Molnár Dóra

Kiberbiztonság Németországban – pillanatkép a német digitális térről[1]

Németország nemcsak gazdasági mutatói és lakosságszáma alapján Európa vezető állama, hanem a digitális és kiberbiztonság terén is kiemelkedő eredményeket tud felmutatni. Az ország a digitális piacot érintően igen kiterjedt és fejlett szabályozással rendelkezik, és sikeresen integrálódott a nemzetközi folyamatokba is, mindennek köszönhetően pedig egyre sikeresebben tudja felvenni a harcot a kibertérben jelentkező kihívásokkal.

A tanulmány Németország digitális és kiberbiztonsági helyzetét vázolja fel, ismertetve a főbb vonatkozó dokumentumokat és a szervezeti hátteret. Bár impozánsak az elért eredmények, a következő években további fejlesztésekre van szükség valamennyi területen ahhoz, hogy Németország a lehető legteljesebb mértékben képes legyen állami intézményeit és állampolgárait a kibertámadásoktól megvédeni.

Kulcsszavak: *kiberbiztonság, Németország, digitális biztonság*

Molnár Dóra: Cyber Security in Germany – Snapshot on the German Digital Space

Germany is the leading European nation in terms of economic power and population figures, however it has also achieved significant results in the field of digital and cyber security. The country can show up a large-scaled and developed regulation of the digital market and it has already successfully integrated in the international processes, the result of which is that it can more and more successfully struggle against the threats in cyberspace.

The study shows the digital and cyber situation of Germany, reviewing the main relevant documents and the organizational background. The results achieved are imposing; however in the upcoming years more innovations will be needed in all fields, so that Germany could fully defend its national institutions and citizens against cyber attacks.

Keywords: *cyber security, Germany, digital security*

[1] A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosító számú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Bevezetés

Németországban igen korán, már 1983-ban bevezették az internetet.[2] Ekkoriban még a Deutsche Telekom volt az egyetlen szolgáltató, amely a BXT *(Bildschirmtext)* hálózatot használta. Egy évvel később az Egyesült Államokból megérkezett az első e-mail-rendszer is, és ezzel hivatalosan is kiépült a német internethálózat. A Deutsche Telekom egészen 1995-ig őrizte monopol helyzetét Németországban, csak ezt követően nyitották meg a piacot a magánvállalkozások előtt. S bár a privatizáció lezajlott, a német állam és a szövetségi kormányok még mindig magukénak tudhatják[3] a Deutsche Telekom részvényeinek egyharmadát, és jelenleg is ez az „állami vállalat" az ország legnagyobb internetszolgáltatója.

Ma Németország a világ legfejlettebb telekommunikációs rendszerekkel rendelkező országai közé tartozik. Ennek szemléltetésére példa, hogy a világháló bevezetését követően Németország volt az első, amely a „Global Info" projekt keretében, 1998-tól kezdődően teljes mértékben digitalizálta könyvtárait.[4] Hasonlóképp illusztrálja a fejlett német viszonyokat az is, hogy mára az országban az internetpenetráció meghaladja a 86%-ot, és jelenleg a német ICT piac a legnagyobb Európában, a világ országai között pedig a negyedik helyen áll. Egy ilyen kiterjedt gazdaság azonban könnyen támadások célpontjává válhat: 2012-ben a szellemi tulajdont ért lopások a német GDP-nek 1,5%-os veszteséget okoztak, de a támadások a lakosságot sem kímélik: 2013-ban a német internethasználók 40%-a (mintegy 21 millió lakos) esett kiberbűnözés áldozatául.[5] Összességében a kiberbűnözés okozta kiadások 2017-re 11,15 milliárd dollárt tettek ki, ami az előző év 7,84 milliárd dolláros kiadásához képest is igen jelentős, 42,4%-os növekedést jelent.[6]

Mindezek alapján látható, hogy Németországban, amely az Európai Unió legnagyobb lakosságú állama, különösen nagy hangsúlyt kell fektetni az információs hálózatok védelmére mind a közszférában és a kritikus infrastruktúra intézményeinél, mind pedig az állampolgárok megvédése érdekében. Az alábbiakban a tanulmány ennek a célkitűzésnek a megvalósításáért tett lépéseket ismerteti.

A hivatalos német dokumentumok rendszere

Németország a kiberbiztonság kérdéskörét a digitális technológiák és infokommunikációs rendszerek védelmébe ágyazva, annak mintegy részeként kezeli, s ennek szellemében formálja stratégiai dokumentumrendszerét is. Az átfogó megközelítést illetően jelenleg két hivatalos dokumentummal is rendelkezik az ország. Az egyik a 2014–2017 közötti időszakra vonatkozó Digitális Agenda, a másik pedig a 2015–2025 közötti időszakot érintő Digitális Stratégia.

---

[2] Timeline, [online]. Forrás: Internethalloffame.org [2017. 11. 11.].

[3] A Deutsche Telekom részvényeinek megoszlásáról lásd: Shareholder structure, [online]. Forrás: Telekom.com [2017. 11. 11.].

[4] Diann Rusch-Feya – Hans Jürgen Becker: Global Info: The German Digital Libraries Project, [online], *D-Lib Magazine,* 5. évf., 1999/4. Forrás: Dlib.org [2017. 11. 11.].

[5] Two in Five Internet Users in Germany Hit by Cybercrime in 2013, [online], 2014. 04. 21. Forrás: Emarketer.com [2017. 11. 11.].

[6] Cost of Cyberscrime Study 2017. Insight on the security investments that make a difference, [online], Ponemon Institute, 2017. 13. o. Forrás: Accenture.com [2017. 11. 11.].

A *Digitális Agenda 2014–2017* elnevezésű stratégiai dokumentumot[7] a német szövetségi kormány 2014. augusztus 20-án adta ki. A digitális teret illetően ez a dokumentum szerepel a stratégiai hierarchia csúcsán, mivel ezt maga a szövetségi kormány jegyzi. Az agenda a német lakosságot a középpontba helyezve három alapvető stratégiai célt rögzít: az elterjedés és a foglalkoztatottság szintjének növelése, a digitális lehetőségekhez való hozzáférés és a részvétel biztosítása, valamint a bizalom és a biztonság megteremtése. Az e célok megvalósításához szükséges alapot az alkotmányban rögzített értékek biztosítják, amelyek érvényesülését nemcsak a valós, hanem a virtuális világban is biztosítani kell. A Digitális Agenda a célok eléréséhez hét területet érintően fogalmazza meg a szükséges intézkedéseket:

