Sipos Zoltán százados

A STUXNET HATÁSA IRÁN INFORMATIKAI HADVISELÉSÉRE

DOI: 10.35926/HSZ.2023.4.2

ÖSSZEFOGLALÓ: *Talán emlékszik az olvasó arra a 2010-ben nyilvánosságra került hírre, amely szerint Irán atomprogramját egy Stuxnet elnevezésű számítógépes vírus két évre visszavetette azzal, hogy a Natanzban található urándúsító centrifugák egyötödét tönkretette. A művelet súlyos károkkal járt, de úgy tűnik, Irán méltó választ adott erre a vírusra és az azt követő támadásokra, ugyanis erős informatikai hadviselő potenciált fejlesztett ki, amellyel visszavágott az őt ért támadásokkal gyanúsított Amerikai Egyesült Államoknak és szövetségeseinek. Napjainkban potenciálja révén képes jelentős károkat okozni a kritikus infrastrukturális hálózatokban, valamint kiterjedt információgyűjtő kibertevékenységet folytat gyakorlatilag az egész fejlett világban.*

KULCSSZAVAK: *informatikai hadviselés, Irán, Stuxnet, kibertámadás*

A SZERZŐRŐL:
Sipos Zoltán százados, PhD-hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola (ORCID: 0000-0001-7017-571X; MTMT: 10066823)

BEVEZETÉS

Az internet elterjedésének kezdetén a kibertérben jórészt a bűnözők és a bűnüldöző szervek vívták az akkor még korántsem jelentős mértékű harcaikat. Jellemzően személyi adatokkal való visszaélés, adatlopás és hitelkártyacsalások okoztak fejtörést az illetékeseknek. A jóindulatú vagy „tréfás" kedvű hekkerek megbénítottak egy-egy weboldalt, kicseréltek egyes weblapokat leginkább azzal a céllal, hogy tudásukkal kérkedjenek. Azokban az időkben még senki sem gondolta – vagy legalábbis nem sokan –, hogy majd nosztalgiával gondolnak vissza ezekre a „boldog békeidőkre". Nem lehet pontosan meghatározni, hogy a kibertér szerepe mikor változott meg.

Nem ismeretes az sem, melyik állam volt az első, amely hadszíntérként tekintett az addig „békés" közegre. A felszínre került eseményekből és tudósításokból konkrét információk hiányában azonban sejthető, hogy ezen a téren a főbb szereplők az Amerikai Egyesült Államok, az Oroszországi Föderáció és a Kínai Népköztársaság voltak. Gyanítható az is, hogy Izrael és Irán is kiveszi a részét az ilyen tevékenységekből. Írásomban ez utóbbival kívánok részletesebben foglalkozni. Nehézségekbe ütközik Iránnal[1] kapcsolatban ilyen vonatkozású információt gyűjteni, mivel az ország társadalmi berendezkedésénél fogva cenzúrázza a befelé és a kifelé történő információáramlást.

[1] Carmen-Cristina Cirlig: Cyber Defence in the EU – Preparing for Cyber Warfare? European Parliamentary Research Service, 10. 2014. http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf (Letöltés időpontja: 2022. 05. 01.)

Szakértők Irán belépését az informatikai hadszíntérre az ország atomprogramját 2010-ben ért súlyos támadást követő időszakra teszik. Talán nem kell emlékeztetni az olvasót arra a hírre, hogy a Stuxnet[2] elnevezésű számítógépes program tönkretett több száz urándúsító centrifugát Natanzban.[3] A támadással mintegy két évvel visszavetették az iráni atomprogramot, valamint jelentős anyagi és erkölcsi károkat is okoztak. Szakértők tudni vélik, hogy a programot állami támogatás mellett amerikai és izraeli programozók készítették.[4] A támadás azon alapult, hogy az MS Windows operációs rendszer egyik sérülékeny pontját kihasználva a Siemens cég által gyártott ipari berendezéseket vezérlő rendszer egyik programozható chipjébe kártékony kódot juttattak be, amely aztán egy speciális algoritmus alapján használhatatlanná tette az urándúsító centrifugákat. A dolog érdekessége, hogy az irániak nem eredeti Siemens termékeket használtak, mert ezek embargó alá estek, hanem valahonnan becsempészték országukba a berendezéseket, ezért nem reklamálhattak a Siemensnél. A történtekről ma már számos esettanulmány áll rendelkezésre a világhálón, akit érdekel, az könnyen kielégítheti ilyen irányú érdeklődését.

Iráni részről nagy volt a felháborodás, amikor világossá vált számukra, hogy támadás áldozatai lettek.[5] Ettől kezdve Irán sebességet váltott, és a későbbi események fényében valószínűsíthető, hogy elszánt bosszúhadjáratba kezdett.

Az igazsághoz hozzátartozik, hogy nem teljesen a nulláról kellett indulniuk. A különböző minőségi programozói fórumokon nagyon sok tehetséges fiatal iráni szakember szerepelt aktívan, amiből arra lehet következtetni, hogy az oktatásban nagy hangsúlyt fektettek, fektetnek a számítástechnikára. Figyelemre méltó ez annak tükrében, hogy az Amerikai Egyesült Államokkal hosszú évek óta fennálló konfliktushelyzetben nem számíthattak olyan fokú segítségre például a Microsofttól, mint a térség egyes arab országai.[6] A Stuxnet-támadást követően az iráni vezetés úgy döntött, hogy a kiberhadviselés terén belép a 21. századba, és komoly szervezésbe kezdett, aminek eredményeként több szervezetet hozott létre.

