplőit jó gyakorlatokkal, fontos és praktikus tudással látja el saját szervezeti információbiztonsági stratégiájuk kialakításával kapcsolatban. A végső változat elfogadását és az abban foglalt intézkedések végrehajtását azonban veszélyezteti a politikai válság és a költségvetés hiánya. Az ajánlott intézkedések megfelelő szintű alkalmazását szervezetspecifikus fejezetek létrehozásával igyekeznek elérni. Természetesen vannak olyan kiemelt szereplők, akik ennél is személyre szabottabb támogatást kapnak, stratégiai, nemzetgazdasági fontosságuk miatt az INCD-vel közösen alakítják ki információbiztonsági rendszereiket. *(Israel National Cyber Directorate 2020/1)*

Az állami kiberbiztonsági ügynökség a szervezeti szintű ajánlásokon túl különböző részterületekre fókuszáló, szabályozási és technikai útmutatókat is közzétesz. Ilyenek például a 2021. januárban megjelent, a távmunka és a koronavírus világjárvány miatt minden korábbinál aktuálisabb mobileszköz menedzsment[38] legjobb gyakorlatok gyűjteménye.

[38] Mobile Device Management – MDM és Enterprise mobility management – EMM

Kifejezetten CISO[39] munkakörökre szabva, azaz információbiztonsági vezetőknek is kiadnak tanulmányokat a teljesség igénye nélkül olyan témákban, mint a hardening - magyarul rendszererősítés *(Israel National Cyber Directorate 2019)*, a szervezeten belüli kibervédelmi gyakorlatok lefolytatása, vagy akár az IoT[40] - dolgok internete alapú tűzoltórendszerek és tűzjelzőkhöz kapcsolódó ajánlások. *(Israel National Cyber Directorate)*

Szakemberhiány a kiberbiztonsági ágazatban

A mindösszesen kilencmilliós lakosságszám, a szigorú bevándorláspolitika és munkavállalói vízumkibocsátás komoly kihívás elé állít minden szereplőt, aki a magasan képzett munkaerő képzésében és foglalkoztatásában érdekelt. A kutatás-fejlesztés, innováció és csúcstechnológia iparágai ráadásul elvárják, hogy a humán erőforrás kitermelésekor folyamatos legyen a megújulási képesség, az ágazatok dinamikus változásainak követése.

Csizmadia Norbert Geopillanat című könyvében vezeti le a Világgazdasági Fórum éves versenyképességei jelentéseiben használt háromszintű fejlettségi besorolást: tényező vezérelt gazdaság, hatékonyság vezérelt gazdaság, innováció vezérelt gazdaság. (*Csizmadia 2016)* Izrael ezen osztályozási rendszerben az utolsó, a legfejlettebb lépcsőfokon áll. Jellegzetessége, hogy az embert és közösségeit a legfontosabb értéknek tartja, illetve az adatok felértékeléséből is arra a következtetésre jut, hogy az emberek innovációs és alkalmazkodási képessége a legfontosabb gazdasági erőforrás.

A szakemberhiányt jelzi, hogy 2019. júliusában a Startup Nation Central kutatása szerint 18.500 betöltetlen álláshely volt a high-tech szcénában. *(Israel Innovation Authority - Startup Nation Central 2019)* A technológiai iparban dolgozók körülbelül 50 százaléka dolgozik startup cég alkalmazásában, míg további 50 százalékuk nagyvállalati K+F központokban. A piaci szereplők körében a leggyorsabban fejlődő, innovatív garázscégekre veszélyt jelentenek a multinacionális vállalatok izraeli kutatási, fejlesztési és innovációs fejlesztő központjai, amelyek jelentősen magasabb fizetésekkel és rendkívül vonzó béren kívüli juttatási csomagokkal csábítják el a tehetséges programozókat, mérnököket, üzletfejlesztőket.