1. A digitális infrastruktúra vonatkozásában az egyik fontos lépés 2016. január 27-én a gyors internethálózatok kiépítését megkönnyítő szabályozást tartalmazó törvény elfogadása volt. Németország célja, hogy 2018-ra a legalább 50 Mbps sebességű internet-hozzáférést az ország egész területén biztosítani tudja – ami elérhetőnek is tűnik annak fényében, hogy ez a sebességű internet már 2016-ban a háztartások 70%-a számára rendelkezésére állt.
2. A digitális gazdaság és a digitális munkahelyek megteremtése körében külön kormányzati segítséggel ösztönzik a fiatal IT-vállalatok és startupok működését. Ezzel kapcsolatban összességében elmondható, hogy Németország már jelenleg is igen jó mutatókkal rendelkezik (lásd lent a további kormányzati dokumentumokban foglaltakat).
3. Az innovatív kormányzás címszó alatt az Agenda a közszféra digitális transzformációját érti. Ez a kormányzati szolgáltatások könnyebb és biztonságosabb elérhetőségét, valamint hatékonyabb ügyintézést takar, amelyet a kormányzat „2020 Digitális Közigazgatás" elnevezésű program keretében részletez.[8]
4. Fontos lépés a lakosság számára a digitális környezet megteremtése, amihez szükséges a német állampolgárok aktív együttműködése is. Ezt egyrészt párbeszédes keretek között képzelik el, így ismertetve meg a lakossággal a rendelkezésre álló lehetőségeket, másrészt pedig az adódó akadályozó tényezők felszámolásával.
5. Az oktatás, a K+F, a kultúra és a média vonatkozásában valamennyi érintett szereplő bevonására szükség van ahhoz, hogy megfelelő tudásbázist kiépítve az ország innovatív maradhasson.
6. Az online térben való biztonság és védelem garantálása mind az egyének, mind pedig a vállalatok számára létkérdés, és az Agendában felmerülő valamennyi kérdés megoldásának kiindulópontját képezi.
7. Az Agendában foglaltaknak – és így a német fejlesztési irányoknak – mind az európai szabályozással, mind pedig a globális, nemzetközi vonatkozásokkal összhangban kell lennie. Németország élharcosa marad az „internet nemzetközi joga" további formálásának, csakúgy, mint az emberi jogok érvényesülésének és érvényesítésének a digitális világban.

[7] Digital Agenda 2014–2017, [online], 2014. 08. Forrás: Digitale-agenda.de [2017. 11. 11.].

[8] A *Digitális Adminisztráció 2020* (Digital Administration 2020) elnevezésű programról szóló összefoglalót lásd: Digital Administration 2020 – Summary, [online]. Forrás: Verwaltung-innovativ.de [2017. 11. 11.].

2017. április 26-án a német kormány értékelte az Agenda három évét, és azt állapította meg, hogy Németország fel van készülve a digitális jövőre. Mindezt alátámasztják azon további kormányzati dokumentumok és intézkedések is, amelyeket a következőkben ismertetek.

A másik kormányzati dokumentum, amely Németország digitalizációval kapcsolatos hivatalos irányvonalait meghatározza, a *Digitális Stratégia 2025*,[9] amelyet a Szövetségi Gazdasági és Energetikai Minisztérium adott ki 2016 áprilisában. A dokumentum kiadásával a kormány célja az volt, hogy az ország a technológiai fejlődés új hullámának is egyik vezető állama legyen, s ezt elsősorban infrastrukturális fejlesztésekkel, a befektetések támogatásával és innovatív fejlesztésekkel kívánják elérni. A stratégia kiadását követő első év értékelése alapján igen biztató kép rajzolódik ki: a szektor bevételei 1,3%-kal nőttek, elérve a 161,4 milliárd eurót,[10] az infokommunikációs szektorban pedig mindössze egy év alatt 21 ezer új munkahelyet sikerült létesíteni.[11]

A stratégia egy 10 pontból álló program alapján képzeli el a fenti célkitűzés megvalósítását.

1. 2025-re létre kíván hozni egy 1 GB-os, az országban mindenhol elérhető optikai hálós hálózatot, amelynek közel 100 milliárd eurós költségvonzata várható. Ezzel kapcsolatban a dokumentum rögzíti, hogy jelenleg a német internet még elég lassú: a háztartások mindössze 6%-a rendelkezik 16 Mbps-os internet-hozzáféréssel (bár a lakosság 96%-ánál a legalább 2 Mbps sebességű internet már elérhető). Ezen a területen a fejlesztés azért is elengedhetetlen, mert a vezetékes globális adatforgalom minden 40 hónapban megduplázódik, míg a mobilforgalom esetében a duplázódás időtartama még rövidebb, mindössze másfél év.
2. Egy új startupkorszak felvirágoztatása, amelyben az új vállalatok és a már működő cégek közötti együttműködést fokozni kell. A startupok a digitális átalakulás motorjai, ezért is fontos a támogatásuk. Ugyanakkor egy új startupvállalkozás beindítása igen költséges: átlagosan 2,5 millió euró befektetést igényel két év távlatában.[12] Problémát jelent, hogy a vállalkozások egy jelentős része nem bizonyul életképesnek és idővel eltűnik a piacról: az 1995 és 2015 között alakult high-tech vállalatok 40%-a megszűnt, ami igen jelentős arányt jelent. Ugyanakkor nagyon biztató tendenciák is vannak, és Berlin ezen a területen is kiemelkedik: 2015-ben 2,1 milliárdnyi beruházást sikerült magához vonzania,[13] s ezzel az európai városok közül az első helyen végzett.[14]
3. A szabályozási keretek megalkotása körében a legfőbb célkitűzés a digitális egységes piac megteremtése mind nemzeti keretek között, mind pedig európai szinten. Ennek egyik előfeltétele az e-kereskedelem előtt tornyosuló akadályok lebontása, mivel ez a terület már jelenleg is a GDP 2,5%-át teszi ki. A dokumentum javasla-

[9] Digital Strategy 2025, [online]. Forrás: De.digital [2017. 11. 11.].

[10] Két területen kiemelkedően emelkedtek a bevételek: a szoftverekből származó összegek 6,3%-kal nőttek, elérve a 23 milliárd eurót, míg az IT-szolgáltatásokból származóak 2,3%-os növekedést mutattak, elérve a 39 milliárd eurót.

[11] Digital Strategy 2025 – One year on, [online], 2017. 03. 20. Forrás: Gtai.de [2017. 11. 11.].

[12] Start-ups benötigen im Schnitt 2,5 Millionen Euro frisches Kapital, [online], 2015. 06. 11. Forrás: Bitkom.org [2017. 10. 10].

[13] Ezen összeg nagy része azonban egyetlen beruházótól, a Rocket Internet vállalattól származott.

[14] Az ötödik és hatodik helyen is német városok állnak: az ötödik Hamburg 296 millió, a hatodik pedig München 206 millió eurós beruházással.

tot fogalmaz meg egy digitális jogi kódex megalkotására, amelyben egyesülhetnek olyan alapelvek, mint a nyitott és tisztességes verseny elve, az adatbiztonság és információs autonómia, vagy az európai harmonizáció.

