

Molnár Dóra

Európai kiberdiplomáciai helyzetkép – Franciaország, az Egyesült Királyság és Németország

Az előző fejezet folytatásaként e fejezet a három vezető európai állam, Franciaország, az Egyesült Királyság és Németország kiberdiplomáciájának alapvető elméleti és gyakorlati kérdéseit mutatja be.

Franciaország mint kiberdiplomáciai nagyhatalom

Talán nem túlzás azt állítani, hogy Franciaország évszázadok óta a diplomácia fellegvára, és a franciák a *soft* eszközök alkalmazásának nagymesterei a politikában. Az ország erejét globális szerepvállalása adja, amelyhez a kiterjedt diplomáciai hálózata szolgál alapul: páratlanul széles körű tagsággal rendelkezik multilaterális és nemzetközi szervezetekben, külföldi kulturális misszióinak száma a legmagasabb, és az 5. legnagyobb segélyező állam.¹ Ezért nem meglepő, hogy a francia politika előszeretettel és hatékonyan használja a diplomácia eszköztárát a kibertérben is – olyannyira, hogy európai szinten első e téren. Ez indokolja, hogy az európai országok vizsgálatát Franciaországgal kezdem, még ha kiberhatalmi potenciál terén van más európai állam, amely megelőzi az országot.

Már az első, 2011-ben kiadott, *Az információs rendszerek védelme és biztonsága: Franciaország stratégiája* című kiberstratégiában megjelenik a kibertérbeli nemzetközi együttműködés szükségessége mint a szükséges cselekvési területek egyike.² Ezt a 2012-ben elfogadott 681. számú szenátusi információs jelentés konkretizálja azzal, hogy a tíz prioritás egyikeként hangsúlyozza a bilaterális kapcsolatok fontosságát, közös akciókat sürget az Észak-atlanti Együttműködés

¹ *La diplomatie française à l'ère numérique*. Consulat Général de France à Ekaterinbourg. 2019. május 29.

² *Défense et sécurité des systèmes d'information: Stratégie de la France*. 2011.

Szervezetével (a továbbiakban: NATO) és az Európai Unióval (a továbbiakban: EU), párbeszédet Kínával és Oroszországgal, valamint támogatja a nemzetközi bizalomépítő intézkedések elfogadását.³ A 2013-ban kiadott Fehér Könyv kiemeli, hogy a kibertámadások kivédése érdekében „globális kormányzati megközelítést” kell alkalmazni, és ennek részeként Franciaország diplomáciai, jogi és politikai eszközeire épít.⁴

Az ország kiberstratégiáját 2015-ben adták ki, *A digitális biztonság nemzeti stratégiája* címmel.⁵ A stratégia öt fő célkitűzést rögzít, amelyek közül az ötödik az *Európa, digitális stratégiai autonómia, a kibertér stabilitása* címet viseli. Franciaország Európa digitális transzformációjában szövetségesi kapcsolatain keresztül kíván részt venni, három főbb módon: az európai stratégia megalkotására vonatkozó menetrend megfogalmazásával közösen más uniós, önkéntesen részt vevő államok, a nemzetközi kibermegbeszéléseken való francia jelenlét és befolyás erősítésével, valamint a kiberkapacitások építésében más államok támogatásával, hozzájárulva ezzel a kibertér globális stabilitásához. A stratégia értelmében a befolyásnövelés fő színterei a nemzetközi szervezetek közül az Egyesült Nemzetek Szervezete (a továbbiakban: ENSZ) és az Európai Biztonsági és Együttműködési Szervezet (a továbbiakban: EBESZ), a bilaterális kapcsolatok miniszteri szintű diplomáciai párbeszéd keretében, valamint a politikai döntéshozók és a tudományos élet szereplői részvételével megrendezett informális nemzetközi fórumokon való aktív jelenlét. A stratégiában foglaltak végrehajtására centralizálták a kiberdiplomácia területét, és 2015-ben a Külügyminisztériumban felállították a kiberdiplomácia és digitális gazdaság nagyköveti pozícióját.⁶

A 2015-ös stratégia elfogadása óta a nemzetközi környezet jelentősen megváltozott. Elég, ha a Charlie Hebdo elleni terrortámadást követő vagy a TV5 televíziócsatorna elleni kibertámadás-sorozatokra gondolunk. Az események új megvilágításba helyezték a kiberbiztonság kérdéskörét Franciaországban is, és az országot aktívabb és erőteljesebb nemzeti és nemzetközi fellépésre sarkallták.