IRÁN KIBERHADVISELŐ SZERVEZETÉNEK FELÉPÍTÉSE[7]

A komplex és többszintű szervezet elsődleges célja Irán kiberhadműveleteinek koordinálása, vagyis az ország ellen irányuló védelmi és az ellenség elleni támadó jellegű feladatok, valamint az iszlámellenes belső ellenzék elleni harc tervezése, szervezése, koordinálása és végrehajtása.

---

[2] David Kushner: The Real Story of Stuxnet: How Kaspersky Lab Tracked down the Malware that Stymied Iran's Nuclear-fuel Enrichment Program. IEEE Spectrum, 26. 02. 2013. https://spectrum.ieee.org/the-real-story-of-stuxnet (Letöltés időpontja: 2013. 02. 26.)

[3] Operation Cleaver. Cylance Report. https://scadahacker.com/library/Documents/Cyber_Events/Cylance%20-%20Operation%20Cleaver%20Report.pdf (Letöltés időpontja: 2023. 03. 01.)

[4] David Siman-Tov – Shmuel Even: A New Level in the Cyber War between Israel and Iran. Institute for National Security Studies Insight No. 1328, 03. 06. 2020. https://www.jstor.org/stable/pdf/resrep25542.pdf?refreqid=excelsior%3A023709b6886c27c75429d01008d785c8&ab_segments=&origin=&initiator=&acceptTC=1 (Letöltés időpontja: 2022. 05. 01.)

[5] Collin Anderson – Karim Sadjadpour: Iran: Target and Perpetrator. In: Collin Anderson – Karim Sadjadpour: Irans's Cyber Threat: Espionage, Sabotage and Revenge. Carnegie Endowment for International Peace, 2018, 9–16. https://www.jstor.org/stable/pdf/resrep26913.8.pdf?refreqid=excelsior%3Af32c6251b9ed7a22d0d5c0ac0bd1402c&ab_segments=&origin=&initiator=&acceptTC=1 (Letöltés időpontja: 2023. 03. 01.)

[6] Ben Hubbard: MBS: The Rise to Power of Mohammed Bin Salman. Tim Duggan Books, New York, 2020, 231.

[7] Kevin Lim: Iran's Cyber Posture. Open Briefing, 18. 11. 2013. https://www.openbriefing.org/intelligence-desks/middle-east-and-north-africa/irans-cyber-posture/ (Letöltés időpontja: 2023. 03. 10.)

Az iráni kiberhadviselés szervezetét az egyes források különféleképpen nevezik meg: *Kiberhadsereg* (The Cyber Army), *Iráni Kiberhadsereg* (The Iranian Cyber Army), *Az Iszlám Forradalmi Gárda Kiberhadserege* (The Cyber Warfare Division of the Islamic Revolutionary Guard Corps) és *Iráni Különleges Műveleti Szervezet* (The Iranian Special Operations Organization). Ez a szervezet az országban működő több katonai és biztonsági szervezetet foglalja magában. Az iráni kiberharcosok elsősorban politikai és vallási szervezetek, valamint gazdasági célpontok ellen tevékenykednek, továbbá kibertámadásokat hajtanak végre az iráni kormány ellenfelei ellen, illetve az ország ellen irányuló külföldi támadások elhárítása érdekében.

Az iráni kiberharcosok által végrehajtott támadások között szerepelnek számos bank és kormányzati szerv ellen indított túlterheléses (DDoS[8]) támadások,[9] valamint bankszámlák feltörése és elektronikus kommunikációs hálózatok megbénítása. Az iráni kiberhadviselők szintén felelősek az Amerikai Egyesült Államokat és más nyugati országokat érintett különböző hekkertámadásokért és adatlopásokért. Az irániak több esetben is együttműködnek az említett országok ellenségeivel is. Így például aktívan részt vettek/vesznek a zimbabwei hírszerzés kiberhadviselési, lehallgatási képességeinek létrehozásában és működtetésében.[10] Ez annak tükrében érthető, hogy az iráni kiberhadviselés az elmúlt években jelentősen megnövelte kapacitását, és az egyik legfejlettebb és legaktívabb kiberharcos csoportnak számít a világon.[11]

A Kibertér Legfelsőbb Tanácsa (Shoray-e Aali-e Fazaye Majazi)

A 2012 márciusában létrehozott legfelsőbb kormányzati testület feladata a legfelsőbb szintű kiberháborús alapelvek kidolgozása. A Tanács megalakulásától kezdve a kibertevékenységben érintett összes iráni szervezetnek (vállalat, iskola, kormányzati szerv stb.) a kidolgozott alapelveknek megfelelően kell működnie. Tagjai az iráni elnök, a legfelsőbb bíró, a parlament elnöke, a rádió és televízió elnöke, az Iszlám Forradalmi Gárda vezérkari főnöke, valamint a belügy-, a titkosszolgálati, a telekommunikációs, továbbá a tudományos és kulturális miniszter.