[39] Chief Information Security Officer – CISO
[40] Internet of Things

A kiberbiztonsági ágazatban az éves átlagfizetés 275.714 NIS (megközelítőleg 25 millió forint). Az IVC Kutatóközpont 2019-es felmérése szerint a vizsgálat idejében megközelítőleg 20.500 főt foglalkoztató kiber cégeknek legalább további 800 magasan képzett munkavállalóra van szüksége. A teljes foglalkoztatotti létszámból 4.500 fő a külföldi vállalatok izraeli K+F központjaiban, 5.900-an pedig a közszférában dolgoznak. A statisztikában nem szerepel a védelmi vállalatok kiber szakértőinek létszáma. Az ágazat foglalkoztatási rátája évi 12 százalékos növekedést mutatott 2015 és 2018 között. *(Solomon 2019)*

Elsődlegesen továbbra is a legfontosabb kibocsátó a felsőoktatás, de bizonyos területeken, így a kibervédelemben hangsúlyosan jelennek meg más iskolarendszerű és azon kívüli képzési programok, intézmények – például nonprofit szervezetek vagy a hadsereg. Jelentős szerepet kap a középiskolai és általában a nem iskolarendszerű képzések rendszere, továbbá az ökoszisztéma-szemlélet, az érdekelt szereplők szoros együttműködése.

Gal-Ezer, Beeri, Harel és Yehudai „Egy középiskolai számítástudományi program" című tanulmányukban időrendi sorrendet követve igazolják, hogy a számítástechnika oktatásnak jelentős hagyományai vannak Izraelben. Középiskolai tantárgyként az 1970-es évek közepén már bevezetésre került ugyan, igaz, akkoriban még nem teljesértékű, elismert tudományos tárgyként, mint a fizika, biológia vagy kémia. *(Gal et al. 2018)* Napjainkban már egészen fiatal korban elkezdődik a felkészítés és a tehetségek korai felismerése. Olyan óvodák is léteznek, amelyek számítógépes képességfejlesztéssel és robotikával kapcsolatos foglalkozásokat szerveznek. A gyerekek kiberképességekkel való felvértezése egyfajta nemzeti küldetéssé vált. A képzési programok célja, hogy felkészítsék őket a katonai hírszerzésben, a védelmi ügynökségeknél, a high-tech iparban vagy a tudományos életben építendő karrierre. Több izraeli iskolában már negyedik osztályban megkezdik a programozás alapjainak elsajátítását, míg a tehetséges 10. osztályosok tanítás utáni órákon titkosítást és kártékony behatolások megfékezését tanulják.

Számos további, nem kiberbiztonsági, de ahhoz szorosan kötődő fiataloknak szóló iskolai és iskola utáni program zajlik folyamatosan és nagy sikerrel a számítástechnika, a robotika, a mesterséges intelligencia, az űripar és általában az ún. STEM[41] - reáltudományok

[41] Science, Technology, Engineering, and Mathematics

területein. Ezek mögött a jól felismert érdekek miatt egyaránt állnak állami, nonprofit és vállalati szereplők. Kiváló példa erre az Intel 5x2 elnevezésű projektje, amely arra biztatja az izraeli középiskolásokat, hogy a legmagasabb szintű matematikai érettségi vizsgát tegyék le. Ebben az Intel 6000 munkatársa segíti őket önkéntesként, és bőséges költségvetésű program, amelyre az elmúlt négy évben 20 millió sékelt, megközelítőleg 6 millió amerikai dollárt fordítottak. *(Intel 2019)*

A munkaerőhiányt és a korai képzések sikerét jól mutatja, hogy az úgynevezett Magshimim programban 2017-ben végzett 234 hallgatóból 61-en már fizetett állásokban dolgoztak a high-tech iparban még a középiskola elvégzése, és a kötelező sorkatonai szolgálat megkezdése előtt. Átlagolt órabérük ráadásul kétszerese a minimálbérnek, az iskolaszünet hónapjaiban, amikor teljes munkaidőt vállalnak, a felnőtt munkavállalók átlagkeresetét is hazaviszik. *(Leichman 2018)*