³ *Rapport d'Information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (I) sur la cyberdéfense.* Par le Sénateur M. Jean-Marie Bockel. Sénat Session extraordinaire de 2011–2012. Enregistré à la Présidence du Sénat le 18 juillet 2012.

⁴ *Livre Blanc. Défense et sécurité nationale.* Paris, 2013.

⁵ *La stratégie nationale pour la sécurité de la numérique* (2015).

⁶ A tisztséget, amelyet 2017. november 22-e óta digitális nagykövetnek neveznek, David Martinon töltötte be.

Az új megközelítést tükrözi a *Támadó kiberműveletek doktrínája*, amelyet 2018. január 18-án publikáltak, mintegy három héttel megelőzve a *Kibervédelmi stratégiai áttekintés* kiadását. A dokumentumban Franciaország nyíltan ír arról, hogy katonai tevékenységének részét képezik a kiberkapacitások, amelyeket szükség esetén kész bevetni. Ez mindenképpen fordulópontot jelez a francia kiberpolitikában, amelyet ez idáig a diszkrét diplomáciai lépések megtétele jellemzett: még olyan nyilvánvaló kiberkonfliktusok esetén, mint az oroszok által szponzorált, a haditengerészet olajutánpótlási csatornáinak kiderítését célzó kibertámadás kapcsán sem lépett fel Franciaország támadó retorikával, hanem a párbeszéd eszközhöz nyúlva igyekezett a feszültséget csillapítani.⁷

2018. február 8-án *Kibervédelmi stratégiai áttekintés* címmel adták ki a legújabb kiberdokumentumot, az ország kibervédelmi ambícióit összefoglaló hivatalos anyagot.⁸ A kibervédelem fehér könyvének is nevezett dokumentum több fejezetben is kitér az egyes kiberdiplomáciai lépések szükségességére, és rögzíti Franciaország adott kérdéssel kapcsolatos álláspontját. Önálló fejezet szól a kibertér szabályozásáról szóló nemzetközi tárgyalásokról, kiemelve az ENSZ és a Kormányzati Szakértők Csoport (Group of Governmental Experts, a továbbiakban: GGE) szerepét és elért eredményeit 2013-tól kezdődően. Franciaország a 2016–2017-es ülésszakon önálló javaslattal állt elő a visszatámadás tilalmának mélyebb szabályozását illetően, és ezt a javaslatot bár támogatták a részt vevő államok, de a tárgyalások megakadtak a nemzetközi jog alkalmazásának módjával kapcsolatos eltérő nézetek miatt. Egy másik fejezet azt mutatja be, hogy az ország hogyan lép fel nemzetközi szinten a kibertérben. A kiberkonfliktusok megelőzése érdekében támogatja a párbeszédet és az együttműködést a szövetségeseivel, a kibertér szabályozását sürgeti, és célja, hogy az európai biztonság és autonómia a kibertérben is biztosítva legyen. A bilaterális kapcsolatai közül kiemeli az Egyesült Államokkal,⁹ Kínával, Indiával,¹⁰ Brazíliával és Japánnal

⁷ Arthur P. B. Laudrain: *France's New Offensive Cyber Doctrine*. 2019. február 26.

⁸ *La Revue Stratégique de Cyberdéfense*. SGDSN, 2018. február 12.

⁹ A francia–amerikai kiberdialógus harmadik állomását 2020. január 22-én, Párizsban rendezték meg. A találkozó központi témája a nemzetközi jog kibertérre történő alkalmazhatósága volt. Lásd *Troisième dialogue stratégique France-États-Unis en matière de cybersécurité (Paris, 22 janvier 2020)*.