4. Az „okoshálózatok" támogatása a gazdaság olyan kulcsfontosságú területein, mint az energiaszektor, a közlekedés, az egészségügy, az oktatás, a közigazgatás,[15] amihez megfelelő és kiszámítható jogi környezetet kell teremteni, beruházásokat könnyítő mechanizmusokat kell felállítani, és nemcsak az össznemzeti szövetségi kereteket kell kiépíteni, hanem a hálózatok európai szinergiáját is.
5. Az adatbiztonság erősítése és az információs autonómia kialakítása azért is kiemelkedően fontos feladatok, mert ezek nélkül az ország könnyen elveszítheti versenyképességét és jövőbeni gazdasági erejét. Ez a kérdéskör a kis és közepes vállalatok esetében különösen fontos, mert 61%-ukat éri kibertámadás (az országos átlag 51%-ával szemben, ami a német gazdaságnak 51 milliárd eurós kárt okoz).[16]
6. A kis- és középvállalatok számára új üzleti modell megalkotása azért is szükséges lépés, mert e vállalatok 51%-a esetében a digitalizáció még nem része az üzleti stratégiájuknak. Erre vonatkozóan már léteznek kezdeményezések, de a német kormány azt is tervezi, hogy a digitalizáció fejlesztése érdekében külön kampányt[17] indít, amelynek részeként 1 milliárd eurót különítenek el e célra a Digitális Beruházási Program[18] keretében 2018-ig.
7. Az Ipar 4.0 megoldások[19] alkalmazása az ország további modernizációjának elengedhetetlen feltétele. Előrejelzések szerint hozzáadott értékként csak Németországban 425 milliárd euró értéket fognak ezáltal előállítani, amelyből a következő öt évben leginkább az autógyártás (13,6%-kal, 52,5 milliárd euró értékben), a gépgyártás (13,2%-kal, 32 milliárd euró értékben), a sorozatgyártással működő iparágak (8,1%-kal, 30 milliárd euró értékben), az elektronikai iparág (13%-kal, 23,5 milliárd euró értékben) és az infokommunikációs szektor (13,4%-kal 15 milliárd euró értékben) fogja a bevételeit növelni. A stratégiában rögzített cél, hogy Németország váljék az Ipar 4.0 megoldások vezető támogató és alkalmazó államává, s ezáltal a világ legmodernebb országa legyen.[20]
8. A digitális K+F terén elérni kívánt kiváló eredményekhez megfelelő ösztönzésre van szükség – ilyen lehet például az adócsökkentés. Jelenleg a német vállalatok mindösz-

---

[15] Ennek támogatására a szövetségi kormány 2015 őszén külön stratégiát fogadott el: az Okos Hálózatok Stratégiáját (Smart Networks Strategy).

[16] In the last two years over half of German companies have been hit by sabotage, [online], 2017. 07. 21. Forrás: Businessinsider.com [2017. 11. 11.].

[17] Digitalisierungsoffensive Mittelstand – Digitalisation campaign for SMEs.

[18] Digitales Investitionsprogramm Mittelstand – Digital investment program for SMEs.

[19] Az Ipar 4.0, más néven a negyedik ipari forradalom (a gőzgépek megjelenése, a tömeggyártás és az automatizálás után), amikor a fizikai-kiberrendszerek veszik át a vezető szerepet a termelésben, s ezáltal a gyártóipar digitalizációja zajlik.

[20] A Szövetséges Gazdasági és Energetikai Minisztérium 2017. június 20-án adta ki a Plattform Industry 4.0 – Digitale Transformation „Made in Germany" elnevezésű brosúráját (lásd: Plattform Industrie 4.0., [online], 2018. 03. Forrás: Bmwi.de [2017. 11. 11.]), amely az e területen rejlő együttműködési lehetőségeket vázolja fel. A platform már jelenleg is a világ legnagyobb együttműködési fóruma több mint 100 vállalat 250 delegáltjával, és számos ország számára modellként tud szolgálni. (A platformról részletesebben lásd: Plattform Industrie 4.0., [online]. Forrás: Plattform-i40.de [2017. 11. 11.]).

sze az éves kutatási költségeik 14%-át költik a digitális technológiák kereskedelmi alkalmazásának kutatására (az Egyesült Államok ennek kétszeresét). Ezen a területen Európa összességében jelentős lemaradásban van a világ más részeihez képest: míg Európa az infokommunikációs technológiákba mindössze a GDP 0,21%-át fekteti be, addig ez az arány Japán esetében 0,57%, az Egyesült Államokban 0,58%, Dél-Koreában pedig 1,47%.[21]

9. A digitális írástudást az élethosszíglan tartó tanulási folyamat szerves részévé kell tenni. A világszinten jelentkező szakemberhiány Németországot is sújtja: az országnak 2020-ig 3,5 millió szakemberre volna szüksége, ugyanakkor jelenleg is 40 ezer álláshely betöltetlen a szektorban. Stratégiai célkitűzés, hogy 2025-re Németországban minden diák rendelkezzen alapvető informatikai ismeretekkel, és az ehhez szükséges oktatási segédanyagok online elérhetők legyenek. Ezáltal az oktatási szektorban kialakított digitális infrastruktúra tekintetében az ország az egyik vezető állammá válhat mind az iskolarendszerű oktatást, mind a szakképzést, mind pedig a felsőoktatást illetően.
10. Mindehhez pedig szükséges egy digitális ügynökség felállítása, amely modern kiválósági központként működhet. Jelenleg ugyanis igen széttöredezett a digitalizációt érintő szervezeti struktúra, s ez a probléma egy központi szerv felállításával orvosolható volna. Az új szövetségi ügynökséget három pillérre építve tervezik felállítani: a kompetenciák összehangolása, a politikai digitális agenda támogatása, valamint a digitális kompetencia fenntartható módon való kiépítése gazdasági, jogi és technikai oldalról egyaránt. Első lépésként a Szövetségi Hálózati Ügynökség elemzési és reagáló képességének fejlesztése várható, majd – az európai jogalkotási folyamat tükrében – a nemzeti, szabályozási jogkörrel rendelkező hatóságok felelősségi körét kell kibővíteni.

A Digitális Stratégia tehát igen átfogóan kezeli a digitalizáció szükségességének kérdéskörét, és minden területet érintően azon van, hogy Németország azt a vezető pozíciót, amelyet már évekkel korábban kivívott magának e területen, meg tudja őrizni azáltal, hogy az újabb és újabb megoldásokat átveszi és azokat minden lehetséges területen alkalmazza. Jó példa erre az Ipar 4.0 megoldások elterjedése: már jelenleg is a német vállalatok fele foglalkozik legalább kísérleti vagy bevezetés előtti fázisban ilyen lehetőségekkel, a vállalatok egyharmada pedig már most is rendelkezik piacképes megoldásokkal.[22] Ezt egyetlen másik állam sem mondhatja el magáról.