Kibervédelmi Parancsnokság (Gharargah-e Defa-e Saiberi)

A szervezet 2010 novemberétől működik az Országos Polgári Védelmi Szervezet (Sazeman-e Padafand-e Gheyr-e Amel) felügyelete alatt. Ez utóbbit 2003-ban hozták létre Hámenei ajatollah parancsára. Maga a védelmi szervezet a vezérkar egyik csoportfőnöksége, a megalakulását követően 2011-ig a Polgári Védelmi Szervezet Állandó Bizottságának volt alárendelve, majd elnöki jóváhagyással átkerült a vezérkari főnök alárendeltségébe. A Polgári Védelmi Szervezet titkárának feladata a kormányzati szervek nem katonai jellegű védelmi tevékenységének a koordinálása – óvóhelyek építése, passzív rendszabályok, mint például az álcázás stb.

---

[8] Distributed Denial of Service.

[9] Frank Umbach: Critical Energy Infrastructure at Risk of Cyber Attack. Konrad Adenauer Stiftung International Reports No. 9/2012., 35–66. https://www.jstor.org/stable/pdf/resrep09954.pdf?refreqid=excelsior%3A44e55c3522be8780d7dfce13e6864a6a&ab_segments=&origin=&initiator=&acceptTC=1 (Letöltés időpontja: 2023. 01. 20.)

[10] János Besenyő: Zimbabwe: An Intelligence Community against Each Other and Everyone. In: Ryan Shaffer (ed.): The Handbook of African Intelligence Cultures. Rowman and Littlefield, 2023, 731–746.

[11] Rafał Wisniewski et al.: Beyond Europe – Reconnecting Eurasia. Logos Verlag Berlin, 2019.

A Kibervédelmi Parancsnokság létrehozásának ötlete már korábban felmerült a szervezet részéről, de létrehozását csak a Stuxnet-támadást követően tudták elérni. A Parancsnokság feladataként az országot és annak infrastrukturális hálózatát ért kibertámadásokra adandó válaszok kidolgozását jelölték meg.[12] Egyelőre nincs információ arra vonatkozóan, hogy bármiféle támadó jellegű tevékenységben is részt venne, de ez nem jelenti azt, hogy a későbbiekben ez nem változhat. A Parancsnokság tagjai között találjuk a hadsereg, az ipar, a telekommunikáció, a tudományok és a titkosszolgálat képviselőit.

2016 augusztusában jelentette be Gholam Reza Jalali dandártábornok, a szervezet parancsnoka, hogy két hónapon belül létrehozzák a kockázatelemző vezető- és irányítórendszert, mivel az elmúlt években számos támadás érte az Iráni Iszlám Köztársaságot elsősorban a kibertérből. Megemlítette, hogy a közelmúltban számos gyakorlatot tartottak biológiai, vegyi és atomtámadásra történő felkészülés jegyében, így most elérkezettnek látják az időt arra, hogy az új szervezet vezetése alatt kidolgozzák a kibervédelmi gyakorlatok rendszerét is.[13] Kifejtette továbbá, hogy az elmúlt évek eseményeinek tükrében kiemelt hangsúlyt kívánnak fektetni a kibertámadások elhárítására.

Az iráni kiberhadsereg

A kiberhadsereg nagyon jól képzett informatikai szakemberekből, hekkerekből, biztonsági szakértőkből áll, akiknek személye titkos. A szervezet hivatalosan nem létezik, ennélfogva alkalmazottai sincsenek. Ugyanakkor nem alaptalan a feltételezés, hogy közvetlenül az Iszlám Forradalmi Gárda gyakorolja felette az irányítást. A kiberhadsereg technikai lehetőségei jelentősek, több nyugati médiaforrást és kormányzati oldalt manipuláltak, illetve a Twittert is. Érdekességként egy adalék a lehetőségeikről: Eric Schmidt, a Google egyik vezérigazgatója egy 2011. decemberi CNN-interjújában elmondta, hogy legnagyobb megdöbbenésükre azt tapasztalták, hogy Irán Dánia teljes internetforgalmát elterelte Iránba, ahonnan visszaterelte Dániába.[14] Majd azt mondta: *„az irániak rendkívüli módon tehetségesek a kiberhadviselés területén."*[15]

A teljesség igénye nélkül álljon itt néhány példa az iráni kiberhadsereg tevékenységéről:

– 2012-ben az iráni hekkercsoportok DNS-támadást hajtottak végre, amelyek eredményeként megbénultak az Amerikai Egyesült Államok és az Egyesült Királyság több bankjának online szolgáltatásai.

---

[12] János Besenyő et al.: Hospital Attacks Since 9/11: An Analysis of Terrorism Targeting Healthcare Facilities and Workers. Studies in Conflict & Terrorism, 24. 06. 2021. https://www.tandfonline.com/doi/abs/10.1080/1057610X.2021.1937821?tab=permissions&scroll=top (Letöltés időpontja: 2023. 01. 06.)

[13] Alexandra Van Dine: After Stuxnet: Acknowledging the Cyber Threat to Nuclear Facilities. In: Mark Cancian (ed.): Project on Nuclear Issues: A Collection of Papers from the 2016 Nuclear Scholars Initiative and PONI Conference Series. Center for Strategic and International Studies (CSIS), 2017, 101–114. https://www.jstor.org/stable/pdf/resrep23162.11.pdf?refreqid=excelsior%3A70f66de01e2b1ca77ebf2d7c6be0938b&ab_segments=&origin=&initiator= (Letöltés időpontja: 2023. 03. 01.)