¹⁰ Az indiai–francia bilaterális kiberdialógust 2019. június 20-án harmadik alkalommal rendezték meg, megvitatta elősorban a kibernormákkal kapcsolatos kérdéseket. Jól jelzi a kétoldalú kiberkapcsolatok fontosságát, hogy India meghívást kapott a 2019-es G7-csúcsra az elnöki tiszet 2019-ben betöltő Franciaországtól. Lásd *Indo-French Bilateral Cyber Dialogue (Paris, 20 June 2019)*.

fennálló kiberkapcsolatait, hozzátéve, hogy a nyugati szövetségeseivel továbbra is mély kapcsolatokat fog ápolni, de egyre nagyobb hangsúlyt helyez a szub-szaharai térségre, ahol kapcsolatok kiépítését sürgeti a frankofón államokkal. Az európai kiberkapcsolatokat három kérdéskör mentén kell rendezni: a technikai, a szabályozási és a kapacitási kérdésekben szükséges a közös alapok megfogalmazása és azok elfogadása. Mind a bilaterális, mind az európai kapcsolatok szempontjából kiemelt helyet foglal el a francia–német kapcsolatrendszer. A két ország közötti együttműködés igen intenzív és kiterjedt, ezt az eddig kiadott két közös jelentés is alátámasztja.¹¹ Végezetül pedig a dokumentumban foglaltak értelmében szükséges egy cselekvési doktrína elfogadása, amely olyan alapvető kérdéseket rögzít, mint a kibertámadások osztályozásának rendszere és a kibercidensekre adandó válaszlehetőségek köre. A kibertér szabályozásának globális rendszerét csak olyan alapelvek mentén lehet megvalósítani, mint a megelőzés, az együttműködés és a stabilitás.

A „támadóbb” szellemű hozzáállás ellenére a francia politikában minden bizonnyal a jövőben is meghatározó szerepet fognak játszani a diplomáciai lépések. Nem véletlen, hogy a különböző nemzetközi szervezetekben Franciaország az egyik legaktívabb tagállam, amikor kiberbiztonsággal kapcsolatos kérdések merülnek fel. Nemcsak az ENSZ-ben – ahogyan a GGE kapcsán arról már szó esett –, hanem a NATO-ban, a G7-ben és az EBESZ-ben is.¹² Ez utóbbi szervezetnél Franciaország igen jelentős szerepet játszott a kiberbiztonsággal kapcsolatos bizalomerősítő intézkedés két csomagjának elfogadásában. A G7-ben való francia részvétellel kapcsolatban kiemelem a 2019. április 5–6-án Dinard francia kisvárosban megrendezett találkozót, ahol elfogadták az úgynevezett Dinard-deklarációt a kiberszabályok kezdeményezéséről.¹³ Ebben üdvözölték az ENSZ közgyűlésének támogató hozzáállását a nemzetközi jog kibertérben alkalmazhatóságáról, és megerősítették szándékukat egy nyitott, biztonságos, stabil, hozzáférhető és békés kibertér támogatása iránt. Együttal megerősítették szándékukat a kiberszabályozási kezdeményezés (Cyber Norm Initiative – CNI) megfogalmazására, amelyet 2019. augusztus 26-án öntöttek formába tíz, a kiber-

¹¹ *ANSSI/BSI Common situational picture*. 1. – 2018. július. *Second Edition of the Franco-German Common Situational Picture*. 2019. május 21.

¹² *La France et la cybersécurité*.

¹³ *Dinard Declaration on the Cyber Norm Initiative*. 2019. április 6.