A két átfogó hivatalos dokumentum mellett mindenképp röviden említést kell tenni néhány aktuális kormányzati forrásról is. Ezek közül elsőként a legfrissebb, 2017. március 1-jén a Szövetséges Gazdasági és Energetikai Minisztérium által kiadott *Digitális*

[21] A lemaradáshoz kapcsolódóan további mutató például, hogy a telekommunikációval összefüggésben kiadott szabadalmak száma az Egyesült Államokban ötszöröse az európainak, és – ehhez kapcsolódóan – a Dolgok Internetével *(Internet of Things – IoT)* összefüggő szabadalmakból Európában mindössze 6%-kal részesedik.

[22] Minden harmadik német cégnek már van „okos" terméke, [online], 2017. 05. 02. Forrás: Hirado.hu [2017. 11. 11.].

Platform Fehér könyvét[23] említem meg. Kiadását egy több hónapos konzultációs folyamat is megelőzte, de közvetlen előzményként említhető az egy évvel korábban, 2016. június 1-jén kiadott *Zöld könyv,*[24] amely azt a kérdéskört járja körül, hogy megfelelő szabályozási keretek kialakításával hogyan lehet jogilag kiszámítható környezetet létrehozni a digitális világban működő vállalatok számára, ahol a tisztességes verseny és a felhasználók érzékeny adatainak védelme biztosított, és érvényesülnek a demokratikus kultúra alapelvei a digitális térben is. A fehér könyv Németországot és Európát elválaszthatatlan egységként kezeli, és a szabályozási keretek megteremtését csak európai keretek között tartja megvalósíthatónak. Elsődleges kívánalom a tisztességes verseny megteremtése. Ezt elősegítheti a versenyeljárások felgyorsítása és a versenyjogi szabályok átdolgozása (például úgy, hogy a versenyhatóságot közvetlen szankcionálási jogkörrel ruházzák fel), támogatva ezzel a modern adatgazdaság kiépítését. Ezzel összefüggésben a fehér könyvben is megjelenik az a legfőbb kormányzati cél, hogy 2025-re országszerte kiépülhessen az 1 Gbps-os internet, amelyre a német kormány 10 milliárd eurót különített el. Mindennek átfogó keretét a demokratikus digitális kultúra biztosítása adja: legfőbb kívánalom, hogy az alapvető jogok érvényesülése a virtuális térben is biztosított legyen, az esetleges jogi hiányosságokat pedig mihamarabb sikerüljön kiküszöbölni.

A kormányzati források köréből végül kiemelem a *Digitális gazdaságról szóló jelentés*t, amelyet 2016. október 1-jén adtak ki.[25] A német fejlődés évek óta töretlen, és ezt a jelentésben foglaltak is teljes mértékben alátámasztják. 2015-ben a német infokommunikációs szektor 223 milliárd euró bevételt termelt, ezzel az Egyesült Államok, Kína, Japán és az Egyesült Királyság után a világ ötödik legnagyobb piacának számít. A német internetgazdaság által generált bevételek összege eléri a 111 milliárd eurót (egy főre vetítve ez 1379 eurót jelent), s ez szintén az ötödik helyre rangsorolja az országot. Bár a digitalizáció mértéke szektoronként eltérő (az egészségügy például a visszahúzó ágazatok között szerepel, míg az infokommunikációs szektorban és a tudásalapú szolgáltatások körében kiemelkedő a digitalizáció mértéke), a digitális gazdasági index mutatói alapján Németország az előző évi 49 ponthoz képest 2016-ban 55 pontot ért el (a lehetséges 100 pontból), és 2021-re várhatóan eléri az 58 pontot, tehát a növekedés stabilitása és volumene adott.

Ha a német digitális gazdaságot összességében értékelni szeretnénk, az ország erősségeit és gyengeségeit egyaránt nevesíteni kell. Az erősségek körében említhető a német piac termékeihez és szolgáltatásaihoz való akadálytalan hozzáférés belföldön és külföldön egyaránt, a német infokommunikációs termékek iránti volumenét tekintve is nagy, de egyre növekvő kereslet (elsősorban Japán részéről, másodsorban Franciaország, India és Kína részéről), a szektor bevételeinek konstans növekedése (amelyet szakemberek a digitális gazdaság mutatójaként értékelnek), valamint az infokommunikációs szektor és a gazdaság más területei közötti olyan erős kapcsolat megléte, mint sehol máshol a világban. A gyengeségek közt említhető első helyen a szakképzett munkavállalók hiánya, de hasonlóképp megoldásra vár

[23] White Paper Digital Platform. Digital regulatory policy for growth, innovations, competition and participation, [online], 2017. 03. 01. Forrás: Bmwi.de [2017. 11. 11.].

[24] Green Paper Digital Platforms, [online], 2016. 06. 01. Forrás: Bmwi.de [2017. 11. 11.].

[25] Monitoring Report: Digital Economy 2016, [online], 2016. 10. 01., Federal Ministry for Economic Affairs and Energy. Forrás: Bmwi.de [2011. 11. 11.].

a hálózatok kiépítése vagy a szabályozási keretek megalkotása, illetve hozzáigazítása a változó nemzetközi környezethez, de problémás továbbá a sikeres startupok hiánya és a lakosság körében a technológia iránti általános érdektelenség. Ha Németországnak ezen gyengeségeket sikerül kiküszöbölnie, valóban világvezető állammá válhat ezen a területen (is).

A német kiberbiztonsági stratégia

Németország 2011-ben alkotta meg első kiberbiztonsági stratégiáját.[26] Ez a stratégia még az úgynevezett első generációs stratégiák sorába illeszkedett, amelyek általában – és így a német is – az online bizalom megteremtését tűzték ki legfőbb célként, növelve ezáltal a gazdasági és társadalmi prosperitást.[27] Németország 2016-ban újabb stratégiát adott ki,[28] amely már a második generációs stratégiák tipikus jegyeit viseli magán. A benne foglaltak ugyanis alkalmazkodtak az elmúlt években megváltozott biztonsági környezethez és a kihívások átalakult természetéhez, és összhangban azzal, hogy a kiberbiztonság a társadalom egészének védelmét érintő nemzeti prioritássá vált, immáron holisztikus megközelítést alkalmaz, amelynek értelmében valamennyi biztonsági szektorra és a társadalom egészére kiterjeszti hatókörét. Mindkét stratégia kiadását megelőzte a *Biztonságpolitikáról és a Bundeswehr jövőjéről szóló Fehér könyv* mint legfőbb biztonságpolitikai dokumentum átdolgozása. A 2016 őszén kiadott fehér könyv[29] már kiemelten foglalkozik a kiberbiztonság kérdéskörével, és a kiberkockázatokat a legmagasabb fokú nemzetbiztonsági kockázatok között említi. Rögzíti továbbá, hogy a kibertérben kialakuló konfliktusok hatásukat tekintve megegyeznek a hagyományos fegyveres konfliktusokkal, és a jövőben ezekkel fokozottan számolni kell.