[14] A dán Jyllands-Posten újság 2005. szeptember 12-én tizenkét karikatúrát közölt Mohamed prófétáról, amelyeket az irániak sértésnek tekintettek. Ez lehet az oka annak, hogy az iráni kiberhadsereg kísérletezett a dán internetes forgalommal.

[15] Thomas M. Chen: Cyberterrorism after Stuxnet. Strategic Studies Institute, US Army War College, 2014. https://www.jstor.org/stable/pdf/resrep11324.pdf?refreqid=excelsior%3A358055d3bfd980941b0cc0031851fd19&ab_segments=&origin=&initiator=&acceptTC=1 (Letöltés időpontja: 2023. 03. 12.)

– Az iráni kiberhadsereg évek óta végez célzott kibertámadásokat az Amerikai Egyesült Államok, Izrael és más országok ellen, ezek közé tartozik például célpontok megfertőzése beépített kártevőkkel, valamint a *phishing* és a *spear phishing* módszerek alkalmazása.
– Az iráni kiberhadsereg felelős állítólag az Amerikai Egyesült Államok és más országok kormányzati oldalainak meghekkeléséért is, köztük például az amerikai Nemzetbiztonsági Ügynökség (NSA[16]) szervereinek feltöréséért.
– Az iráni hekkercsoportok többször célba vettek izraeli vállalatokat, például a Harel biztosító- és pénzügyi szolgáltatót, melynek információit és pénzügyi adatait ellopták.[17]
– Feltételezhetően az iráni kiberhadsereg áll a 2012-es Aramco-támadás mögött, amely a világ egyik legnagyobb olajipari vállalatát érte és súlyos anyagi károkat okozott.
– Állítólag az iráni hekkercsoportok voltak felelősek a 2020-as amerikai elnökválasztási kampányban történt támadások egy részéért is, amelyek célja a választási folyamat destabilizálása volt.
– Sikerült bejutniuk a holland DigiNotar vállalat mind a nyolc szerverére, és legalább 300 ezer hamis digitális tanúsítványt hoztak létre, melyekkel feltörték iráni állampolgárok Yahoo- és Gmail-levelezését, valamint be tudtak lépni Facebook- és AOL-fiókjaikba is. A szerver üzemeltetői a betörést csak nagyjából egy hónap elteltével észlelték.
– Az iráni hekkerek nem titkolták hovatartozásukat, amikor behatoltak az amerikai Comodo biztonsági céghez, amely szintén digitális tanúsítványokat állít ki, és hátrahagyták az alábbi perzsa nyelvű üzenetet: „Janam Faday-e rahbar", ami nagyjából annyit jelent, hogy „feláldozom életem a vezéremért". A behatolás és hamis tanúsítványok generálása lehetővé tette számukra, hogy nem csak olyan tanúsítványt tudtak generálni, amely az internetes titkos kommunikációhoz szükséges, hanem olyat is, amelyekkel kártékony szoftvereket megbízhatóként tudtak terjeszteni.
– A Forradalmi Gárda sohasem ismerte el hivatalosan a kiberhadsereget, de azért elejtettek utalásokat arra vonatkozóan, hogy rendelkeznek ezzel a képességgel. Például 2011 áprilisában Mojtaba Zolnoor, a Gárda parancsnokának szóvivője azt mondta, hogy sikerült a saját erőikkel bejutniuk ellenséges webhelyekre.

Baszidzs paramilitáris szervezet

A Baszidzs (Sāzmān-e Basij-e Mostaz'afin) egy önkéntes alapon létrejött mozgalom, amelyet Homeini ajatollah még 1979-ben, az iráni iszlám forradalom idején szervezett meg. Jellemzően fiatal civil önkéntesekből állt, akik részt vettek az Irak elleni háborúban. A háború végeztével azonban a szervezet nem oszlott fel, hanem bekapcsolódott a hétköznapi életbe, így részt vesz a rendfenntartó egységek, a hadsereg és a vallási élet tisztaságát felügyelő szervezetek munkájában. Helyi szinten jöttek létre alapszervezetek, amelyek a helyi vallási vezetők irányítása alatt állnak, de ugyanakkor alá- és fölérendeltségi rendszerben egységekbe is szervezték őket.

A mozgalom parancsnoka közvetlenül a Forradalmi Gárda parancsnokának és természetesen Irán elnökének is alá van rendelve. A mozgalomnak 2007-ig volt egy fegyveres szárnya

[16] National Security Agency.
[17] Siman-Tov–Even: i. m. 1–4.

is, de ezt áthelyezték a Forradalmi Gárda alárendeltségébe. A fegyver nélküli állományból kerül ki az informatikai hadviselő részleg. Ez nem egy magasan képzett állomány, hiszen a mozgalom tagjainak túlnyomó része alacsonyabb műveltségű, egyszerű fiatalokból áll. A feladatuk az, hogy minden lehető fórumon támogassák a kormányt és az iszlám vallást. Ezért a mozgalom ellátja őket számítógépekkel, internet-hozzáféréssel, részükre blogok tízezreit hozták létre, amelyeken rendszeresen posztolniuk kell, a kormányt támogató hozzászólásokat kell írniuk iráni és nemzetközi weboldalakon. Természetesen rendszeresen posztolniuk kell a jól ismert Facebook-, Twitter-, Youtube- és más oldalakon is. Az ilyen viszonylag egyszerű feladatok mellett a Baszidzs vezetése létrehozott egy úgynevezett kibertanácsot azzal a feladattal, hogy fejlessze a mozgalom informatikai hadviselési képességét, és a jelenleg rendelkezésére álló kevés számú hekkert a Forradalmi Gárda szakembereinek irányítása mellett vesse be. A Teheráni Katonai Körzet parancsnokának 2012. évi beszámolója szerint az elmúlt években mintegy 1500 kiberharcost sikerült felkészíteniük.