térben alkalmazandó alapvető szabály megalkotásával.¹⁴ Mindez jól illeszkedik a francia soft politika sikertörténetébe, bár hozzá kell tenni, hogy nem volt előzmények nélküli egy ilyen kezdeményezés elfogadása. 2018. november 12. és 14. között ugyanis az UNESCO párizsi székháza adott otthont az Internetkormányzási Fórum (Internet Governance Forum) tizenharmadik éves ülésének, ahol Emmanuel Macron francia elnök maga jelentette be a *Párizsi felhívást* a bizalom és biztonság kibertérben való megteremtésére.¹⁵ A felhívásban foglaltak széles körű elfogadását jól jelzi, hogy azt azonnal több mint 500 entitás (állam, szervezet és vállalat) támogatta.¹⁶ A kép teljességéhez azonban az is hozzátartozik, hogy a három „nagy” kiberállam mindegyike visszautasította a kezdeményezést, megtorpedózva ezzel annak globális elfogadhatóságát. A felhívással és számos hasonló kezdeményezéssel Franciaország célja, hogy kibernagyhatalomként tartsák számon világsgazte. Talán ez a cél vezérelte az országot 2019. szeptember 9-én is, amikor a francia Védelmi Minisztérium hivatalos dokumentumban rögzítette véleményét arról, hogy a nemzetközi jog Franciaország szerint miként alkalmazható a kibertérben¹⁷ – ezzel is úttörő kiberdiplomáciai szerepet vállalva.

Németország

Bár Németország 2004-től aktívan részt vett az ENSZ kiberbiztonsági tanácskozásain és más két- és többoldalú fórumokon, az együttműködés technikai kérdésekre korlátozódott. Az első, 2011. évi német kiberbiztonsági stratégia megemlítette ugyan a kiberbiztonság nemzetközi és diplomáciai dimenzióit, egészen a Snowden-ügyig azonban Németország nem játszott különösebb szerepet a kiberpöröndön. Csak ezt követően kezdeményezte Angela Merkel német kancellár érintettsége okán Németország – Brazíliával karöltve – az ENSZ-ben a magánélethez való jog védelméről és sérthetetlenségéről szóló határozat elfogadását a digitális kor vonatkozásában, amelynek eredményeképp 2013. december 18-án megszületett a 68/167. sz. közgyűlési határozat. Ez Németország jelentős

¹⁴ *Initiative pour des normes dans le cyberspace. Synthèse des enseignements tirés et des bonnes pratiques.* 2019. augusztus 26.

¹⁵ *Appel de Paris pour la confiance et la sécurité dans le cyberspace.* 2018. november 12.

¹⁶ *Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans la cyberspace.* Liste des soutiens à l'appel de Paris (actualisé le 14 novembre 2018.).

¹⁷ Przemyslaw Rogusky: *France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I.* 2019. szeptember 24.

kiberdiplomáciai sikere volt, különösen úgy, hogy a dél-amerikai támogatással globális szintre sikerült emelnie e kérdéskört. Innentől kezdve Németország a kiberdiplomácia aktív támogatójává vált. 2016-ban az EBESZ német elnöksége alatt fogadták el a kibertérbeli bizalomerősítő intézkedések második csomagját, majd 2016–2017-ben Németország diplomáciai képviselői elnököltek a UN GGE-n is.

Az egyre aktívabb német fellépés alapjai az ország kiberbiztonsági stratégiájában keresendők, 2016-ban adták ki az ország második kiberstratégiáját.¹⁸ A dokumentum már kiemelten kezeli az együttműködés fontosságát, amely azonban nem korlátozódhat nemzeti keretek közé, hanem összeurópai, sőt világszintű együttműködési csatornákat kell kialakítani. A stratégia négy cselekvési területet nevesít, amelyek közül az egyik Németország megfelelő pozicionálása az európai és a nemzetközi kiberbiztonsági politikai megbeszéléseken. Ez egyértelműen mutatja, hogy a kiberdiplomácia kiemelt területté nőtte ki magát, és az ország biztonságát befolyásoló alapvető tényezővé vált. Ennek részeként Németország hangsúlyozza a kétoldalú partneri kapcsolatok fontosságát is, főként olyan területeken, mint az információmegosztás és a határon átnyúló szolgáltatásokkal kapcsolatos biztonsági kérdések összehangolása, valamint a kapacitások megosztása, másrészt a fejlesztési együttműködés terén, ahol elsősorban a biztonság- és bizalomerősítő intézkedések segítségével érhetők el sikerek.