Mivel a katonai szolgálat a legtöbb izraeli zsidó fiatalnak a középiskola elvégzése után kötelező – fiúknak és lányoknak egyaránt, ezért az Izraeli Védelmi Erők (IDF[42]) is érdekeltté válik és profitál a fiatal tehetségekbe történő befektetésből. Két kiber-képzési programból érkeznek a katonák a nemzetközileg is elismert ún. 8200-as Hírszerző Egységbe, amely a digitális kommunikáció elfogására és a közel-keleti ellenséges államokkal kapcsolatos hírszerzési tevékenységre szakosodott. Az Egység számos korábbi tagja végül a csúcstechnológiai és kiberbiztonsági iparágban kezd karriert, a legsikeresebb vállalatokat 8200-as veteránok alapították. *(Estrin 2018)* Osnat Lautman az izraeli high-tech üzleti siker titkát kereső könyvében írja, hogy a speciális egység katonáiból startupperekké vált vállalkozók szoros kapcsolatot ápolnak egymással, ezt úgy hívják maguk között, hogy a „biztonsági hálózat". Ezekből az informális és formális szálakból jelentős előnyöket kovácsolnak akár a politikai, akár az üzleti életben. *(Lautman 2015)* A leírtak teljes mértékben összecsengenek Barabási Albert-László „A képlet" c. könyvének több törvényével, különösen a hármas számúval, amely kimondja, hogy az alkalmasság korábbi sikerekkel párosítva jövőbeni sikerekhez vezet, és ha az előbbihez társas befolyásolás kapcsolódik, akkor a siker nem ismer korlátokat. *(Barabási 2018)*

Az IDF nem csupán a hadseregbe belépő, a katonai szolgálatra felkészülő fiatalok felkészítésére tekint befektetésként, hanem a leszerelő hadfiak elhelyezkedési lehetőségeinek

[42] Israeli Defense Forces.

támogatására is. Utóbbi motiváció okán indították el az úgynevezett Cyber4s elnevezésű, frissen leszerelt izraeli katonák kiberbiztonsági képzésére kidolgozott féléves képzési programot. Keretében a kiberipar junior pozícióira képeznek ki korábban kiemelt fontosságú, a harcoló alakulatokban, de nem technológiai pozíciókban szolgálatot teljesítő exkatonákat. A kezdeményezés a koronavírus világjárvány okozta munkaerőpiaci kihívások kezelésében is segítséget nyújt a résztvevőknek és az őket alkalmazó vállalatoknak. *(Solomon 2020)*

A Shabak, Izrael belbiztonsági szolgálatának célja, hogy megvédje az országot a kémkedéstől és a terrorizmustól. Jelmondatához híven – „a láthatatlan pajzs" a legfejlettebb hírszerző és elhárító technológiai eszközök alkalmazói és egyúttal fejlesztői is. Az országhatárokon belüli kémkedés felderítése, megelőzése, a közéleti, politikai vezetők személyes biztonságának fenntartása, a terrorizmus elleni harc, az állami stratégiai eszközök védelme megkövetelik a kibervédelmi képességek legmagasabb szintjét. Ennek megfelelően a Technológiai és Kiber Divízió folyamatosan arra törekszik, hogy a legjobb szakértőket toborozza. A tanulmány írásakor hatvannál is több, döntően fejlesztői és technológiai projektmenedzseri álláspályázatot hirdet a belbiztonsági szolgálat. *(Shabak 2020)*

Számos piaci szereplő, ún. „code school" – programozóiskola is kínál olyan képzéseket, amelyek elvégzése után elérhetővé válnak a high-tech szektor, és akár a kiberbiztonsági vállalatok junior pozíciói. Ilyen például az Israel Tech Challenge (ITC), amely az IDF 8200-as elit egysége által ihletett képzési modulokat kínál. Olyan nagyvállalatok vesznek részt a tananyagfejlesztésben, mint az Intel, az Apple, a Samsung, a Dell vagy a HP. A munkaerőhiány és e cégek érdekeltsége teszi lehetővé a 4-5 hónapos tanulás egyedülálló finanszírozási modelljét: a diák számára egészen addig térítésmentes, amíg nem találnak megfelelő, jól fizető munkát. A tandíjat tehát utólagosan fizetik vissza, ha az új állásukban egy bizonyos összegnél többet keresnek. *(Secret Tel-Aviv 2018)*

Konklúzió

2020 bizonyára vastag betűkkel és fájdalmas emlékekkel írja be magát a történelemkönyvekbe. Nincsen olyan ország és ágazat, amelyet ne szőne körül és fojtogatna a vírus. Izrael ugyanúgy, ahogyan az egész világ óriási károkat szenvedett, és szenved még a cikk megírásakor is a világjárvány következményei miatt.

