HADMÉRNÖK

XII. Évfolyam „KÖFOP" szám – 2017. október

MÉRFÖLDKÖVEK A BRIT KIBERBIZTONSÁG FEJLŐDÉSÉBEN I. AZ ELMÉLETI HÁTTÉR MEGALAPOZÁSA: A KIBERBIZTONSÁGI STRATÉGIA

MILESTONES IN THE DEVELOPMENT OF THE BRITTISH CYBER SECURITY I. ESTABLISHING THE THEORETICAL BACKGROUND: THE CYBER SECURITY STRATEGY

MOLNÁR Dóra

(ORCID: 0000-0002-1476-5253)

molnar.dora@uni-nke.hu

Absztrakt

A tanulmány az Egyesült Királyság kiberbiztonsági stratégiai dokumentum rendszerének fejlődését tekinti át. A kiberbiztonság területén az ország a vezető hatalmak közé sorolható, és az előkelő helyezésének egyik oka éppen a jogi szabályozás egyedi és kifinomult mivoltában keresendő.

Az Egyesült Királyság 2011-ben elfogadott első kiberbiztonsági stratégiáját 2016-ban váltotta le az új, második generációsnak tekinthető stratégiai dokumentum, amely immáron az egész társadalomra és valamennyi biztonsági szektorra vonatkozóan tartalmaz megállapításokat és ambiciózus célkitűzéseket. A stratégia a „3D stratégiája", ugyanis a megvédeni (defend) – elrettenteni (deter) – fejleszteni (develop) hármas eszközrendszer segítségével kívánja 2021-re elérni a vízióként kitűzött állapotot: az ország biztonságos, a kiberfenyegetésekre rugalmasan reagálni képes, prosperáló és magabiztos legyen a digitális világban.

A tanulmány a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett Egyed István Posztdoktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: *kiberbiztonság, Egyesült Királyság, kiberstratégia*

Abstract

The study summarizes the development of the cyber security strategic documents in the United Kingdom. Concerning cyber security, the country is among the leading nations, the reason of which is mainly based on the unique and sophisticated features of legal and regulatory frameworks.

In the United Kingdom, the country's first cyber security strategy adopted in 2011 was replaced in 2016 by the new, second generation strategic document, which contains statements and ambitious targets concerning the whole society and all the security sectors. This strategy is a so-called '3D strategy" as it aims at reaching its declared vison of being secure and resilient to cyber threats, prosperous and confident in the digital world by 2021 building on the principles of defend – deter – develop.

„The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in (the) István Egyed Postdoctoral Program."

Keywords: *cyber security, United Kingdom, cyber strategy*

A kézirat benyújtásának dátuma (Date of the submission): 2017.09.18.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.10.31.

BEVEZETÉS

Az internetbirodalom gyors növekedése és ezzel párhuzamosan a kibertér ki- és átalakulása nem csak a mindennapi életben vezetett drasztikus változásokhoz, hanem a világgazdaságban is jelentős változásokat indukált. 2016-ra az internethasználók száma elérte a 3 milliárd főt – amely közel a világ népességének a fele –, és a G-20 országok körében az internetgazdaság volumene meghaladta a 4,2 milliárd dollárt. [1] Ha az internetgazdaságra mint valamely nemzetállam gazdaságára tekintenénk, akkor az az Egyesült Államok, Kína, Japán és India után a világ ötödik legerősebb gazdasága volna.

Ebben az internet-uralta világban az Egyesült Királyság a világ egyik legnagyobb internet-alapú gazdaságával rendelkezik. Az internet-gazdaság volumene 2010-ben elérte a 120 milliárd fontot (amely további 36 milliárd font beruházást és 26 milliárd fontnyi kormányzati kiadást ösztönzött, ezzel összesen 187 milliárd fontot magánénak tudva), amely egyben azt is jelenti, hogy a brit GDP 8,3%-át tette ki. 2016-ra az internet-gazdaság még tovább növekedett, és összértéke elérte a 347 milliárd fontot – ezzel a brit GDP 12,4%-ából részesedve.[1] [1] Ezek az adatok egyértelműen igazolják azt, hogy az Egyesült Királyság mekkora hangsúlyt fektet a világháló fontosságára, amelyből egyúttal az is következik, hogy a kibertér védelme számára létérdek. Ennek köszönhető az, hogy az alább bemutatott brit kiberbiztonságra vonatkozó hivatalos stratégiák és dokumentumok tartalmukat és megközelítésmódjukat tekintve világviszonylatban is kiemelkednek és jövőbemutató gondolatokat fogalmaznak meg.

Jelen tanulmány – mint a kétrészes publikáció első része – a brit kiberbiztonság elméleti hátterét tárja fel; a 2017-ben az Egyesült Királyság kiberhelyzetének jellemzését és a gyakorlati eredmények bemutatását a brit kiberhelyzetet bemutató publikáció következő része fogja tartalmazni.

A BRIT KIBERSTRATÉGIA FEJLŐDÉSE

A Kormányzati Kommunikációs Központ (Government Communications Headquarters, a továbbiakban: GCHQ) kommunikációs és elektronikai biztonsági csoportja[2] 2001-ben ismerte fel először a kormányzati adatok adatvédelmének fontosságát. Ekkor egy felelős kormányzati szakember kinevezését javasolták, akinek feladata egy egységes megközelítés kidolgozása lett a kormányzati adatok kezelése és biztonságuk garantálása érdekében.