A 2016-os stratégia kibertér-definíciója tükrözi azt a fent már említett német megközelítést, miszerint a hangsúlyt a digitális térre mint egységes egészre helyezik, és a kiberbiztonság kérdéskörét ennek keretein belül szabályozzák. A kibertér német értelmezés szerint az internetet és az infokommunikációs eszközöket foglalja magába (ezzel szemben általánosan elfogadott, hogy a kibertér a fizikai és virtuális infokommunikációs rendszerek hálózatát jelenti). Ennek értelmében kibertámadásnak minősül az IT-rendszerek elleni olyan

[26] Cyber Security Strategy for Germany, [online], 2011. Federal Ministry of the Interior. Forrás: Cio.bund.de [2017. 11. 11.].

[27] A 2011-es német kiberbiztonsági stratégiában foglaltak részletes ismertetésétől eltekintek, mivel az abban foglaltak szinte kivétel nélkül megvalósultak a 2011–2016. között eltelt öt esztendő alatt. A stratégia 10 nagy területet érintően fogalmazta célkitűzéseit: 1. a kritikus információs infrastruktúra védelme; 2. az IT-rendszerek biztonságának garantálása; 3. az IT-biztonság erősítése a közigazgatásban; 4. Nemzeti Kiberreagálási Központ felállítása; 5. Nemzeti Kiberbiztonsági Tanács felállítása; 6. a bűnözés hatékony ellenőrzése a kibertérben; 7. hatékony koordinált akciók végrehajtása, hogy Európában és világszerte is biztosítható legyen a kiberbiztonság; 8. megbízható információs technológiák használata; 9. a szükséges személyi állomány biztosítása a szövetségi ügynökségeknél; 10. a kibertámadásokra adandó válaszokhoz megfelelő eszközpark.

[28] Cyber-Sicherheitsstrategie für Deutschland, [online], 2016, Bundesministerium des Innern. Forrás: Bmi.bund.de [2017. 11. 11.].

[29] White Paper on German Security Policy and the Future of the Bundeswehr 2016, [online], 2016. 06., The Federal Government. Forrás: Bundeswehr.de [2017. 11. 11.].

támadás is, amely veszélyeztetheti az információs rendszerek megbízhatóságát vagy integritását – jelezve ezzel is az adatvédelem fontosságát.[30]

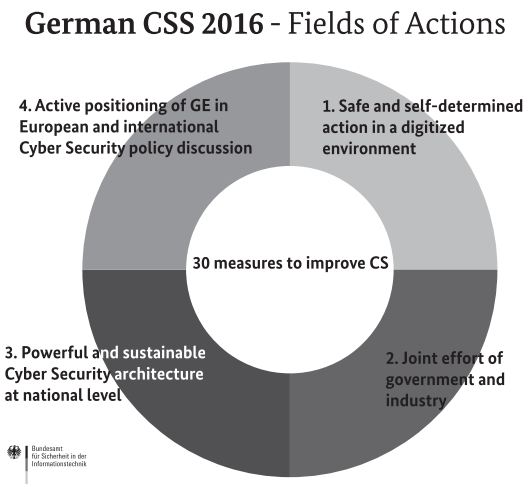
A német stratégiában a gazdasági prosperitás és a digitális téren történő innovációk egymást kölcsönösen feltételezik és támogatják. Ugyanakkor a dezinformációs és manipulációs támadások száma és hatása egyre jelentősebbé válik, s ez hosszú távon a társadalmi stabilitást is aláásható. Ezért a kiberbiztonságot olyan központi kihívásként kell kezelni, amely területen bekövetkezett esetleges támadás az államot, az üzleti szférát és a társadalmat egyaránt közvetlenül érint(het)i. A központi kormányzatnak mindenképpen oroszlánrészt kell vállalnia a kiberbiztonság szabályozásában és az incidenskezelésben, valamint valamennyi szektorra és érintett személyi körre vonatkozóan kiterjedt konzultációkat kell folytatnia. Az együttműködés azonban nem korlátozódhat nemzeti keretekre, hanem összeurópai – de lehetőség szerint világméretű – együttműködési csatornákat kell kialakítani. Németország a bilaterális partneri kapcsolatok fontosságát hangsúlyozza, elsősorban az információmegosztás és a határon átnyúló szolgáltatásokkal kapcsolatos biztonsági kérdések összehangolása, valamint a kapacitások megosztása terén. Emellett fontosnak tartja a fejlesztési együttműködés fontosságát is, elsősorban olyan területeken, mint a kibertérben történő biztonság- és bizalomerősítő intézkedések terén a fejlődő államok vonatkozásában. Németország továbbra is élharcosa az adatbiztonság garantálásának; ez a kérdéskör a stratégiában is kiemelten szerepel, külön nevesítve azt a nemzetközi együttműködéssel összefüggésben is. Az egyes nemzetközi szervezetek vonatkozásában a stratégia külön részletezi, hogy mely szervezet a kiberbiztonság melyik területét érintően lát el különösen fontos feladatokat.

A stratégia kiemelten kezeli a német ipar erősítésének kérdéskörét, s a versenyképesség javítása és a nemzeti informatikai ipar megerősítése érdekében javasolja az *„IT Security Made in Germany"* termékek és szolgáltatások kifejlesztését.

A stratégia újításának tekinthető egyrészt az, hogy a kiberbiztonság katonai dimenzióját külön is nevesíti, és azt elkülönülten kezeli a civil kiberbiztonsági kérdésektől. Másrészt nóvum, hogy a külföldi megfigyelési technikák visszaszorítása érdekében célul tűzi ki egy nemzetközileg elfogadott exportellenőrzési rendszer kiépítését.

Mindezen irányvonalakat a stratégia négy nagy cselekvési területbe sorolva ismerteti. Ezek az 1. ábra alapján a biztonságos és önálló cselekvés a digitális környezetben; a kormányzat és az ipar közös erőfeszítései; az erős és fenntartható kiberbiztonsági rendszer kiépítése nemzeti szinten, valamint Németország megfelelő pozicionálása az európai és a nemzetközi kiberbiztonsági politikai megbeszéléseken.

[30] Ez egyúttal azt is jelenti, hogy Németországban a kibertérben végzett kutatás is kiberbűncselekménynek minősülhet – míg más államok esetében ez a digitális információ, a kiberhálózatok vagy az infokommunikációs eszközök elleni kibertámadásnak minősülne.