A kiberbűnözők és más rosszindulatú támadók mindig megtalálják azokat a gyenge pontokat, amelyeket haszonszerzésre vagy károkozásra használhatnak. Ezt támasztja alá Fehér

Krisztián információbiztonsági szakértő, világossá téve, hogy a számítástechnika eredendően, felépítéséből adódóan sérülékeny, így két megoldás együttes alkalmazása érhet el eredményt: a használatot még nem ellehetetlenítő ún. rendszererősítés – azaz a rosszindulatú szereplők számára túl körülményessé tenni a behatolást, a második elem pedig a felhasználói tudatosság magas fokának elérése. *(Fehér 2016)* A biztonság tehát egy mítosz - még egy olyan országban is, ahol a kibervédelem széleskörű oktatása már egész fiatal korban elkezdődik, ahol a húzóágazat a high-tech, és az emberek ösztöneibe kódolva él az éberség és a gyanakvás. Ez számunkra nem hiteltelenséget vagy reputációvesztést kell, hogy jelentsen, sokkal inkább figyelmeztetést. A hackerek és az APT csoportok módszerei egyre kifinomultabbak, életünk pedig csak bonyolultabb és gyorsabb lesz, megnehezítve egy átverés észlelését.

Izrael a fejlett kiber-ellenállóképessége mellett is számos kihívással küzd, ahogyan azt a cikk is bemutatta, ezeket viszont jól kezelte, és a rendkívül súlyos incidensekben is kevés sebet szerzett. 2020-ban mindemellett öt úgynevezett unikornist, azaz 1 milliárd amerikai dollár értékű kibervédelmi vállalatot termelt ki. Összesen 2.9 milliárd amerikai dollárnyi befektetés landolt az ágazat piaci szereplőinél, több, mint 100 ügylet keretében, a kiberipar pedig 6.85 milliárd amerikai dollár értékű exportot termelt a nemzetgazdaságnak. Ezek a számok azt eredményezték, hogy 2021 elején a világ összes unikornisának 33 százaléka izraeli cég, a globálisan összegzett befektetéseknek pedig 31 százaléka került a kiber-nemzet startup és scale-up vállalkozásihoz. *(Israel National Cyber Directorate 2020/2)*

Az izraeli kiber-ágazat kiemelkedő üzleti eredményei és a ránehezedő nyomás ellenére a védelmi képességek kiállták a próbát. Minden bizonnyal 2021 sem lesz nyugodtabb év az előzőnél, a legjobb stratégia pedig valószínűleg a nemzetközi együttműködés megerősítése és a legjobb gyakorlatok cseréje lesz – ezekben pedig Magyarország és Izrael közös sikereket érhet el.

Irodalomjegyzék

BARABÁSI A. L. (2018) *A képlet*. Budapest, Libri, ISBN 978-963-433-191-9. pp. 117.

CATTARUZA, A. (2020) *A digitális adatok geopolitikája*. Budapest, Pallas Athéné Könyvkiadó. ISBN 978-615-5884-95-5. pp. 92.

CSIZMADIA N. (2016) *Geopillanat*. Budapest, L'Harmattan Kiadó. ISBN 978-963-414-147-1. pp. 211-212.

FEHÉR K. (2016) *Kezdő hackerek kézikönyve*. Budapest, BBS-INFO Kiadó. ISBN 978-615-5477-44-7. pp. 25.

FEHÉR K. (2018) *Hacker-technikák*. Budapest, BBS-INFO Kiadó. ISBN 978-615-5477-65-2. pp. 48.

LAUTMAN, O. (2015) *Israeli Business Culture*. ISBN 978-965-92504-5-5. pp. 42.

MARSHALL, T. (2016) *A földrajz fogságában*. Budapest, Park Könyvkiadó. ISBN 978-963-355-411-1. pp. 10.

PAPP-VÁRY Á. (2019) *Országmárkázás*. Budapest, Akadémiai Kiadó. ISBN 978-963-454-345-9. pp. 41.

Internetes források

ACKERMAN, G. (2020) *Israel Power Plants Have Fended Off Cyber Attacks, Minister Says*. Bloomberg. https://www.bloomberg.com/news/articles/2020-01-29/israel-power-plants-have-fended-off-cyber-attacks-minister-says [Letöltve: 2021.01.03.].

ALEXANDER, K. (2020) *Israeli-Gulf cyber cooperation*. Modern Diplomacy. https://moderndiplomacy.eu/2020/12/23/israeli-gulf-cyber-cooperation/ [Letöltve:2021.01.12.].