A rendőrség

Az iráni rendőrség egyre nagyobb szerepet játszik az internetes műveletekben, és a hagyományos kiberbűnözés elleni harcban már évek óta aktív. A 2009-es választásokat követően szerepe megnőtt és új feladatokat is kapott. A választást követően a rendőrség parancsnoka, Ismail Ahmadi-Moghadam bejelentette, hogy létrehozták a kiberrendőrséget, amelynek nevét 2011 januárjában FETA rendőrségre változtatták. A FETA az Információlétrehozó és -Cserélő Rendőrség elnevezés perzsa nyelvű rövidítése. Szerepe egyrészről megegyezik a más országokban is működő kiberbűnüldöző szervek feladataival. Van azonban egy másik feladata is, amely eléggé sajátságos és eléggé hangsúlyos is. Ez pedig az úgynevezett politikai és biztonsági bűnök elleni küzdelem. Egy teheráni rendőri vezető 2011-ben úgy nyilatkozott, hogy munkájukhoz hekkereket is igénybe vesznek majd, mert az a céljuk, hogy bejussanak köztörvényes bűnügyekkel kapcsolatba hozható e-mail-fiókokba, weboldalakra, valamint majd felhasználják képességieket a politikai ellenzék soraiba történő bejutásra is. A szervezet képességei ilyen téren megközelítik majd a kiberhadsereg képességeit, bár annál jóval kisebb nagyságrendben. Fő feladatuknak tekintik, hogy az internetfelhasználókra teljes rálátásuk legyen, tevékenységüket teljes kontroll alatt tarthassák.

A FETA elérte azt, hogy az internetkávézók tulajdonosai minden információt legyenek kötelesek átadni szervezetüknek, és csak olyanok használhassák a szolgáltatást, akik hitelt érdemlően tudják igazolni személyazonosságukat. Az előírások szerint egy gépet egyszerre csak egy személy használhat, zártláncú televíziót kell üzemeltetniük a kávézóban, amelynek folyamatosan rögzítenie kell a forgalmat úgy, hogy a felhasználók azonosíthatók legyenek. A rögzített felvételt hat hónapig meg kell őrizniük és kérésre a hatóság részére át kell adniuk. Naplózniuk kell a vendégek internetes tevékenységével kapcsolatos minden adatot.

Weboldal-engedélyező Tanács

A Kulturális Forradalom Legfelsőbb Tanácsa által létrehozott szervezet feladata már a nevéből is következik. A Weboldal-engedélyező Tanács 2009-es létrehozásától folyamatosan figyelemmel kíséri azokat a weboldalakat, amelyek valamilyen szempontból „ártalmasnak", rendszerellenesnek tekinthetők. A Tanács a legfőbb ügyészből, a rendőrség főparancsnokából, az állami rádió és televízió vezetőjéből, valamint a kulturális, a tudományos, a titkosszolgálati és a telekommunikációs miniszterekből áll. Működése során már számos

weboldalt blokkolt. A szervezet hatalmára és a súlyára jellemző, hogy egykori államfőjük, a Forradalmi Gárda egykori főparancsnoka, a nemzet hőse, a köztiszteletnek örvendő Akbar Hásemi Rafszandzsáni is kénytelen volt hivatalos weboldaláról néhány visszaemlékezését törölni. Az inkriminált írások eltávolításáig a felhasználók elől a teljes weboldalt blokkolták.

A fenti szervezetek felállítása és működtetése, valamint a szervezeti elemek összehangolt működése csak egy része Irán kibervédelmi rendszerének. Szakértőik javaslatára az amerikai függés és kiszolgáltatottság minimalizálására Irán szeretné magát a világhálótól függetleníteni, ezért előállt a saját internet ötletével.

Nemzeti internetprojekt[18]

Az iráni vezetés részéről a telekommunikációs és információtechnológiai miniszter nyilatkozata szerint saját internetet kívánnak indítani, amely gyorsabb és biztonságosabb lenne a hagyományos világhálónál. A miniszter úgy nyilatkozott, hogy a két internet párhuzamosan létezne egymás mellett, ugyanakkor néhány név nélkül nyilatkozó illetékes állítása szerint a saját internet beindítása esetén a hagyományosat egyszerűen lekapcsolnák.

A saját internet bevezetését biztonsági okokra hivatkozva látják indokoltnak. Elképzelésük szerint a saját internethez saját keresőmotort is készítenének, és ezzel elérhetetlenné tennék a globális keresőket (Google, Yahoo stb.). A kereső neve „Ya Hagh" lenne, ami nagyjából annyit tesz magyarul, hogy „Oh, Istenem". A telekommunikációs miniszter elképzelése szerint a saját keresőmotor beindításával egy időben az adatközpontok és a hosztszolgáltatások is országhatáron belülre kerülnének. Ehhez a témához kapcsolódik a rendőrség parancsnokának az a kijelentése, miszerint a számítógépes információs rendszerek nem lehetnek az ország határán kívül, illetve *„a Google nem keresőmotor, hanem egy kémeszköz"*.