2004-ben a brit kormány kiadta első információbiztonsági stratégiáját és kiépített egy külön hálózatot azok számára, akik különösen kitettek informatikai kockázatoknak. Ezt követően azonban két olyan esemény is történt, amelyek újabb lépések megtételére késztették a brit kormányt. Az első incidenst hivatalosan 2007. november 20-án jelentették be, amikor nyilvánosságra hozták, hogy mintegy egy hónappal korábban az Adó- és Vámhivataltól 25 millió brit állampolgár (akik nagy része gyermek) érzékeny adatai kerültek illetéktelen kezekbe. [2] Egy évvel később, 2008 januárjában a Védelmi Minisztérium nyilvánosságra hozta egy olyan alkalmazott laptopjának ellopását, amelyen 600.000 katona adatait tárolták, majd ezt követően fény derült arra is, hogy a minisztériumból az elmúlt évek során „eltűnt” mintegy 700 laptop és 120 pendrive, amelyeken érzékeny adatokat tároltak. [3] Ezek az incidensek súlyosan ártottak a kormányzat reputációjának és egyúttal rávilágítottak arra is,

[1] Összehasonlításképpen a G-20 országoknál az internet-gazdaság 2010-ben átlagosan a GDP 4,1%-át tette ki, 2016-ban pedig az 5,3%-át.
[2] Communications-Electronics Security Group (CESG)

hogy az információs kockázatok kezelését a kiemelt kormányzati feladatok között kell kezelni.

Az Egyesült Királyság *2009*-re ismerte fel a kiberfenyegetések egyre jelentősebb és növekvő veszélyét és alkotta meg *első kiberbiztonsági stratégiáját*. A stratégia célként tűzte ki, hogy túllépve a kormányzati információs rendszerek védelmén a brit gazdaságot és társadalmat sikerüljön megvédenie a kiberfenyegetésekkel szemben. Ehhez szoros együttműködést képzelt el nem csak a nagyvállalatokkal, hanem az állampolgárokkal is. Míg 2009-ben a kormányzat súlyosabb fenyegetésként értékelte a klímaváltozást, a terrorizmust, a bukott államisággal összefüggő kockázatokat és a banki szektort sújtó pénzügyi válságot, mint a kibertámadások jelentette veszélyt, addig a 2010-ben kiadott új Nemzeti Biztonsági Stratégiában már a négy kiemelt kockázat egyikeként[3] definiálta azt. [4] Ennek szellemében 2010 novemberében a brit kormány bejelentette, hogy elindít egy négyéves programot, amely megvalósítására 650 millió fontot különít el. [5] Ez a program lett a Nemzeti Kiberbiztonsági Program (National Cyber Security Programme), amely 2015-ig történő megvalósításának keretét a 2011 novemberében kiadott új kiberbiztonsági stratégia jelentette. A deklaráltan öt évre készített stratégiát 2016 novemberében váltotta fel az új kiberbiztonsági stratégia, amely szintén ötéves időintervallumra vonatkozóan tárgyalja az ország kiberbiztonsági helyzetét érintő legfontosabb kérdéseket.

A tanulmány következő részében előbb értékeli az első ötéves ciklusban elért eredményeket, majd részletesen bemutatja a jelenleg hatályban lévő stratégia irányvonalait, célkitűzéseit és a megvalósításhoz szükséges feltételrendszert.

KIBERBIZTONSÁG 2011 ÉS 2015 KÖZÖTT – A 2011-ES KIBERBIZTONSÁGI STRATÉGIA

A 2011-ben kiadott brit kiberbiztonsági stratégia címe: *Megvédeni és segíteni az Egyesült Királyságot egy digitális világban* (Protecting and Promoting the UK in a digital world). [6] A stratégia rögzíti azt az elméleti keret- és feltételrendszert, amelyben az Egyesült Királyság képes lesz 2015-re megvalósítani mindazt, amelyet a stratégia előbb általános jelleggel vízióként rögzít, majd amelyet négy célkitűzés keretében konkretizál.

A stratégia *vízióként* rögzíti, hogy 2015-re az ország egy vibráló, rugalmas és biztonságos kibertérből gazdasági és szociális értéket kovácsoljon, s ebben a kibertérben a brit lépések – amelyeket az olyan alapvető értékek vezérelnek, mint a szabadság, a tisztesség, az átláthatóság és a joguralom elve – hozzájáruljanak a prosperitás és a nemzetbiztonság szintjének növeléséhez és egy erős társadalom kiépüléséhez. Ennek elérése érdekében *négy célkitűzést* rögzít a dokumentum:

1. az Egyesült Királyság képes legyen kezelni a kiberbűnözést és a világ egyik legbiztonságosabb helyévé váljon, ahol a kibertérben is biztonságosan lehet kereskedni;
2. az Egyesült Királyság még rugalmasabban tudjon reagálni a kibertámadásokra és érdekeit jobban meg tudja védeni a kibertérben;
3. az Egyesült Királyság a jövőben is segítse egy nyitott, stabil és vibráló kibertér kialakítását, amelyet az ország is biztonságosan tud használni és amely segíti a nyitott társadalmak kialakulását;

[3] A kormányzat a további három kiemelt kockázatként a nemzetközi katonai válságokat, a terrorizmust és a súlyos szerencsétlenségeket (mint például a természeti katasztrófák vagy az influenzajárvány) definiálta.

4. az Egyesült Királyság rendelkezzen megfelelő kiber szaktudással, gyakorlattal és képességekkel, amelyek a kiberbiztonsági célkitűzések megvalósításához szükségesek.