Németország a stratégiában foglaltakat a gyakorlatba is fokozatosan átülteti, ahol fokozott szerepet szán a kétoldalú kapcsolatoknak. Kiemelt stratégiai partnere az Egyesült Államok, ezért nem véletlen, hogy a kiberpárbeszédük is hosszú és tartalmas múltra tekint vissza. 2012 óta évente megrendezik a kétoldalú kibertalálkozót, hol Washingtonban, hol Berlinben. A találkozások alkalmával olyan kérdéseket vitatnak meg, mint 2016-ban például a nemzetközi jog kibertérben való alkalmazhatóságának kérdése vagy az emberi jogok online érvényesülése, de jól kirajzolódik közös gondolkodásmódjuk a kibertér többszereplős (*multi-stakeholder*) kormányzati modelljében is.¹⁹

Kínával 2016 novemberében született meg egyezés arról, hogy a két állam a kiberkérdések vonatkozásában egy speciális mechanizmus segítségével folytatja a párbeszédet, de kétoldalú szerződés aláírására a mai napig nem került sor.²⁰ Legutóbb 2020 januárjában folytatott Merkel kancellár tárgyalásokat Kíná-

¹⁸ *Cyber Security Strategy for Germany 2016*. Federal Ministry of the Interior, 2016.

¹⁹ *Joint Statement on U.S.-Germany Cyber Bilateral Meeting*. 2016. március 24.

²⁰ Christopher Burgess: *Dissectiong China's Global Bilateral Cybersecurity Strategy*. 2016. október 9.

ban egy, az amerikai–kínai egyezményhez hasonló német–kínai kiberegyezmény megalkotásáról, annak előfeltétele azonban a *no spy* klauzula beiktatása az amerikai Huawei-botránynak köszönhetően. Amikor azonban a kancellárt az egyezményről kérdezték, ő diplomatikusan mindössze annyit mondott, hogy Németország és Kína több szinten is folyamatosan tárgyal egymással számos kétoldalú és nemzetközi kérdéstről.²¹

A német bilaterális paletta ugyanakkor nem szűkül le a nagy partnerállamokra, hanem rendkívül színes képet mutat. Németország például jó kétoldalú kiberkapcsolatokat ápol Szingapúrral. A szingapúri miniszterelnök 2017-ben látogatást tett Németországban, amely alkalommal a két fél közös szándéknyilatkozatot írt alá a kiberbiztonsági együttműködésről olyan területeken, mint az információmegosztás vagy a közös kutatások. A látogatást 2018 júniusában Merkel kancellár viszonzta, s ennek keretében a két ország vezetője védelmi szerződést is kötött, külön kiberklauzulával.²²

Németország számos nemzetközi intézményben aktívan lép fel a kiberbiztonsági kérdések tárgyalásakor, de talán mindezen fellépések közül kiemelkedik az EBESZ-ben játszott szerepe. Predesztinálva is volt arra, hogy élére álljon az EBESZ-beli kezdeményezéseknek. Egyrészt azért, mert történelmileg politikai és gazdasági szálak kötik mind a Kelethez, mind a Nyugathoz, az EBESZ pedig összeköti e térségek vezető hatalmait is. Másrészt azért, mert Németország vezető állam e területen – elég, ha az adatvédelem területén felállított technikai sztenderdekre és szabályozásra gondolunk. Harmadrészt pedig azért, mert Németország hatékonyan vesz részt olyan, a kibertérbeli normák és szabályok megalkotásával foglalkozó szervezetekben, mint a GGE, ráadásul az itt szerzett tapasztalatait kamatoztatni is tudja.²³

Az EBESZ 2013-ban megalkotta a kibertérbeli bizalomerősítő intézkedések első csomagját, amely megfelelő alapul szolgált a továbblépéshez. A 2016-os német EBESZ-elnökség alatt mindhárom kosárban külön tárgyalták a bizalom- és biztonságerősítő intézkedések lehetséges körét. Az első kosár vonatkozásában 2013-ban még csak önkéntes megállapodások sorát rögzítették a tagállamok

²¹ Guy Chazan: *German Cyber Security Chief Backs 5G ‘No Spy’ Deal over Huawei*. *Financial Times*, 2020. február 28.