Szakértők nem értenek egyet abban, hogy Irán elképzelései a saját internettel kapcsolatban megvalósíthatók-e vagy sem.

AZ IRÁNI KIBERHADVISELÉS IRÁNYAI

Az irániak kibertevékenysége alapvetően három fő területet foglal magában:

1. Az informatikai védelmi rendszerük az atomlétesítményeiket és egyéb infrastrukturális hálózataikat ért támadásokat követően fő feladatának tekinti a rendszereik védelmét, azok minél hatékonyabb szeparálását a külvilágtól, és ennek érdekében szigorú rezsimszabályokat léptettek életbe, amelyek az állami és az ipari szektor minden résztvevőjére nézve kötelező érvényűek.
2. A belső ellenzék elleni harc, aminek keretében igyekeznek minden egyes másként gondolkodót, politikai aktivistát vagy egyszerűen csak az iszlám vallással szerintük össze nem egyeztethető tartalmat meglátogató vagy letöltő személyt nyilvántartásba venni, tevékenységüket ellenőrizni, igyekeznek korlátozni az úgynevezett „káros" tartalmakhoz történő hozzáférést.
3. A kiberhírszerzés ugyancsak fontos helyet foglal el kiberhadviselésük rendszerében. Ez alatt nemcsak a klasszikus hírszerzési feladatokat értik, hanem érdekességként elmondható, hogy ezt sok esetben – mint azt később látható – egyfajta bosszúálló

[18] Cyberspace and Cyber Warfare Capabilities of Iran. Securityzap.com, 14. 05. 2015. https://securityzap.com/cyberspace-of-iran/ (Letöltés időpontja: 2023. 03. 12.)

eszköznek is tekintik. Számos olyan támadásra derült fény, amelyekre az információszerző feladat elvégzése után került sor, és jelentős értékű károkozással járt.

Irán kiberhadviselése 2010-től elsősorban az Amerikai Egyesült Államok és térségbeli szövetségesei, illetve gazdasági érdekeltségeik ellen, valamint a szerintük iszlámellenes megnyilvánulásokat megengedő országok ellen irányulnak. Természetesen a térségben Izrael a fő ellenségük. Izraelt és annak haderejét támadják az informatikai hadviselés minden eszközével, és ebbe bevonják az általuk támogatott Hamaszt és a Hezbollahot, valamint a palesztin hekkereket. Az izraeli haderő egy neve elhallgatását kérő őrnagya 2015 augusztusában interjút adott a Times of Israel internetes újságnak, amelyben elmondta, hogy a hadsereg C4I-rendszerei[19] folyamatos támadásnak vannak kitéve, bár ezek eredményességéről biztonsági okokra hivatkozva nem nyilatkozott.[20] Valószínű, hogy az izraeli fél sem hagyja szó nélkül ezeket a támadásokat, és úgy tűnik, hogy esetenként a kibertérből átlép a való világba is, hiszen 2013 októberében lakásától nem messze holtan találták Mojtaba Ahmadit, aki az iráni kiberhadviselés parancsnoka volt. A vizsgálatok szerint egy elhaladó motorkerékpárról adták le azt a két halálos lövést, amely végzett a célszeméllyel. Az iráni kormány Izraelt vádolta a merénylet elkövetésével.[21]

AZ IRÁNI KIBERHADVISELÉS MÓDSZEREI

Mint köztudott, Irán az Amerikai Egyesült Államokkal fennálló feszült viszony miatt hátrányban van, hiszen az egyes technológiákat érintő embargó miatt nehezebben fér hozzá bizonyos információkhoz és eszközökhöz, mint az informatikai hadviselésben élenjáró Oroszország és Kína. A hátrányból erényt kovácsolva az iráni kiberharcosok kénytelenek kreatívan alkalmazni a megtévesztés művészetét. Jellemzően a gondos felderítést követően célirányos elektronikus levelekkel, dokumentumokkal, animációkkal, meghívókkal, bölcsességeket tartalmazó PowerPoint-bemutatókkal, játékokkal vagy weboldalakkal tévesztik meg áldozataikat, vagyis előszeretettel alkalmazzák a *social engineering* – az emberi naivitás kihasználása – módszerét.

Szemléltetésül álljon itt egy példa. A Közel-Keleten nagy felháborodást keltett, amikor 2012-ben kiderült, hogy a biztonsági szakértők által „Mahdi" (Megváltó)-nak elnevezett műveletek, illetve kibertámadások mögött Irán áll. A „Mahdi" projekt lényege az volt, hogy a felhasználók részére jellemzően PowerPoint-bemutatókat küldtek, amelyek elindításuk után letöltöttek a célgépre egy kémprogramot, amely aztán folyamatosan kapcsolatban állt az irányító szerverrel. A kémprogram figyelte a billentyűleütéseket, beállítástól vagy eseménytől függően időközönként képernyőfotót készített, 27 különböző típusú fájlt töltött fel a vezérlőszerverhez, megszerezte a meghajtó fájlszerkezetét, képes volt hangfelvételt készíteni a helyiségben elhangzottakról, illetve a különböző mikrofon- és kamerahasználatot (csetelést) is képes volt rögzíteni.