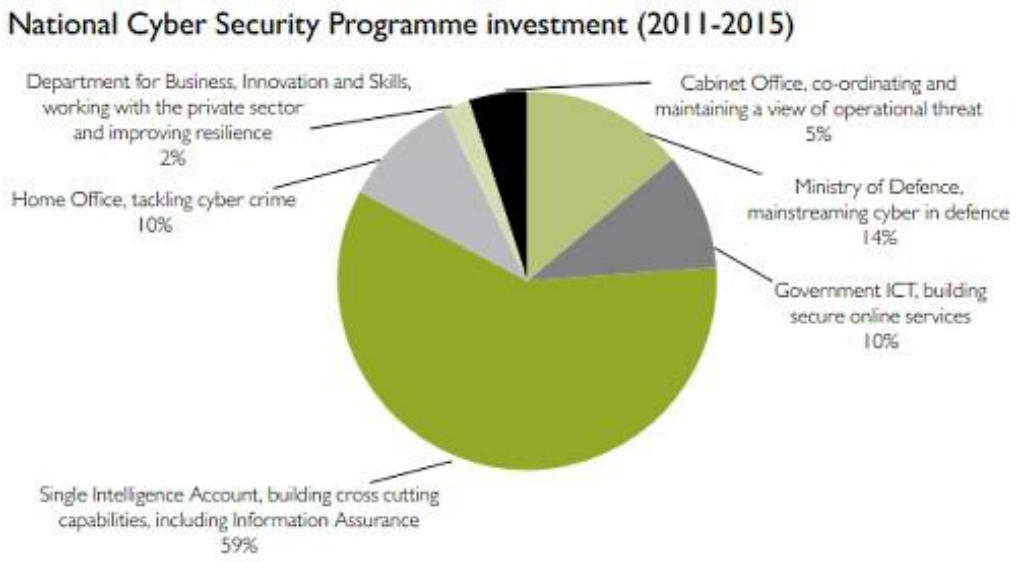
A célkitűzésekre tekintve megállapítható, hogy a stratégia világszinten is egyedülálló a tekintetben, amekkora súllyal a brit kormány becsatornázza a brit vállalatok kereskedelmi érdekeinek támogatását az egyre növekvő nemzetközi kiberbiztonsági piacon. 10 vezető hatalomra kiterjedő nemzetközi összehasonlítást végezve 2012-ben jelent meg a Kiberhatalmi Index (Cyber Power Index).[4] Ez – többek között – értékelte azt is, hogy a fenti négy célkitűzés közül melyik célkitűzés hány állam stratégiájában jelenik meg. Ennek eredményeként az első cél négy másik országnál van nevesítve, míg a második és a negyedik célkitűzés valamennyi ország stratégiájában megjeleni. Ezzel szemben a harmadik cél mindössze egy állam, az Egyesült Államok stratégiai dokumentumában szerepel. [7] Az index mutatói alapján egyértelműen kirajzolódott az, hogy az Egyesült Királyság (már 2012-ben) a világ vezető kiberhatalma, megszerezve 76,8 pontot az elérhető 100 pontból.[5]

A célok megvalósulása esetén a kiberbiztonság érzékelhetően növekedni fog a magánszemélyek, a vállalatok és a kormányzat esetében is. Az egyes állampolgárok pontosan tudni fogják, hogyan védjék meg magukat az internetes bűnözéssel szemben. A vállalatok ismerni fogják azokat az online térből érkező fenyegetéseket, amelyekkel szembe kell nézniük, ismerni fogják rendszereik sérülékeny pontjait és szorosan együtt fognak működni a kormányzattal, a kereskedelmi szövetségekkel és üzleti partnereikkel a kockázatok csökkentése érdekében. A kormányzat pedig a kibertérben való biztonságos működésre fogja bátorítani a vállalkozásokat, a kritikus infrastruktúra kibertámadásokkal szembeni védelmét erősíteni fogja, saját képességeit megerősíti, hogy képes legyen felismerni és leküzdeni a kibertérben őt ért támadásokat és igyekszik olyan kiberbiztonsági szolgáltatásokat nyújtani, amelyekre a világ minden táján szükség lehet. Mindezek alapvető feltétele az oktatási háttér és szakképzés megteremtése, és nem nélkülözhető a más országokkal és szervezetekkel való együttműködés sem.

A célok eléréséhez jelentős anyagi erőforrást is rendelkezésre bocsátottak azzal, hogy a 2011-2015 közötti időszakban a Nemzeti kiberbiztonsági program keretében 650 millió fontot terveztek befektetni az egyes kormányzati szektorok kiberbiztonságának fejlesztésébe. Az 1. sz. ábra mutatja, hogy mely szektorok mekkora mértékű támogatásban részesültek. A titkosszolgálatok és a Védelmi Minisztérium kiemelkedően magas, összesen 73%-os részesedésének indoka az, hogy ezen szervezetek kiemelkedően fontos szerepet játszanak abban, hogy az országra leselkedő, alapvetően más országokból érkező kiberfenyegetéseket felderítsék és az állam sérülékenységét e téren csökkenteni tudják.

[4] A kiberhatalmi index négy kategóriában osztályozta a legfejlettebb államokat (G-20): a jogi és szabályozási keretek (az Egyesült Királyság 97,3 ponttal holtversenyben a második), a gazdasági és szociális kontextus (az Egyesült Királyság 56 ponttal az ötödik), a technológiai infrastruktúra (az Egyesült Királyság torony magasan vezetve 89,1 ponttal az első) és az digitális infrastruktúra kiépítettsége (az Egyesült Királyság 61,4 ponttal az ötödik).

[5] A második helyen az Egyesült Államok végzett 75,4 ponttal, a harmadik Ausztrália 71 ponttal, a negyedik Németország 68,2 ponttal, az ötödik pedig Kanada 66,6 ponttal.



1. ábra A Nemzeti kiberbiztonsági program keretében a 2011. és 2015. közötti időszakra allokált 650 millió font szektoronkénti megoszlása. [6]

A fenti összeget évente növekvő mértékben tervezték az egyes szektorok rendelkezésére bocsátani annak megfelelően, ahogyan egyre növekvő intenzitással épül ki a brit kiberbiztonsági infrastruktúra. Míg 2011-12-ben 105 millió font befektetését irányozták elő, az ezt követő években 115 millió, 180 millió, végül 210 millió font állt rendelkezésre. [8]

Lévén, hogy a 2011-es stratégiát 2016-ban felváltotta egy új stratégia, ezért a dokumentumban foglalt további kérdésekkel jelen tanulmány részletesebben nem foglalkozik. Fontosnak tartom ugyanakkor *az első ötéves periódus értékelését*. A stratégiában foglaltak előrehaladásáról évente értékelést kellett készíteni, és ennek megfelelően 2016-ban is elkészült az éves értékelés, amely egyben az ötéves ciklus átfogó értékelésének is jelenti. [9] A négy fő célterületet érintően elért eredmények a következőkben foglalhatók össze:

1. *Az online kereskedelem biztonságos feltételeinek megteremtését magában foglaló első célkitűzés körében:*

A kiberbiztonsági szektor maga is igen jelentős növekedést tudhat magáénak az ötéves periódus alatt: 10 milliárd fontról 17 milliárd fontra nőtt és jelenleg már mintegy 100.000 embert foglalkoztat. Igen jelentős annak a partnerségi hálónak a létrehozása, amely 10 regionális csoportot, több mint 1750 szervezetet és 5000 magánszemélyt fog össze. A szerveződést 2013 márciusában hozták létre *CISP* (Kiberbiztonsági Információ-megosztási Partnerség – Cyber Security Information Sharing Partnerhip), és célja a valósidejű információ-megosztás a piac és a kormányzat érintett szereplői között. [10]

Mindenképpen említést kell tenni a Cyber Essentials kormányzati programról, amely olyan alapvető biztonsági intézkedések megtételét követeli meg a vállalatoktól, amelyekkel könnyen és eredményesen tudják felvenni a harcot az internetes bűnözéssel szemben. A követelményeket teljesítő vállalatok (alap vagy emelt szintet tanúsító) oklevelet kapnak, és felkerülnek a „képesítéssel" rendelkezők listájára. Ez egyúttal előfeltétele annak, hogy egy vállalattal a kormányzat a jövőben megbízást köthessen. [11]

2. *A kibertámadásokra rugalmasan reagáló Egyesült Királyság és a kibertérben való hatékonyabb érdekvédelemmel kapcsolatos célkitűzés körében:*

E körben fontos fejleményt volt a *CERT-UK*, azaz a brit hálózatbiztonsági reagáló csoport (computer emergency response team) felállítása 2014-ben, amely a hálózatbiztonsági kérdésekben érintett szervezetek központi fórumaként szolgál és havonta három gyakorlat segítségével teszteli a kiber reagáló képességet. [12] Emellett a kibertartalékos program

(*Cyber Resesrve*), amelyet 2013-ban indítottak el, egyedülálló a világban, és hatékony kezdeményezésnek bizonyult a Kibervédelmi Partnerség (Defence Cyber Protection Partnership) és az Összhaderőnemi Kibercsoport (Joint Forces Cyber Group) is.[6]

3. A nyitott társadalmakat támogató nyitott, vibráló és stabil kibertér megteremtésére irányuló célkitűzés körében:

A „Londoni Folyamat" (London Process) keretében megrendezett konferenciák mellett az Egyesült Királyság évente *30 nemzetközi projektben* vesz részt, melyek célja, hogy a kiberbiztonsági ismereteket és tudást széles körben terjesszék.

4. A megfelelő és szükséges kiber tudással, gyakorlattal és képességgel rendelkező Egyesült Királyság létrehozására irányuló célkitűzés körében:

A kiberismeretek oktatását már az alsó fokú oktatásban megkezdték: 800 általános iskola bevonásával mintegy 23.000 diák szerzett alapvető ismereteket 2012 óta. A felsőoktatásban valamennyi alapképzés esetében bevezettek egy kiberbiztonsági közös modul tárgyat, a mesterképzésen pedig a GCHQ által kiadott standardnek megfelelően már 12 akkreditált kiber-mesterképzés létezik. Jelenleg három kutatóintézet rendelkezik kiberbiztonsági profillal, 13 kiválósági központot hoztak létre, és cél, hogy 2019-re 100 doktoranduszt tudjon magáénak a már működő két kiberbiztonsági doktori iskola.

A célkitűzések tehát bár meglehetősen ambiciózusnak mondhatók, mégsem bizonyultak irreálisaknak, hiszen az elért eredmények magukért beszélnek. Felismerve a kiberbiztonság fontosságát, az Egyesült Királyság már az első ötéves ciklus alatt a várakozásokhoz képest felülteljesített. A célok elérésére az előre tervezett 650 millió font helyett végül 860 millió fontot költött, ám mindez csak az előszele annak, amelyet a második ötéves periódus alatt e területen el szeretne érni.

KIBERBIZTONSÁG 2016 ÉS 2021 KÖZÖTT – A 2016-OS KIBERBIZTONSÁGI STRATÉGIA

A brit kormány 2016. november 1-jén adta ki az Egyesült Királyság új Nemzeti kiberbiztonsági stratégiáját, amely ismét deklaráltan öt évre készült. [13] A 2016 és 2021 között időszakra vonatkozó dokumentum – amely kiadását nagy várakozás előzte meg – rögzíti a brit kormány legfontosabb célkitűzéseit, hogy az ország a kibertérben (is) nagyobb biztonságban tudhassa magát 2021-re. A célok megvalósítására minden eddiginél több erőforrást terveznek allokálni: öt év alatt 1,9 milliárd font áll rendelkezésre a kiberbiztonsági reformok és intézkedések megtételére.

A 2015. november 23-án kiadott új Nemzeti biztonsági stratégia már a legmagasabb prioritású[7] kockázatok között említi a kiberfenyegetéseket. [14] Ez azt jelenti, hogy a brit politika öt éven belül reálisan számol kibertámadások bekövetkeztével. Ennek megfelelően a

[6] Ezen kezdeményezésekkel és az elért eredményekkel a tanulmány második része részletesen is foglalkozik.