ARKIN, D. (2018) *The world needs multi-layered, multi-dimensional cybersecurity systems.* Israel Defense. https://www.israeldefense.co.il/en/node/32887 [Letöltve: 2021.01.04.].

BIG NEWS NETWORK (2021) *Israeli manufacturers launch cybersecurity HQ following rise in attacks.* https://www.bignewsnetwork.com/news/267448715/israeli-manufacturers-launch-cybersecurity-hq-following-rise-in-attacks [Letöltve: 2021.01.07.].

BOB, Y. J. (2020) *Cyber authority to victims post-Shirbit hack: Get new identity cards.* The Jerusalem Post. https://www.jpost.com/breaking-news/shirbit-hackers-to-leak-more-documents-by-9-am-if-money-not-received-651276 [Letöltve: 2021.01.06.].

BOB, Y. J. (2020) *NSA, Israeli, UK cyber chiefs confront new hacker threats in corona era*. The Jerusalem Post. https://www.jpost.com/jpost-tech/nsa-israeli-uk-cyber-chiefs-confront-new-hacker-threats-in-corona-era-639475 [Letöltve: 2021.01.13.].

BOB, Y. J. (2020) *With no cyber law, can gov't stop Shirbit-style cyberattacks?* The Jerusalem Post. https://www.jpost.com/israel-news/cyber-lawyer-to-post-law-needs-amending-to-bolster-cybersecurity-650949 [Letöltve: 2021.01.14.].

CAHANE, A. (2018) *The New Israeli Cyber Draft Bill – A Preliminary Overview*. The Federmann Cyber Security Research Center. https://csrcl.huji.ac.il/news/new-israeli-cyber-law-draft-bill#_ftn1 [Letöltve: 2021.01.14.].

CLEARSKY CYBER SECURITY LTD. (2020) *Pay2Kitten - Pay2Key Ransomware – A New Campaign by Fox Kitten*. https://www.clearskysec.com/wp-content/uploads/2020/12/Pay2Kitten.pdf [Letöltve: 2021.01.09.]

DOMBE, A. R. (2021) *Servers of Ben Gurion University breached*. Israel Defense. https://www.israeldefense.co.il/en/node/47630 [Letöltve: 2021.01.08.].

ESTRIN, D. (2018) *In Israel, teaching kids cyber skills is a national mission*. The Times of Israel. https://www.timesofisrael.com/in-israel-teaching-kids-cyber-skills-is-a-national-mission/ [Letöltve: 2021.01.20.].

GAL-EZER, J., BEERI, C., HAREL, D. & YEHUDAI, A. (2018) *A High-School Program in Computer Science*. The Open University of Israel. https://www.openu.ac.il/personal_sites/download/galezer/high-school-program.pdf [Letöltve: 2021.01.18.].

HAARETZ (2020) *Iran Says One of Two 'Large Scale' Cyber Attacks Targets Country's Ports.* https://www.haaretz.com/israel-news/tech-news/iran-says-one-of-two-cyber-attacks-targets-country-s-ports-1.9239908 [Letöltve: 2021.01.09.].

HAARETZ (2020) *UAE Hit With Cyberattacks in Response to Ties With Israel, Official Says.* https://www.haaretz.com/israel-news/tech-news/uae-hit-with-cyberattacks-in-wake-of-israel-deal-official-says-1.9351738 [Letöltve: 2021.01.10.].

IBM SECURITY (2020) *New Destructive Wiper "ZeroCleare" Targets Energy Sector in the Middle East*. https://www.ibm.com/downloads/cas/OAJ4VZNJ [Letöltve: 2021.01.04.].

INTEL (2019) *Intel in Israel*. https://www.intel.com/content/www/us/en/corporate-responsibility/intel-in-israel.html [Letöltve: 2021.01.19.].

INTER-UNIVERSITY COMPUTATION CENTER CYBER & DATA SECURITY SERVICES. https://www.iucc.ac.il/en/infrastructuretechnologies/cyber/ [Letöltve: 2021.01.08.].

ISRAEL CYBER ALLIANCE, *Cyber security is Israel*. https://israelcyberalliance.com/cyber-security-in-israel-2/ [Letöltve: 2021.01.02.].