²² Prashanth Parameswaran: *Singapore-Germany Cyber Cooperation in Focus with Introductory Visit*. 2018. augusztus 14.

²³ *Three Priorities for Cyber Diplomacy under the German OSCE Chairmanship 2016*. Berlin, German Institute for International and Security Affairs. 2015. november 11.

közötti katonai együttműködésről. Megegyezés született, hogy az EBESZ-t platformként használják a kibertámadásokról szóló információcserére és a nemzeti kapacitások kiterjesztésének kölcsönös támogatására. A német elnökség kifejezett célja volt, hogy a mérnököket (elsősorban az informatikusokat) is bevonják a kiberdiplomáciába (nem csak az első kosarat érintően), amelytől olyan, a diplomáciai feszültségeket csökkentő hatást várnak, mint az 1950-es évek óta megrendezett Pugwash-konferenciák²⁴ fejleményei. A második, gazdasági kosárba tartozó lépésekhez referenciapontként szolgált a 2015-ben elfogadott német információbiztonsági törvény, amely a kritikus infrastruktúra védelmével kapcsolatban magasabb biztonsági követelményeket írt elő. A német törvényben foglaltak hivatkozási alapul szolgáltak a NIS-irányelv megalkotásakor is. A központi német kiberszerv, a Szövetségi Információbiztonsági Hivatal (BSI)²⁵ pedig számos EBESZ-partner számára a műszaki szakértelem modelljeként szolgált. Mindezek a fejlemények új horizontot nyitnak az EBESZ gazdasági együttműködés kontextusában. A harmadik kosár esetében az emberi jogok, azon belül is az interneten megvalósuló szólásszabadság kérdése a problematikus. A német elnökségnek mindenekelőtt a cenzúrával, a hálózati megfigyeléssel és a szerzői jogi kérdésekkel kapcsolatos dilemmára kellett választ találnia.

Németország kiemelt külpolitikai prioritásként kezeli a kibertér szabályozásának kérdéseit. Határozottan kiáll amellett, hogy a globális kérdéseket csak közös szabályozás mentén lehet megoldani – s e körbe tartozik a kiberbiztonság kérdése is. A probléma nem kezelhető csak nemzeti szinten, szükséges az államok, nemzetközi szervezetek, civil szervezetek és a tudományos szféra közti szoros együttműködés. Deklarálja a nemzetközi jog kibertérben való alkalmazhatóságát és alkalmazandóságát, valamint támogatja a multilaterális megközelítést.²⁶ Mindenképp diplomáciai sikernek tekintendő, hogy 2019 novemberében Németország adhatott otthont az ENSZ Internetkormányzás Fórumának.

²⁴ A béke és a leszerelés kérdéseivel foglalkozó, évente megrendezett konferenciák, amelyeken a nemzetközi tudományos élet jeles képviselői vesznek részt 1957 óta.

²⁵ Bundesamt für Sicherheit in der Informationstechnik – Federal Office for Information Security (BSI).

²⁶ *Cyber Policy: Multilateral Solutions for the Future*. Federal Foreign Office, 2019. szeptember 25.