[7] A birt Nemzeti biztonsági stratégia a kockázatokat 3 típusba sorolja: az ún. tier 1 kockázatokkal az Egyesült Királyságban valószínűleg rövid időn belül (azaz ötéves távlatban) ténylegesen is szemben kell néznie (e körben hat kockázatot nevesít a dokumentum, köztük a kiberfenyegetések körét is); az ún. tier 2 kockázatok közé sorolt hét problémakör esetében azok bekövetkezése rövid, időn belül nem várható; az ún. tier 3. kockázatok (szám szerint szintén hét) bekövetkezésével csak hosszabb távon számol az ország. A kockázatok értékelése egy 2010-ben kifejlesztett módszer alapján történik. Ez a Nemzeti Biztonsági Kockázatok Értékelése (National Security Risk Assessment), amelyet a 2015-ben kiadott Nemzeti biztonsági stratégia is tartalmaz. [15]

dokumentum a négy kiemelt politikai prioritás között is megjeleníti a kiberbiztonság területét azzal összefüggésben, hogy az ország e területen meg szeretné őrizni világvezető szerepét.

Az Egyesült Királyság a világ egyik vezető digitális nemzete, ezért jövőbeni fejlődése nagyban függ attól, hogy a kibertérben jelentkező, a technológiára, az adatokra és a hálózatokra leselkedő fenyegetésekkel szemben mennyire képes magát megvédeni. Felismerve azt, hogy a brit gazdaság, a kormányzat és a kritikus infrastruktúra intézményei a kibertérben alakuló viszonyok változásától milyen nagymértékben függnek, az Egyesült Királyság a stratégiában megfogalmazottak alapján a jövőben is kiemelkedően nagy hangsúlyt fog fektetni e terület további fejlesztésére. Az első öt évben elért eredmények mindehhez jó alapot szolgáltatnak nemcsak a kitűzött és elért célok tekintetében, hanem a befektetett anyagi erőforrásokat is beleértve. Ugyanakkor egy olyan átfogó megközelítésre lesz szükség, amely az egyik oldalról értékeli a kiberfenyegetések dinamikusan változó természetét és azok számbeli növekedését (figyelembe véve az ország függőségi viszonyait és sérülékenységét), a másik oldalról pedig a piaci-alapú helytelen megközelítést felváltva a kormányzat aktív bevonása és e terület irányítójává válása vált szükségessé azzal, hogy a kormányzati szektor nem hagyható magára, feladatait csak az állampolgárok, a vállalatok és egyéb partnerek segítségével fogja tudni eredményesen ellátni.

A stratégia értékeli a *stratégiai környezetet*, amelyben a lefektetett elméleti kérdéseket a gyakorlatba is át kell ültetni. E körben előbb bemutatja az országra potenciálisan fenyegetést jelentők körét, majd a sérülékeny területeket. *Fenyegetést öt féle személyi kör jelenthet*: a kiberbűnözők (közülük is kiemelve a Kelet-Európában pénzszerzési céllal tevékenykedő orosz nyelvű szervezett bűnözői csoportokat), egyes államok (akik közül jelenleg bár kevés jelenthet közvetlen veszélyt, azonban kiberkémkedési tevékenységet több állam is folytat és manapság egyre több állam fejleszt támadó kiberkapacitásokat is), a terroristák (akik ugyan nem elsősorban a kibertérben támadnak, és bár szerény kapacitásokkal bírnak e területen, tevékenységük hatása mégis igen nagy lehet), a hacktivista csoportok (akik decentralizált csoportokat jelentenek és általában korábbi sérelmeiket torolják meg ily módon), valamint a kisebb veszélyt jelentő, nem kellően képzett magánszemélyek, akik mások által kifejlesztett programok használatával támadhatnak a kibertérben.[8] A *sérülékeny területek* között első helyen említendő az internethez kapcsolódó eszközök egyre nagyobb száma. A 2011. évi stratégia elfogadása óta eltelt években ugyanis az internet használata sokkal kiterjedtebbé vált, egyre több, a háztartásokban használt eszköz csatlakozik a világhálóhoz, amelynek köszönhetően a „dolgok internete" világában[9] már nem csak ezen eszközökben okozható kár, hanem maguk az eszközök azok, amelyeket károkozásra lehet felhasználni. A második problémás terület a szegényes kiberfelkészültség, amelynek köszönhetően a kibertámadók nem túl bonyolult megoldásokkal is célt tudnak érni mind a lakosok, mind a vállalatok elleni tevékenységük során. Több kormányzati programot is elfogadtak, amelyek a jobb felkészültséget próbálják elősegíteni. E körben a 2012-ben elfogadott „10 lépés a kiberbiztonság felé" elnevezésű program[10] (amely 10 kritikus területet érintően fogalmazza meg ajánlásait. [16]) és a 'Közös kibertámadások: a hatások csökkentése' c. program [17] bizonyultak a legjelentősebb kezdeményezéseknek. Problémás továbbá a kiberképzés területe: a vállalatok kevesebb, mint egyötöde segítette hozzá munkavállalóit kiberismeretek megszerzéséhez [18]; valamint az, hogy számos brit vállalat nem frissíti programjait és a régi verziók igen sérülékenyek tudnak lenni. Végül, de nem utolsó sorban meg kell említeni azt az

[8] Őket nevezik „script kiddies"-nek.

[9] Mára elterjedt az Internet of Things (IoT) kifejezés használata, amely a háztartásokban (is) használt, internetre csatlakoztatott eszközök hálózatát foglalja magába.

[10] 2017. április 4-én a programokban szereplő ajánlásokat visszavonták.

alapvető jellemző tulajdonságot is, hogy minimális feltételek szükségesek ahhoz, hogy valaki egy rendszert meg tudjon hekkelni: a szükséges információk publikusak, így könnyen érthetők, ezért minimális szakismeret birtokában végezhető ez a tevékenység.

A fent vázolt stratégiai kontextusban a stratégiában rögzített *vízió* egy olyan Egyesült Királyságot vázol fel, amely biztonságos, rugalmasan képes reagálni a kiberfenyegetésekre, prosperáló és magabiztos a digitális világban. Hogy ez megvalósulhasson, *három stratégiai célt* fogalmaz meg a stratégia – ezért *nevezhetjük a 2016-os kiberstratégiát a „3D stratégiájának"* is: megvédeni (defend), elrettenteni (deter), fejleszteni (develop). Ezek megvalósuláshoz pedig elengedhetetlen a nemzetközi fellépés (lásd a 2. sz. ábrát).