ISRAEL INNOVATION AUTHORITY - STARTUP NATION CENTRAL (2019) *High Tech Human Capital Report 2019*. https://www.startupnationcentral.org/wp-content/uploads/2020/02/Start-Up-Nation-Centrals-High-Tech-Human-Capital-Report-2019-2.pdf [Letöltve: 2021.01.17.].

ISRAEL MINISTRY OF FOREIGN AFFAIRS (2017) *Israel - Visegrad Group Joint Statement.* https://mfa.gov.il/MFA/PressRoom/2017/Pages/Israel-Visegrad-Group-Joint-Statement.aspx [Letöltve: 2021.01.12.].

ISRAEL NATION CYBER DIRECTORATE. Cyber protection for the organization. https://www.gov.il/he/departments/topics/organization_cyber_protection [Letöltve: 2021.01.16.].

ISRAEL NATIONAL CYBER DIRECTORATE (2020) *Draft public address on improvements and additions to defense theory*. https://www.gov.il/he/departments/publications/Call_for_bids/tohag_draft [Letöltve: 2021.01.16.].

ISRAEL NATIONAL CYBER DIRECTORATE (2020) *The Israeli cyber industry continues to grow: record fundraising in 2020*. https://www.gov.il/en/departments/news/2020ind [Letöltve: 2021.01.28.].

ISRAEL NATIONAL CYBER DIRECTORATE (2020) *The Israeli Police Cyber Unit arrested suspects of stealing hundreds of thousands of ILS from Israeli citizens.* https://www.gov.il/en/departments/news/accounttakeover [Letöltve: 2021.01.03.].

ISRAEL NATIONAL CYBER DIRECTORATE (2019) *Best Practices Hardening Computer Systems.* https://www.gov.il/BlobFolder/generalpage/hardingcomputersystem/en/hardening.pdf [Letöltve: 2021.01.06.].

JOFFRE, T. (2020) *State comptroller to review preparedness for cyberattack on elections*. The Jerusalem Post. https://www.jpost.com/israel-news/state-comptroller-to-review-preparedness-for-cyberattack-on-elections-651380 [Letöltve: 2021.01.13.].

KABIR, O. (2020) *UAE views Israel as a strategic cybersecurity partner, says head of national cyber authority*. Calcalist. https://www.calcalistech.com/ctech/articles/0,7340,L-3874096,00.html [Letöltve: 2021.01.12.].

KAHAN, R. (2020) *Pay2Key hackers claim they breached IAI servers*. Calcalist. https://www.calcalistech.com/ctech/articles/0,7340,L-3883010,00.html [Letöltve: 2021.01.09.]

KOI, T. (2020) *Kiberfegyvereket loptak el a FireEye-től.* HWSW. https://www.hwsw.hu/hirek/62656/fireeye-red-team-betores-hacker-kiberbiztonsag.html [Letöltve: 2021.01.05.].

LEICHMAN, A. K. (2018) *The Israeli high-school kids earning high-tech salaries*. Israel21C. https://www.israel21c.org/the-israeli-high-school-kids-earning-high-tech-salaries/ [Letöltve: 2021.01.19.].

LEVUSH, R. (2019) *Israel: Knesset Passes Amendment Law Recognizing Role of National Cyber Directorate in Protecting Cyberspace.* The Library of Congress. https://www.loc.gov/law/foreign-news/article/israel-knesset-passes-amendment-law-recognizing-role-of-national-cyber-directorate-in-protecting-cyberspace/ [Letöltve: 2021.01.14.].

LYNGAAS, S. (2020) *Israel, UAE say they're allies in cyberspace. They have plenty of tech power to draw upon*. CyberScoop. https://www.cyberscoop.com/israel-uae-cybersecurity-deal-tech-firms/ [Letöltve: 2021.01.10.].

MARCUS, J. (2020) *Iran navy 'friendly fire' incident kills 19 sailors in Gulf of Oman*. BBC. https://www.bbc.com/news/world-middle-east-52612511 [Letöltve: 2021.01.09.].

MARGIT, M. (2020) *Israel to launch 'Cyber Defense Shield' for health sector*. The Jerusalem Post. https://www.jpost.com/israel-news/israel-to-launch-cyber-defense-shield-for-health-sector-627304 [Letöltve: 2021.01.05.].

NKFI HIVATAL (2019) *Magyar-izraeli ipari kutatásfejlesztési együttműködési pályázat.* https://nkfih.gov.hu/palyazoknak/nkfi-alap/magyar-izraeli-ipari-kf-egyuttmukodesi-palyazat/2019-2110-tet-il [Letöltve: 2021.01.12.].