1. ábra: A 2016-os német kiberbiztonsági stratégiában rögzített négy cselekvési terület

Forrás: National Cybersecurity Strategy 2016, [online], 2017. 04. 26., Samuel Rothenpieler (BSI) előadása Athénban. Forrás: Enisa.europa.eu [2017. 11. 11.]

A német kiberbiztonsági szervezetrendszer[31]

A német stratégiafejlődés mozgatórugója a Szövetségi Belügyminisztérium, amely szorosan együttműködik a Külügyminisztériummal, a Védelmi Minisztériummal, a Gazdasági és Energetikai Minisztériummal és az Igazságügyi Minisztériummal. A 2011-es stratégiának megfelelően a kormányzat felállított egy *nemzeti incidenskezelő központot (Nationales Cyber-Abwehrzentrum – NCAZ),* amelynek a feladata a kormányzati szervek közötti műveleti szintű kooperáció és IT-incidensek esetén a válaszlépések összehangolása. A NCAZ az incidensekre való gyors reagálás érdekében nemzeti irányítási-vezetési és elemzőközponti funkciókat lát el. Emellett tájékoztatja a társadalmat a sérülékenységekről, támadásokról, elkövetőkről. A Belügyminisztérium irányítása alá tartozó Szövetségi Információbiztonsági Hivatal *(Bundesamt für Sicherheit in der Informationstechnik – BSI)*[32] felel az incidenskezelő központ feladatainak végrehajtásáért. Más hatóságok, mint a Szövetségi Alkotmányvédelmi Hivatal *(Bundesamt für Verfassungsschutz – BfV)* és a Civil Védelem és Katasztrófavédelmi Szövetségi Hivatal *(Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – BBK),* a Szövetségi Bűnügyi Rendőriroda *(Bundeskriminalamt – BKA),* a Szövetségi Rendőrség *(Bundespolizei – BPOL),* a Bűnügyi Vámhivatal *(Zollkriminalamt – ZKA),* a Szövetségi Hírszerzési Hivatal *(Bundesnachrichtendienst – BND),* a német hadsereg (Bundeswehr) és a kritikusinfrastruktúra-üzemeltetőket felügyelő hivatalok is együttműködnek egymással

[31] The State of IT Security in Germany 2016, [online], 2016. 10., Federal Office for Informations Security. Forrás: Bsi.bund.de [2017. 11. 11.].

[32] A BSI-t eredetileg 1991-ben hozták létre IT-biztonsági szolgáltatások nyújtására a köz- és a magánszféra számára.

az incidenskezelő központon belül a konkrét eseteknek megfelelően. A központ incidens esetén a Szövetségi Belügyminisztériumot közvetlenül tájékoztatja. A BSI a fent leírtakon túl a nemzeti kiberbiztonsági hatóság szerepét is betölti, és felel a kiberbiztonsági stratégia végrehajtásáért. A BSI emellett a központi kiberincidens-bejelentő központ is, így az infokommunikációs termékekkel kapcsolatos sérülékenységekről is ez a szerv adja ki a figyelmeztetést és javasol ellenlépéseket.

A fent leírtakon túl a 2011-ben megalakult Nemzeti Kiberbiztonsági Tanács (*Nationaler Cyber-Sicherheitsrat* – a továbbiakban: Tanács), amelynek a feladata a kormányzaton belüli tárcák, valamint a köz- és magánszféra közötti kooperáció erősítése és a legfelsőbb szintű vezetők számára javaslatok megfogalmazása stratégiai kérdésekben. A Tanács a Szövetségi Kormányzati Információtechnológiáért Felelős Megbízott/Biztos *(Beauftragter der Bundesregierung für Informationstechnik – BfIT)* irányítása alá tartozik, és tevékenységében részt vesznek a Szövetségi Kancellária és az államtitkárságok, valamint a szövetségi tárcák és a szövetségi régiók képviselői, szükség esetén pedig az üzleti élet és tudományos közvélemény képviselői is. A Tanács mellett működik a Kiberbiztonsági Szövetség *(Allianz für Cyber-Sicherheit)*.[33] A BSI által 2012-ben alapított non-profit szervezet a legkiterjedtebb nemzeti együttműködési platform 100 partnervállalat mintegy 2000 résztvevőjével. Nyitva áll az üzleti világ és tudományos közélet, valamint a hivatalos szervezetek intézményei előtt, és célja az információcsere segítése és egy átfogó tudásbázis létrehozása – ennek érdekében eddig mintegy 100 dokumentumot adott ki a folyamatos figyelmeztetések és havi jelentések mellett.

A BSI által működtetett Nemzeti Információtechnológiai Szituációs Központ *(Nationales IT-Lagezentrum)*[34] a nemzeti és globális IT-biztonság fejleményeit kíséri figyelemmel az IT-biztonsági incidensek gyors felderítése, elemzése és a hatékony válaszlépések megtétele érdekében. Súlyos IT-incidenseket Nemzeti Információtechnológiai Krízisreagáló Központtá átalakulva képes kezelni.

Németországban számos *CERT*[35] működik. Az elsőt 1994-ben a BSI hozta létre (BSI-CERT), amely főként információgyűjtéssel foglalkozott. 2001-ben kormányzati CERT-té, CERT-BUND-ra[36] változtatva a nevét, jelenleg pedig már nemzeti CERT-ként üzemel, együttműködve mind az állami, mind a nem állami CERT-ekkel. A BSI 2006-ban hozta létre az állampolgárok CERT-jét, a Bürger-CERT-et.[37]

A kiberbiztonság védelmi aspektusai a Szövetségi Védelmi és Honvédelmi Minisztérium illetékességi körébe tartoznak. 2016-ban felállították a Kiber- és Információs Parancsnokságot *(Kommando Cyber- und Informationsraum – KdoCIR),* amely a Bundeswehr kibertevékenységet végző egységeit olvasztotta magába és a kiber-, IT- (hálózati), katonai hírszerzési, geoinformációs és műveleti kommunikációért felelős. A Védelmi Minisztérium tervei szerint a jövőben képes lesz visszavágni az országot támadó kiberműveletek esetén.

[33] Alliance for Cyber Security, [online], Federal Office for Information Security. Forrás: Allianz-fuer-cybersicherheit.de [2017. 11. 11.].
[34] IT-Lagezentrum, [online]. Forrás: Bsi.bund.de [2017. 11. 11.].
[35] Computer emergency response team – feladatuk a hálózatbiztonsági incidenskezelés és az információ terjesztése.
[36] CERT-Bund, [online]. Forrás: Bsi.bund.de [2017. 11. 11.].
[37] Bürger-CERT, [online]. Forrás: Buerger-cert.de [2017. 11. 11.].