2. ábra A 2016-os kiberstratégia stratégiai célkitűzései [19]

A stratégiai célok megvalósításában széles alanyi kör vesz részt: az egyének, a vállalatok, a szervezetek és fő felelősként a brit kormányzat. A piac és a kormányzat együttműködésének e téren bár voltak látható eredményei már az elmúlt öt évben is, azonban még mindig túl sok hálózat nem biztonságos, a piac még mindig nem megfelelően értékeli a kiberfenyegetések jelentőségét és túl sok vállalatot ér „primitív" kibertámadás, amelyek kivédhetők volnának. Ezért a jövőben a kormányzatra sokkal nagyobb szerep kell, hogy háruljon, ugyanis egyrészt kizárólag a kormányzat számára érhetők el bizonyos, a kibervédelemhez nélkülözhetetlen eszközök (mint például a titkosszolgálatok bevonása), másrészt pedig csak a kormányzat képes a köz- és magánszféra között kooperációt és információ-megosztást biztosítani.

A stratégiai célokhoz visszatérve, az első a *védelem (defend)*. E célkitűzés lényege, hogy a brit köz-, magán- és kereskedelmi hálózatok, adatok és rendszerek kibertámadásokkal szembeni védelme biztosított legyen. Ennek egyik eszköze az „Aktív kibervédelem" program[11], amely célja, hogy az Egyesült Királyság más államok szemében kemény célpont legyen, és a brit internet és telekommunikációs forgalom sokkal kevésbé legyen sérülékeny. [20] A védelmet segíti elő továbbá a biztonságos internet megteremtése, melynek egyik eszköze, hogy olyan online termékeket adnak el a felhasználóknak, amelyek gyárilag beépített védelemmel vannak ellátva. Szintén ide sorolható a kormányzat védelme (amelyet az interneten elérhető kormányzati szolgáltatások növekvő száma is indokol), valamint a kritikus infrastruktúra intézményeinek és más kiemelt szektoroknak a védelme. Mindehhez elengedhetetlen az üzleti és a közszféra hozzáállásának megváltozása és az online szolgáltatásokba vetett bizalom kiépülése, valamint az, hogy a következmény megelőző-

[11] Active Cyber Defense (ACD)

elhárító-felszámoló tevékenységeket központosítsák[12] – a holisztikus megközelítést szem előtt tartva.

A stratégiai célkitűzések között második helyen az *elrettentés (deter)* szerepel. A Nemzetbiztonsági stratégia is rögzíti, hogy a védelem az elrettentésnél kezdődik – s ez igaz nem csak a kibertérben, hanem valamennyi hadszíntér esetében. Az ellenségnek ugyanis tudnia kell, hogy büntetlenül nem tehet semmit, mert az Egyesült Királyság azonosítani fogja őt és megteszi vele szemben a szükséges intézkedéseket. Ennek érdekében a britek tovább folytatják a már megkezdett globális kiberszövetség kiépítését és továbbra is támogatják a nemzetközi jog kibertérben történő alkalmazását. Az elrettentés körében a stratégia legfigyelemreméltóbb megállapítása, hogy az ország deklaráltan támadó kiberképességekre kíván szert tenni. A támadó képességeket a teljes spektrumú kapacitások részének tekinti, amely segítségével károkozás céljával képesek szándékosan behatolni az ellenség rendszereibe és hálózataiba. Ennek megvalósítása érdekében útjára indították a Nemzeti támadó kiberprogramot (National Offensive Cyber Programme – NOCP), amely a maga nemében világszinten is egyedülálló. [21] Mindemellett nem szabad figyelmen kívül hagyni a kódfejtési képességfejlesztési célkitűzést sem, amelyet nemzetbiztonsági érdekek indokolnak, és amely célja, hogy az érzékeny és titkos brit információk biztonságát és jogosulatlan felhasználás elleni védelmét garantálni tudják.

A harmadik stratégiai cél a *fejlesztés (develop)*, melynek lényege, hogy az ország hogyan tudja megszerezni és fejleszteni azon eszközöket és képességeket, amelyekre a kibertámadásokkal szembeni védelem céljából szüksége van. Ehhez mindenekelőtt jól képzett kiberbiztonsági szakemberek szükségeltetnek, amely azonban csak hosszú távú, mintegy húsz éves célkitűzés lehet reálisan, tehát jelen stratégia időkeretét jóval meghaladja. Ennek keretében a kiberképzést iskolai programok segítségével, minőségi közép- és felsőoktatással, tanárképzéssel és Védelmi Kiberakadémiák (Defence Cyber Academy) mint kiválósági központok felállításával képzelik el. A kibertudományok és technológia területén is további előrelépés szükséges, amelyet megkönnyíthet az akadémiai szféra és az üzleti szféra között szorosabb együttműködés. Ennek keretét a készülőben lévő kibertudományi és technológia stratégia fogja képezni.

A három stratégia cél megvalósítása csak megfelelő *nemzetközi keretek* között képzelhető el. Az Egyesült Királyság továbbra is élharcosa a szabad, nyitott, békés és biztonságos kibertér megteremtésének, ahol a nemzetközi jog alkalmazandó és az alapvető emberi jogok érvényesülését biztosítani kell online és offline egyaránt. Ebben az Egyesült Királyság számít nem csak a hagyományos szövetségesire, hanem új partnereire is, és igyekszik kihasználni az olyan multilaterális fórumok adta befolyásolási lehetőségeit, mint az Egyesült Nemzetek Szervezete (ENSZ), a G20, az Európai Unió, az Észak-atlanti Együttműködés Szervezete (NATO), az Európai Biztonsági és Együttműködési Szervezet (EBESZ), az Európa Tanács vagy a Brit Nemzetközösség.