NOCAMELS (2020) *Israel Is Number 1 Target For Hackers And Cybercriminals – Report.* https://nocamels.com/2020/12/israel-target-hackers-cybersecurity-cybercriminals/ [Letöltve: 2021.01.02.].

ORBACH, M. & HAZANI, G. (2020) *Israel's supply chain targeted in massive cyberattack.* Calcalist. https://www.calcalistech.com/ctech/articles/0,7340,L-3881337,00.html [Letöltve: 2021.01.07.].

ORSZÁGOS KATASZTRÓFAVÉDELEMI FŐIGAZGATÓSÁG. *A kritikus infrastruktúra*. https://regi.katasztrofavedelem.hu/index2.php?pageid=lrl_index [Letöltve: 2021.01.08.].

PAGANINI (2020) *Tens of thousands Israeli websites defaced*. Security Affairs. https://securityaffairs.co/wordpress/103570/hacktivism/israeli-websites-defaced.html [Letöltve: 2021.01.10.].

PAYCALE (2021) *Salary for Skill in Israel: Cyber Security*. https://www.payscale.com/research/IL/Skill=Cyber_Security/Salary/Page-4 [Letöltve: 2021.02.].

REUTERS (2020) *Israel says it thwarted serious cyber attack on power station.* https://www.reuters.com/article/us-israel-cyber-powerstation/israel-says-it-thwarted-serious-cyber-attack-on-power-station-idUSKBN1ZS1SU [Letöltve: 2021.01.04.].

SECRET TEL AVIV (2018) *Best Coding And Tech Schools In English In Tel Aviv*. https://www.secrettelaviv.com/magazine/blog/useful-info/best-coding-schools-in-english-in-tel-aviv [Letöltve: 2021.01.23.].

SHABAK (2020) *Career in the Shin Bet*. https://www.shabak.gov.il/career/jobs/Pages/TechnologicalUnits.aspx?pk_campaign=quiz&pk_kwd=klali-3001#cbpf=* [Letöltve: 2021.01.22.].

SHMULAN, E. (2020) *Iranian Hackers Test Israeli Cyber Mettle*. Mishpacha. https://mishpacha.com/iranian-hackers-test-israeli-cyber-mettle/ [Letöltve: 2021.01.08.]

SOLOMON, S. (2019) *Israel cybersecurity sector hamstrung by shortage of labor, report says.* The Times of Israel. https://www.timesofisrael.com/israel-cybersecurity-sector-hamstrung-by-shortage-of-labor-report-says/ [Letöltve: 2021.01.02.].

SOLOMON, S. (2020) *Program arms discharged fighters with cyberskills, wins IDF Chief of Staff award.* The Times of Israel. https://www.timesofisrael.com/progam-arms-discharged-fighters-with-cyberskills-wins-idf-chief-of-staff-award/ [Letöltve: 2021.01.22.].

THE ISRAEL INSTITUTE FOR BIOLOGICAL RESEARCH (IIBR). https://iibr.gov.il/Pages/Who-We-are.aspx [Letöltve: 2021.01.06.].

THE JERUSALEM POST (2020) *Israel must use Intelligence to mitigate cyber attacks: official.* https://www.jpost.com/cybertech/israel-must-use-intelligence-to-mitigate-cyber-attacks-senior-official-632012 [2021.01.15.].

THE JERUSALEM POST (2020) *Israel Police reports a staggering 8,377 cyberattacks for 2020.* https://www.jpost.com/jpost-tech/israel-police-reports-a-staggering-8377-cyberattacks-for-2020-653378 [Letöltve: 2021.01.03.].

THE STATE COMPTROLLER AND OMBUDSMAN OF ISRAEL (2019) *Matanyahu Englman. State Comptroller and Ombudsman of the State of Israel.* https://www.mevaker.gov.il/En/About/mevakrim/Pages/Englman.aspx [Letöltve: 2021.01.13.].

THE TIMES OF ISRAEL (2020) *Israeli vaccine research centers reportedly among sites targeted by hackers.* https://www.timesofisrael.com/israeli-vaccine-research-centers-reportedly-among-sites-targeted-by-hackers/ [Letöltve: 2021.01.05.].