A vezető (európai) kiberhatalom: az Egyesült Királyság

Az Egyesült Királyság – hasonlóan a nagyhatalmakhoz – idejekorán felismerte a kiberbiztonság és a kiberdiplomácia fontosságát, amelyet a stratégiai dokumentumaiban is megjelenít, és a gyakorlatban is sikeresen alkalmaz. Az első kiberbiztonsági stratégiát még 2009-ben adták ki, azt azonban hamar, 2011-ben felváltotta egy új stratégia, amely öt éves távlatban vázolta fel a fő irányvonalakat, célkitűzéseket és a megvalósításhoz szükséges feltételrendszert. A stratégia címe: *Megvédeni és segíteni az Egyesült Királyságot egy digitális világban (Protecting and Promoting the UK in a Digital World)*.²⁷ A dokumentum négy célkitűzést fogalmaz meg, amelyek közül a második célkitűzés kapcsán van szerepe a kiberdiplomáciának. Az ország megfogalmazott célja, hogy rugalmasan tudjon reagálni a kibertérbeli fenyegetésekre és támadásokra, valamint hatékonyabban tudja érdekeit megvédeni és érvényesíteni a kibertérben. Ez proaktív magatartást és aktív részvételt feltételez a kibertér alakításának folyamatában, amelynek elsődleges eszközei mind békés eszközök: részben diplomáciai, részben pedig gazdasági jellegűek, ugyanis a brit kormány igen nagy súllyal csatornázza be a brit vállalatok kereskedelmi érdekeinek támogatását az egyre növekvő nemzetközi kiberbiztonsági piacra. Érdemi előrelépést jelent a harmadik kiberstratégia,²⁸ amelyet a brit kormány 2016. november 1-jén adott ki, ismét deklarálta öt évre. A dokumentum három stratégiai célt fogalmaz meg, ezért nevezhetjük a 2016-os kiberstratégiát a „3D stratégiájának” is: megvédeni (*defend*), elrettenteni (*deter*), fejleszteni (*develop*), amelyek megvalósulásához elengedhetetlennek tartja a nemzetközi fellépést. A célkitűzések közül a második kapcsán kiemelt szerep jut a kiberdiplomáciának. Az elrettentést ugyanis nemcsak *hard* eszközökkel képzelik el (mint a támadó kiberképességek fejlesztése), hanem az együttműködési csatornák további szélesítésével és mélyítésével is – ahogyan a stratégia fogalmaz: a britek tovább folytatják a már megkezdett globális kyberszövetség kiépítését, és továbbra is támogatják a nemzetközi jog kibertérben történő alkalmazását. A három stratégiai cél megvalósítása csak megfelelő nemzetközi keretek között képzelhető el. Az Egyesült Királyság továbbra is élharcosa a szabad, nyitott, békés és biztonságos kibertér megteremtésének,

²⁷ *The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World*. 2011. november.

²⁸ *National Cyber Security Strategy 2016–2021*. United Kingdom, HM Government, 2016. november 1.

ahol a nemzetközi jog alkalmazandó, és az alapvető emberi jogok érvényesítése biztosított online és offline egyaránt. Ebben az Egyesült Királyság számít nemcsak a hagyományos szövetségeseire, hanem új partnereire is, és igyekszik kihasználni az olyan multilaterális fórumok adta befolyásolási lehetőségeit, mint az ENSZ, a G20, az Európai Unió, a NATO, az EBESZ, az Európa Tanács vagy a Brit Nemzetközösség.²⁹

A globális kiberbiztonság kiépítése célkitűzésének megvalósításában kiemelt szerep jut a kétoldalú kiberkapcsolatoknak. A britek hagyományos szövetségesei közül kétségkívül az Egyesült Államok áll az első helyen, amellyel a „különleges kapcsolat” (*special relationship*) – vagy ahogyan az utóbbi időben hívják, „a legfontosabb kétoldalú kapcsolat” (*the most important bilateral partnership*) – keretében igen szoros kapcsolatokat ápol a szigetország a kiberkérdések vonatkozásában is már közel egy évtizede. Már 2011-ben rögzítették a magánszektor és az üzleti élet szereplői bevonásának, a kutatás-fejlesztés, valamint a joguralom alapintézményei kibertérben való alkalmazásának szükségességét.³⁰ 2015-ben Washingtonban Obama elnök és Cameron miniszterelnök egyeztetett az együttműködés részletkérdéseiről,³¹ amelyet végül 2016. szeptember 7-én intézményesített a két védelmi miniszter által aláírt kiberegyezmény.³²

Bár a szigetország még nem írt alá bilaterális egyezményt Kínával, azonban 2015. október 22-én a kínai elnök angliai látogatásán a két ország közös nyilatkozatot adott ki a globális, átfogó stratégiai partnerségük kiépítéséről, útjára indítva ezzel a bilaterális kapcsolat „aranykorát”.³³ Ennek részeként rögzítették, hogy egymás ellen nem folytatnak, illetve nem támogatnak a szellemi tulajdon, üzleti titkok vagy bizalmas üzleti információk jogosulatlan eltulajdonítására irányuló kiberakciókat, amelyek célja a versenylőnyhöz jutás.³⁴

Az Egyesült Államokkal fennálló speciális partneri viszony nyomán nem meglepő, hogy az Egyesült Királyság 2012-ben Japánnal is kétoldalú kiberkapcsolatokat létesített. A kétévenkénti találkozókat ötödik állomását Tokióban

²⁹ Molnár Dóra: *Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia*. *Hadmérnök*, 12. (2017), II. különszám „KÖFOP”. 136–148. 144.