A BRIT KIBERBIZTONSÁGI STRATÉGIARENDSZER ÉRTÉKELÉSE

A kiberbiztonságot illetően is több olyan mutató létezi, amelyek segítségével az egyes államok rangsorolását elvégezhetjük. Elsőként az ENSZ szakosított intézménye, a Nemzetközi Távközlési Egyesület (International Telecommunication Union, a továbbiakban: ITU) által jegyzett *Globális kiberbiztonsági index*ről teszek rövid említést. [22] Az index öt

[12] E terület fő felelőse a Nemzeti Kiberbiztonsági Központ (National Cyber Security Center), amely tevékenységét a tanulmány második része mutatja be részletesen.

területet[13] vizsgálva osztályozza az államokat. Az első területet a jogi kérdések alkotják, amellyel kapcsolatban az index a jogalkotási, szabályozási és képzési alterületeket különíti el. Bár az európai államok rangsorában Észtország, Franciaország és Norvégia foglalják el a dobogós helyeket, minimálisan lemaradva követi őket az Egyesült Királyság, amely a jogi területet illetően, hibátlan, 100%-osnak értékelt teljesítményt tudhat magáénak. Összteljesítményét tekintve az Egyesült Királyság 78,3%-os teljesítménnyel világviszonylatban a 12. helyet foglalja el.[14]

Mindezt alátámasztja a fent már említett *Kiberhatalmi Index* is, melynek első mérőszáma a jogi és szabályozási keretek fejlettsége alapján osztályozza a vizsgált államokat. Ezen a területen az Egyesült Királyság – holtversenyben az Egyesült Államokkal – a második helyen végzett az elérhető 100 pontból 97,3 pontot megszerezve. Ez jól jelzi, hogy az ország milyen fejlett stratégia kultúrával rendelkezik, és joggal nevezhető nagy stratégának a kiberbiztonság területén is.

A képet azonban árnyalja a harmadik mutatószám, a *Kiberfelkészültségi Index*. [23] Ez hét szempont[15] alapján rangsorol kilenc[16] vezető hatalmat, ugyanakkor végkövetkeztetésként megállapítja, hogy még egyik állam sem tekinthető teljes körűen felkészültnek kiberbiztonsági viszonyait tekintve. [24] Az Egyesült Királyság jelenleg részben tekinthető működőképesnek mind a hét vizsgált területen – köztük az elsőként nevesített nemzeti kiberstratégia vonatkozásában is.

KÖVETKEZTETÉSEK

Bátran állíthatjuk, hogy *az Egyesült Királyság kibernagyhatalom*. Ez a kijelentés a tanulmányban vizsgált jogi-szabályozási kérdéseket illetően mindenképpen helytálló, s ezt a különböző értékelési rendszerek is alátámasztják.

Az ország a stratégiaalkotás terén mindig is az élen járt. A vezető hatalmak jellemzően a 2010-es évek körül alkották meg első kiberbiztonsági stratégiájukat – ahogyan tette azt az Egyesült Királyság is 2009-ben, majd 2011-ben. Ezek a stratégiák még az ún. első generációs stratégiák sorába illeszkedtek, amikor még az online bizalom megteremtése szerepelt a célkitűzések élén. Az elmúlt évek alatt azonban az infokommunikációs rendszerek rohamos terjedésnek indultak, amely következtében a kihívások természete is megváltozott, és mára a gazdaság és a társadalom nagymértékben (ha nem teljes mértékben) az instabil rendszerektől vált függővé. Ezért a kiberbiztonság olyan nemzeti prioritássá vált, amely már az egész társadalom vonatkozásában értelmezendő. A fejlett államokban ezen folyamatokra válaszul születtek meg az ún. második generációs kiberstratégiák – ahogyan az Egyesült Királyságban is 2016-ban. Ez már olyan holisztikus megközelítést alkalmaz, amely a kiberbiztonság garantálását csak valamennyi szereplő együttes részvételével tartja megvalósíthatónak, beleértve az egyes állampolgárokat, a kormányzat valamennyi ágazatát, valamint a közszféra, a nemzeti infrastruktúra és a gazdaság valamennyi szereplőjét és a nemzetközi partnereket.

A hatályos stratégia hűen tükrözi az ország kiberbiztonság kérdésköréhez való hozzáállását. Célrendszere egyedülállóan ambiciózus, mégsem elrugaszkodott a valóságtól,

[13] Ezek a jogi, a technikai, a szervezeti, a kapacitásépítési és együttműködési területek.

[14] Az európai országok között harmadik Norvégia a világon a 11. helyen áll (78,6%-os teljesítménnyel), az Európában második Franciaország a 8. (81,9%-kal), a vezető európai állam, Észtország pedig az 5. (85,6%-kal).

[15] A hét vizsgált szempont a nemzeti kiberstratégia, az incidenskezelés, az e-bűnüldözés, az információ-megosztás, a beruházások és K+F, a diplomácia és kereskedelem, valamint a védelem és válságkezelés.

[16] Ezek az Egyesült Államok, Japán, Franciaország, Németország, Egyesült Királyság, Olaszország, India, Hollandia, Szaúd-Arábia.

mivel a célok elérése érdekében már megindított brit programok segítségével az ötéves ciklus végére valamennyi célkitűzés megvalósítható. Ezáltal azon szempontok esetében is sikerülhet javítani az értékeléseken, amelyeknél jelenleg az Egyesült Királyság minimális lemaradást tudhat magáénak, és az intézkedések végeredményeképp első lehet az egyenlők között a kiberhatalmak rangsorában. Azonban nem szabad megfeledkezni arról, hogy még egy ilyen, stabil alapokon álló rendszert is érhet olyan kibertámadás, amelyre a felkészülés szinte lehetetlen. Elég, ha a 2017. májusi, a brit egészségügyi rendszert ért kibetámadásra gondolunk, amely során a WannaCry zsarolóvírussal csak az Egyesült Királyságban[17] 300.000 számítógépet fertőztek meg, s ezzel napokra képesek voltak megbénítani az egészségügyi rendszert. [26] Vagy megemlíthető a „Panama papírok" ügye, amellyel összefüggésben még az akkori brit miniszterelnök, David Cameron lemondása is felmerült. [27] Ez jelzi nem csak a biztonsági szektorok szoros összefonódását, hanem azt is, hogy a kibertér feletti uralom megszerzésében és birtoklásában mekkora potenciál rejlik már napjainkban is.