[19] Command, Control, Communications, Computer, Intelligence: vezetés, irányítás, kommunikáció, számítógép, hírszerzés.

[20] David Shamah: Official: Iran, Hamas Conduct Cyber-attacks against Israel. The Times of Israel, 13. 08. 2015. http://www.timesofisrael.com/official-iran-hamas-conduct-cyber-attacks-against-israel/ (Letöltés időpontja: 2023. 03. 12.)

[21] Wisniewski et al.: i. m.

Hogyan tudták ezt végrehajtani, amikor egy makrót futtató PowerPoint-fájl figyelmeztetést generál? Nos, elterelték a felhasználó figyelmét azzal, hogy például mereven kellett néznie négy pontot a képernyő közepén, vagy egy vicces fejtörőt kellett megoldania, így szinte önkéntelenül „okézta" le a figyelmeztetést, és már minden ment a maga útján. A módszer eléggé hatásos volt, mivel rövid idő alatt a későbbiekben 800 áldozatot azonosítottak az irányítószervereket leleplező biztonsági szakemberek. Túlnyomórészt Iránból, de Izraelből, az Egyesült Arab Emírségekből és Afganisztánból választottak „értékes" célpontokat. További trükkjük volt, hogy a kártevőt olyan „ügyetlenül" készítették, hogy a szakemberek egy-egy elszórt esetből kezdő amatőrökre gondolhattak, és nem sejtették, hogy itt államilag támogatott kémkedés áll a háttérben.[22]

Ez a módszer rendkívüli módon jellemzi az állami szinten folytatott iráni informatikai hadviselést. Ezt a módszert *plausible deniability*nek hívják, ami magyarul nagyjából annyit tesz, hogy a „hiteles tagadás lehetősége". Esetünkben ez azt jelenti, hogy a hekkertámadásokat olyan módon szervezik és hajtják végre, hogy azok inkább tűnjenek egy lelkes amatőr vagy amatőrökből álló csapat művének, mintsem állami támogatással végrehajtott, szervezett akciónak. Ezért készítik a programjaikat viszonylag primitív módon, esetenként nyilvános forráskódokat kissé módosítva, hogy megtévesszék a biztonsági elemzőket.

Irán politikai berendezkedéséből adódóan rendkívül erős a cenzúra szerepe. Az állampolgárok csak erősen szűrt tartalmat érhetnek el az interneten. Ennek kijátszására virtuális magánhálózaton (VPN[23]) keresztül csatlakoznak az internetre, és így a valós IP-címeik elrejtését követően „külföldiekként" érhetik el a kívánt „tiltott" tartalmat. A FETA – amelynek a belső ellenzék figyelemmel kísérése is a feladata – olyan VPN-programokat készít, amelyekbe már eleve be van építve a megfigyelő modul, vagy módosítja a meglevő programok telepítő programját. Ezeket a programokat aztán ügynöki úton eljuttatják az ellenzéki csoportokhoz, valamint külföldi webhelyeken, fájlcserélőkön keresztül terjesztik. Az állampolgár, aki egy kis pornográf tartalmat vagy esetleg kormánykritikát is szeretne látni, az letölti, és örül annak, hogy sikerült kijátszania a cenzúrát, pedig ha tudná… Szerény becsléssel számítva az Iránban használt VPN-programok mintegy háromnegyede ilyen manipulált szoftver.[24]

ÖSSZEFOGLALÁS

Amikor Iránról a kibertér vonatkozásban beszélünk, akkor az a kifejezés általában Irán informatikai hadviselési képességeire utal. Az ország kormánya és katonai szervei aktívan fejlesztik a kibertérben történő támadás és védekezés képességeit, és az iráni kiberharcosok részt vesznek olyan támadásokban is, amelyek külföldi számítógépes rendszerek ellen irányulnak. A téma jelentősége az elmúlt években növekedett, az ország kormányzata pedig egyre inkább használta az informatikai hadviselést politikai és gazdasági érdekei megvalósításában. Az iráni kiberharcosok általában a megtévesztés, a *phishing* és a *social engineering*

[22] Gabi Siboni – Sami Kronenfeld: Iranian Cyber Espionage: A Troubling New Escalation. Institute for National Security Studies Insight No. 561, 16. 06. 2014. https://www.jstor.org/stable/pdf/resrep08433.pdf?refreqid=excelsior%3A0c89a621f20f321f3f882d3384b83467&ab_segments=&origin=&initiator= (Letöltés időpontja: 2023. 01. 25.)

[23] Virtual Private Network.

[24] Jack Caravelli – Sebastian Maier: Deciphering Iran's Cyber Activities. Disarat No. 18, King Faisal Center for Research and Islamic Studies, 12. 2016. https://kfcris.com/pdf/27b74972d7db3c7547badfbf7f9ddbd158c8e256cd743.pdf (Letöltés időpontja: 2023. 01. 25.)

módszereit használják, hogy bejussanak a célrendszerekbe és ellopják vagy megsemmisítsék az ott található érzékeny információkat.

Az iráni kibertérképnek azonban van egy másik oldala is, amely a politikai ellenzék és a civilek számára jelent veszélyt. Az iráni hatóságok ugyanis szigorú cenzúrát alkalmaznak az interneten, ezért az állampolgárok csak korlátozottan férnek hozzá az online információkhoz. Emiatt az iráni ellenzéki csoportok és a civilek gyakran VPN-kapcsolatokat használnak a kormányzati megfigyelés elkerülése érdekében. Erre az iráni hatóságok is léptek, és olyan VPN-szoftvereket hoznak létre, amelyekkel képesek megfigyelni az állampolgárok internetes tevékenységeit.