A Bundeswehr Stratégiai Hírszerző Egysége *(Kommando Strategische Aufklärung, Abteilung Informations- und Computernetzwerkoperationen)* főként védelmi célú kapacitások kiépítésén dolgozik, bár már támadó kapacitással is rendelkezik.[38] Legújabb fejlemény pedig, hogy 2017 áprilisában felállították a német kibervédelmi parancsnokságot is, bonni székhellyel, amely kezdeti 260 fős létszáma már a nyárra 13 500 főre emelkedett, és a tervek szerint 2021-re éri el a teljes készültség állapotát, 14 500 fővel (köztük 1500 polgári alkalmazottal). A kiberegység fogja védeni valamennyi katonai egység biztonságát, beleértve a földi, légi, tengeri, orvosi alakulatokat és az egyesített erőket is.[39]

A német kiberbiztonság értékelése

Az egyes államok kiberbiztonságát több mutató segítségével is értékelhetjük. Ezek közül kiemelem az ENSZ szakosított intézménye, a Nemzetközi Távközlési Egyesület (*International Telecommunication Union* – a továbbiakban: ITU) által jegyzett *globális kiberbiztonsági indexet,*[40] amely öt: jogi, technikai, szervezeti, kapacitásépítési és együttműködési területen értékeli az államok felkészültségét. Az összesített értékelést tekintve Németország a három nagy kategóriába sorolt listán a középső kategóriában lévő államok között foglal helyet. Ez összpontszámot tekintve 0,679 pontot jelent, amellyel az európai országok körében a 11., világviszonylatban pedig a 24. helyen áll.[41] Az egyes területeken elég jelentős eltérések vannak az ország fejlettségét illetően. Az első, a jogi területen az összesített értékelés – a három fokozatú skálán – közepesnek mondható a kiberbiztonsági felkészítés-képzés kategóriában elért rossz eredmény következtében (amelyet még a másik két kategória kiváló minősítése sem tudott kellőképp ellensúlyozni). Kiemelkedően teljesített viszont a technikai területet illetően: mind a hat alkategóriájában a legjobb minősítést érte el Németország. A szervezeti keretek körében összességében a legjobb minősítést kapta, azonban a kapacitásépítés és az együttműködés kategóriáiban csak közepest, az olyan területeken meglévő hiányosságok miatt, mint például a két- és többoldalú egyezmények igen alacsony száma, vagy a szegényes oktatási programkínálat.

Hasonló eredményt mutat a *kiberhatalmi index* is,[42] amely négy kategóriában vizsgálja a világ 20 legfejlettebb államának kiberbiztonsági szintjét. Az összesítést tekintve Németország 68,2%-kal a 4. helyen áll,[43] azonban elég nagyok az eltérések az egyes kategóriákban kapott értékelések között. Az első mérőszám a jogi és szabályozási keretek fejlettségét méri, amely alapján Németország a G20-országok vezető állama lett, közel hibátlan teljesítményt magáénak tudva 99,3 ponttal. A második kategória esetében, amely a gazdasági-szociális helyzetet vizsgálja a 7. helyet foglalja el 52,9 ponttal. A technológiai

[38] Germany Reveals Offensive Cyberwarfare Capability, [online], 2012. 06. 08. Forrás: Atlantic Council [2017. 11. 11.].
[39] Kiberegységet állít fel a német hadsereg, [online], 2017. 04. 06. Forrás: Hu.euronews.com [2017. 11. 11].
[40] Global Cybersecurity Index 2017, [online], 2017, International Telecommunication Union, Geneva, Switzerland. Forrás: Itu.int [2017. 11. 11.].
[41] A ranglistát Szingapúr vezeti 0,925 ponttal, őt követi az Egyesült Államok 0,919 ponttal, a harmadik helyen pedig Malajzia áll 0,893 ponttal.
[42] Cyber Power Index 2012, [online]. Forrás: Sbs.ox.ac.uk [2017. 11. 11.].
[43] Az index alapján a vezető államok az Egyesült Királyság 76,8%-kal, az Egyesült Államok 75,4%-kal és Ausztrália 71%-kal.

infrastruktúra vonatkozásában 60,6 ponttal az ötödik, míg a digitális infrastruktúra kiépítettsége terén 58 ponttal a hatodik.

A képet azonban árnyalja a harmadik mutatószám, a *kiberfelkészültségi index*.[44] Az index hét szempont[45] alapján osztályoz kilenc[46] vezető hatalmat, ugyanakkor végkövetkeztetésként megállapítja, hogy még egyik állam sem tekinthető teljes körűen felkészültnek kiberbiztonsági viszonyait tekintve. Németország jelenleg mind a hét vizsgált területen csak részben tekinthető működőképesnek, hasonlóan a többi vizsgált államhoz.[47]

Összegzés

Az IT-biztonság helyzetét évente értékelik Németországban. A legfrissebb jelentés 2017. november 8-án jelent meg, amelyet a szövetséges német belügyminiszter, Thomas de Maizière és a BSI elnöke, Arne Schönbohm mutatott be ünnepélyes keretek között. Bár a jelentés a szélesebb közönség számára még nem elérhető, annyi azonban már kiszivárgott, hogy az értékelés szerint a kiberfenyegetések még mindig igen magas szintet mutatnak, és ezek ellen eredményesen fellépni csak megfelelő lépésekkel lehet, így például egyes gyakran használt szoftverek sérülékenységének csökkentésével. Ezen a területen Németország jelentős lépéseket tett. „Megfelelő digitális gondosságra van szükség, felváltva a digitális nemtörődömség időszakát" – fogalmazott a miniszter összegző helyzetértékelésében.[48] Ennek látható jelei már mutatkoznak olyan lépések formájában, mint a 2015. évi IT-biztonsági törvény megalkotása, az uniós NIS-irányelv német jogba történő átültetése, az új, 2016. évi kiberbiztonsági stratégia megalkotása, vagy a BSI jogköreinek kiszélesítése. Ugyanakkor nem szabad megfeledkezni arról sem, hogy a bipoláris időszakban az Egyesült Államok által nyújtott nukleáris védőernyő helyét mostanra a kibervédőernyő vette át és jelenti a német biztonság egyik garanciáját.[49] Ez a kibervédőernyő azonban nemcsak véd (mint ahogyan azt korábban a nukleáris tette), hanem annak égisze alatt az amerikai vállalatok a lehető legtöbb adatot is összegyűjtik, s ezáltal Németország jelentős versenyhátrányba kerül a digitális gazdaságra való átállás terén. Emellett Németországban valós probléma az agyelszívás veszélye, mert fiatalok tömege dönt úgy, hogy az óceán túlpartján kezd inkább karrierbe, ez pedig további társadalmi feszültségeket generál. Végül pedig, bár Németország a védőernyő égisze alatt szívesen megspórolná az ICT-beruházások költségeit, ezt azonban nem teheti meg, mert ez esetben a közvetlen pénzügyi előnyök nem a német vállalatoknál, hanem az amerikai partnereknél fognak jelentkezni.