FELHASZNÁLT IRODALOM

[1] *The Internet Economy in the G-20. The $4.2 Trillion Growth Opportunity.* The Boston Consulting Group report. 2012. március https://www.bcg.com/documents/file100409.pdf (letöltés ideje: 2017. október 11.)

[2] *Data lost by Revenue and Customs.* 2007. november 21. http://news.bbc.co.uk/2/hi/7103911.stm (letöltés ideje: 2017. október 11.)

[3] *MoD admit loss of secret files.* 2008. július 18. http://news.bbc.co.uk/2/hi/uk_news/7514281.stm (letöltés ideje: 2017. október 11.).

[4] *A Strong Britain in an Age of Uncertainty: The National Security Strategy.* HM Government, United Kingdom, 2010. október https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf (letöltés ideje: 2017. október 11.)

[5] *Securing Britain in an Age of Uncertainty: Strategic Defense and Security Review.* HM Government, United Kingdom, 2010. október https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33835/desider_30_Nov_2010.pdf (letöltés ideje: 2017. október 11.)

[6] *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world.* 2011. november https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (letöltés ideje: 2017. október 11.)

[7] *The Cyber Power Index 2012.* Booz Allan Hamilton and the Economist Intelligence Unit, 2012. január, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf (letöltés ideje: 2017. október 11.)

[17] A zsarolóvírus jelenlétét több, mint 100 országban regisztrálták. [25]

[8] *The UK cyber security strategy.:Landscape review.* Report by the controller and audit gerenal. HC 890, Session2012-2013., National Audit Office, United kingdom, 2013. február 12. https://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf (letöltés ideje: 2017. október 11.)

[9] *The UK Cyber Security Strategy 2011-2016. Annual Report,* HM Cabinet Office, United Kingdom, 2016. április https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf (letöltés ideje: 2017. október 11.)

[10] *Government launches information sharing partnership on cyber security.* Cabinet Office, United Kingdom, press release, 2013. március 27. https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security (letöltés ideje: 2017. október 11.)

[11] *Cyber Essentials Sheme – Summary.* HM Government, United Kingdom, 2014. július https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf (letöltés ideje: 2017. október 11.) – lásd még: http://www.cyberessentials.org/ (letöltés ideje: 2017. október 11.)

[12] http://www.ukcert.org.uk/ (letöltés ideje: 2017. október 11.)

[13] *National Cyber Security Strategy 2016-2021*. HM Government, United Kingdom, 2016. november 1., https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (letöltés ideje: 2017. október 11.)

[14] *National Security Strategy and Strategic Defense and Security Review 2015. A Secure and Prosperous United Kingdom.* HM Government, United Kingdom, 2015. november 23. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf (letöltés ideje: 2017. október 11.)

[15] *Decision-making on national security.* United Kingdom Parliament, 2016. július 8., https://publications.parliament.uk/pa/jt201617/jtselect/jtnatsec/153/15307.htm (letöltés ideje: 2017. október 11.)

[16] *'10 Steps to Cyber Security.'* HM Goverment, United Kingdom, 2012., https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary (letöltés ideje: 2017. október 11.)

[17] *'Common Cíber Attack: Reducing The Impact.'* HM Goverment, United Kingdom, 2015. https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/common-cyber-attacks-summary (letöltés ideje: 2017. október 11.)

[18] Cyber Security Beaches Survey 2016. HM Government – Ipsos MORI – University of Portsmouth, 2016. május, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf (letöltés ideje: 2017. október 11.)

[19] *The UK Cyber Security Strategy 2016-2021 – A New Sheriff in Town?* http://www.ascentor.co.uk/2017/01/theres-sheriff-town-uk-cyber-security-strategy-2016/ (letöltés ideje: 2017. október 11.)

[20] *Active Cyber Defence – Tackling cyber attacks on the UK.* National Cyber Security Center, 2016. november 1., https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk (letöltés ideje: 2017. október 11.)

[21] BURGESS, Matt: *The government peldges to 'damage, disrupt and destroy' cyberattackers who target the UK.* 2016. november 2. http://www.wired.co.uk/article/uk-offensive-cyber-security-attacks (letöltés ideje: 2017. október 11.)

[22] *Global Cybersecurity Index 2017.* International Telecommunication Union, Geneva, Switzerland, 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (letöltés ideje: 2017. október 11.)

[23] *Cyber Readiness Index Country Profiles.* http://www.potomacinstitute.org/academic-centers/cyber-readiness-index (letöltés ideje: 2017. október 11.)

[24] *United Kingdom Cyber Readiness at a Glance.* Potomac Institute for Policy Studies, 2016. október, http://www.potomacinstitute.org/images/CRI/CRI_UK_Profile_PIPS1.pdf (letöltés ideje: 2017. október 11.)

[25] *Massive ransomware cyber-attack hits nearly 100 countries around the world.* 2017. május 12. https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs (letöltés ideje: 2017. október 11.)

[26] *NHS seeks to recover from global cyber-attack as security concerns resurface.* 2017. május 13. https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack (letöltés ideje: 2017. október 11.)

[27] *Panama Papers: Protesters demand Cameron's resignation.* 2016. április 9. http://www.aljazeera.com/news/2016/04/panama-papers-protesters-demand-cameron-resignation-160409184433734.html (letöltés ideje: 2017. október 11.)