FELHASZNÁLT IRODALOM

- Anderson, Collin – Sadjadpour, Karim: *Iran: Target and Perpetrator*. In: Anderson, Collin – Sadjadpour, Karim: Irans's Cyber Threat: Espionage, Sabotage and Revenge. Carnegie Endowment for International Peace, 2018, 9–16. https://www.jstor.org/stable/pdf/resrep26913.8.pdf?refreqid=excelsior%3Af32c6251b9ed7a22d0d5c0ac0bd1402c&ab_segments=&origin=&initiator=&acceptTC=1
- Besenyő János – Márton Krisztina – Shaffer, Ryan: *Hospital Attacks Since 9/11: An Analysis of Terrorism Targeting Healthcare Facilities and Workers.* Studies in Conflict & Terrorism, 24. 06. 2021. https://www.tandfonline.com/doi/abs/10.1080/1057610X.2021.1937821?tab=permissions&scroll=top; DOI: 10.1080/1057610X.2021.1937821
- Besenyő János: *Zimbabwe: An Intelligence Community against Each Other and Everyone*. In: Ryan Shaffer (ed.): The Handbook of African Intelligence Cultures. Rowman and Littlefield, 2023, 731–746.
- Caravelli, Jack – Maier, Sebastian: *Deciphering Iran's Cyber Activities.* Disarat No. 18, King Faisal Center for Research and Islamic Studies, 12. 2016. https://kfcris.com/pdf/27b74972d7db3c7547badfbf7f9ddbd158c8e256cd743.pdf
- Chen, Thomas M.: *Cyberterrorism after Stuxnet*. Strategic Studies Institute, US Army War College, 2014. https://www.jstor.org/stable/pdf/resrep11324.pdf?refreqid=excelsior%3A358055d3bfd980941b0cc0031851fd19&ab_segments=&origin=&initiator=&acceptTC=1
- Cirlig, Carmen-Cristina: *Cyber Defence in the EU – Preparing for Cyber Warfare?* European Parliamentary Research Service, 10. 2014. http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf
- Cyberspace and Cyber Warfare Capabilities of Iran. Securityzap.com, 14. 05. 2015. https://securityzap.com/cyberspace-of-iran/
- Hubbard, Ben: *MBS: The Rise to Power of Mohammed Bin Salman*. Tim Duggan Books, New York, 2020.
- Kushner, David: *The Real Story of Stuxnet: How Kaspersky Lab Tracked down the Malware that Stymied Iran's Nuclear-fuel Enrichment Program.* IEEE Spectrum, 26. 02. 2013. https://spectrum.ieee.org/the-real-story-of-stuxnet
- Lim, Kevin: *Iran's Cyber Posture.* Open Briefing, 18. 11. 2013. https://www.openbriefing.org/intelligence-desks/middle-east-and-north-africa/irans-cyber-posture/
- Operation Cleaver. Cylance Report. https://scadahacker.com/library/Documents/Cyber_Events/Cylance%20-%20Operation%20Cleaver%20Report.pdf
- Shamah, David: *Official: Iran, Hamas Conduct Cyber-attacks against Israel.* The Times of Israel, 13. 08. 2015. http://www.timesofisrael.com/official-iran-hamas-conduct-cyber-attacks-against-israel/
- Siboni, Gabi – Kronenfeld, Sami: *Iranian Cyber Espionage: A Troubling New Escalation.* Institute for National Security Studies Insight No. 561, 16. 06. 2014. https://www.jstor.org/stable/pdf/resrep08433.pdf?refreqid=excelsior%3A0c89a621f20f321f3f882d3384b83467&ab_segments=&origin=&initiator=

- Siman-Tov, David – Even, Shmuel: *A New Level in the Cyber War between Israel and Iran.* Institute for National Security Studies Insight No. 1328., 03. 06. 2020. https://www.jstor.org/stable/pdf/resrep25542.pdf?refreqid=excelsior%3A023709b6886c27c75429d01008d785c8&ab_segments=&origin=&initiator=&acceptTC=1
- Umbach, Frank: *Critical Energy Infrastructure at Risk of Cyber Attack.* Konrad Adenauer Stiftung International Reports No. 9/2012., 35–66. https://www.jstor.org/stable/pdf/resrep09954.pdf?refreqid=excelsior%3A44e55c3522be8780d7dfce13e6864a6a&ab_segments=&origin=&initiator=&acceptTC=1
- Van Dine, Alexandra: *After Stuxnet: Acknowledging the Cyber Threat to Nuclear Facilities.* In: Mark Cancian (ed.): Project on Nuclear Issues: A Collection of Papers from the 2016 Nuclear Scholars Initiative and PONI Conference Series. Center for Strategic and International Studies (CSIS), 2017, 101–114. https://www.jstor.org/stable/pdf/resrep23162.11.pdf?refreqid=excelsior%3A70f66de01e2b1ca77ebf2d7c6be0938b&ab_segments=&origin=&initiator=
- Wisniewski, Rafał – Wallas, Tadeusz – Stelmach, Andrzej: *Beyond Europe – Reconnecting Eurasia.* Logos Verlag Berlin, 2019.