---

[44] Cyber Readiness Index Country Profiles, [online]. Forrás: Potomacinstitute.org [2017. 11. 11.].

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

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

[47] Germany Cyber Readiness at a Glance, [online], 2016. 10., Potomac Institute for Policy Studies. Forrás: Potomacinstitute.org [2017. 11. 11.].

[48] Cyber threat situtation requires digital diligence, [online], 2017. 11. 08. Forrás: Bmi.bund.de [2017. 11. 11.].

[49] Dornfeld László – Keleti Artúr – Barsy Miklós – Kilin Józsefné – Berki Gábor – Pintér István: *Műhelymunkák. A virtuális tér geopolitikája,* [online], Geopolitika Tanács Közhasznú Alapítvány, 2016/1, 5.2. fejezet. Forrás: Mek.oszk.hu [2017. 11. 11.].

Összességében azonban megállapítható, hogy Németország felismerte a kiberterület fontosságát és azt, hogy az ország biztonságának garantálása elképzelhetetlen e terület kontrollja és folyamatos fejlesztése nélkül. Ennek érdekében mindent megtesz mind a szabályozás, mind a gyakorlati lépések terén, és a már meglévő kapacitásai további bővítésével és nemzetközi kapcsolatai szélesítésével a jövőben is képes lehet fenntartani jó kibervédelmi képességeit – a támadó képességek fejlesztéséről nem is beszélve.

FELHASZNÁLT IRODALOM

Alliance for Cyber Security, [online], Federal Office for Information Security. Forrás: Allianz-fuer-cybersicherheit.de [2017. 11. 11.]

Bürger CERT, [online]. Forrás: Buerger-cert.de [2017. 11. 11.]

CERT-Bund, [online]. Forrás: Bsi.bund.de [2017. 11. 11.]

Cost of Cyberscrime Study 2017. Insight on the security investments that make a difference, [online], Ponemon Institute, 2017. Forrás: Accenture.com [2017. 11. 11.]

Cyber Power Index 2012, [online]. Forrás: Sbs.ox.ac.uk [2017. 11. 11.]

Cyber Readiness Index Country Profiles, [online]. Forrás: Potomacinstitute.org [2017. 11. 11.]

Cyber Security Strategy for Germany, [online], 2011. Federal Ministry of the Interior. Forrás: Cio.bund.de [2017. 11. 11.]

Cyber threat situtation requires digital diligence, [online], 2017. 11. 08. Forrás: Bmi.bund.de [2017. 11. 11.]

Cyber-Sicherheitsstrategie für Deutschland, [online], 2016. Bundesministerium des Innern. Forrás: Bmi.bund.de [2017. 11. 11.]

Digital Administration 2020 – Summary, [online]. Forrás: Verwaltung-innovativ.de [2017. 11. 11.]

Digital Agenda 2014–2017, [online], 2014. 08. Forrás: Digitale-agenda.de [2017. 11. 11.]

Digital Strategy 2025 – One year on, [online], 2017. 03. 20. Forrás: Gtai.de [2017. 11. 11.]

Digital Strategy 2025, [online]. Forrás: De.digital [2017. 11. 11.]

Dornfeld László – Keleti Artúr – Barsy Miklós – Kilin Józsefné – Berki Gábor – Pintér István: *Műhelymunkák. A virtuális tér geopolitikája,* [online], Geopolitika Tanács Közhasznú Alapítvány, 2016/1, 5.2. fejezet. Forrás: Mek.oszk.hu [2017. 11. 11.]

Germany Cyber Readiness at a Glance, [online], 2016. 10., Potomac Institute for Policy Studies. Forrás: potomacinstitute.org [2017. 11. 11.]

Germany Reveals Offensive Cyberwarfare Capability, [online], 2012. 06. 08. Forrás: Atlantic Council [2017. 11. 11.]

Global Cybersecurity Index 2017, [online], 2017, International Telecommunication Union, Geneva, Switzerland. Forrás: Itu.int [2017. 11. 11.]

Green Paper Digital Platforms, [online], 2016. 06. 01. Forrás: Bmwi.de [2017. 11. 11.]

In the last two years over half of German companies have been hit by sabotage, [online], 2017. 07. 21. Forrás: Businessinsider.com [2017. 11. 11.]

IT-Lagezentrum, [online]. Forrás: Bsi.bund.de [2017. 11. 11.]

Kiberegységet állít fel a német hadsereg, [online], 2017. 04. 06. Forrás: Hu.euronews.com [2017. 11. 11]

Minden harmadik német cégnek már van „okos" terméke, [online], 2017. 05. 02. Forrás: Hirado.hu [2017. 11. 11.]

Monitoring Report: Digital Economy 2016, [online], 2016. 10. 01. Federal Ministry for Economic Affairs and Energy. Forrás: Bmwi.de [2011. 11. 11.]

National Cybersecurity Strategy 2016, [online], 2017. 04. 26., Samuel Rothenpieler (BSI) előadása Athénban. Forrás: Enisa.europa.eu [2017. 11. 11.]

Plattform Industrie 4.0., [online], 2018. 03. Forrás: Bmwi.de [2017. 11. 11.]

Plattform Industrie 4.0., [online]. Forrás: Plattform-i40.de [2017. 11. 11.]

Rusch-Feya, Diann – Becker, Hans Jürgen: Global Info: The German Digital Libraries Project, [online], *D-Lib Magazine,* 5. évf., 1999/4. Forrás: Dlib.org [2017. 11. 11.]
Shareholder structure, [online]. Forrás: Telekom.com [2017. 11. 11.]
Start-ups benötigen im Schnitt 2,5 Millionen Euro frisches Kapital, [online], 2015. 06. 11. Forrás: Bitkom.org [2017. 10. 10]
The State of IT Security in Germany 2016, [online], 2016. 10., Federal Office for Informations Security. Forrás: Bsi.bund.de [2017. 11. 11.]
Timeline, [online]. Forrás: Internethalloffame.org [2017. 11. 11.]
Two in Five Internet Users in Germany Hit by Cybercrime in 2013, [online], 2014. 04. 21. Forrás: Emarketer.com [2017. 11. 11.]
White Paper Digital Platform. Digital regulatory policy for growth, innovations, competition and participation, [online], 2017. 03. 01. Forrás: Bmwi.de [2017. 11. 11.]
White Paper on German Security Policy and the Future of the Bundeswehr 2016, [online], 2016. 06., The Federal Government. Forrás: Bundeswehr.de [2017. 11. 11.]