³⁰ *US-UK Cyber Communiqué*. 2011. május 25.

³¹ *Fact Sheet: U.S.-United Kingdom Cybersecurity Cooperation*. The White House, Office of the Press Secretary. 2015. január 16.

³² *U.S. – U.K. Cyber Agreement Opens Doors for Both Nations*. DoD News, 2016. szeptember 18.

³³ A brit politika egyes elemeiről részletesebben lásd *The Making of UK Strategy towards China*. 2019. április 4.

³⁴ *UK-China Joint Statement 2015*. Foreign and Commonwealth Office, 2015. október 22.

tartották 2020. január 31-én.³⁵ A megbeszélés alkalmával a kapacitásépítés és a nemzetközi porondon történő együttműködés lehetőségeiről tárgyaltak. Ez összhangban van a 2018-ban megrendezett negyedik találkozó során meghatározott fő együttműködési területekkel, amelyek között szerepel még a szabályalapú nemzetközi kiberrendszer támogatása és az IoT eszközök biztonságos használatával kapcsolatos nemzeti megoldások megosztása is.³⁶

Az ázsiai bilaterális kapcsolatok közül végül Indiát emelem ki, amely a britek számára is hatalmas gazdasági potenciált rejt magában. Elég, ha arra gondolunk, hogy már ma is 600 millió internetfelhasználó és 650 millió mobilhasználó él az országban. Az indiai–brit biztonsági együttműködés egyik fontos aspektusát jelentik a kiberkérdések, és a 2012 óta folytatott indiai–brit kiberdialógus keretében olyan témák vannak napirenden, mint a kiberkockázatok csökkentése, a kiberbűnözés kezelése és az internetkormányzás globális, multilaterális, transzparens és demokratikus rendszerének kiépítése. 2018 áprilisában Londonban a két ország ötéves, 14 területre kiterjedő együttműködésről szóló keretmegállapodást írt alá. India ilyen széles körű kiberegyüttműködési megállapodást az Egyesült Királyságon kívül ez idáig csak az Egyesült Államokkal kötött.³⁷

Az Egyesült Királyság számos európai országgal is létesített már kétoldali kiberkapcsolatot. Közülük a lengyel–brit kiberegyüttműködési megállapodást emelem ki, nem elsősorban a benne foglaltak miatt (amely lényegi újdonsággal nem szolgál), hanem regionális jelentősége okán: a britek e kapcsolaton keresztül kívánják a kelet-európai és a nyugat-balkáni kiberkapacitás-építési programokat támogatni.³⁸

Végezetül az Egyesült Királysággal kapcsolatban nem szabad megfeledkezni a Brit Nemzetközösségről, amely már önmagában is régóta fennálló diplomáciai fórum a részt vevő államok számára, de az utóbbi években már önálló napirendi kérdésként szerepel a kiberbiztonság kérdésköre is. A részt vevő államok együttműködésüket 2018. április 20-án intézményesítették a kiberdeklaráció aláírásával.³⁹ A nyilatkozat rögzíti a kölcsönös segítségnyújtási kötelezettséget a kiberkapacitások építésében és a kibertérrel kapcsolatos egységes vízió

³⁵ *The 5th Japan–UK Bilateral Consultations on Cyberspace*. 2020. január 31.

³⁶ *The 4th Japan–UK Bilateral Consultations on Cyberspace*. Japan-UK Joint Press Release, 2018. március 16.

³⁷ Rahul Roy-Chaudhury: *India-UK Cybersecurity Cooperation: The Way Forward*. 2019. november 22.

³⁸ *UK–Poland Cyber Cooperation Commitment*. 2017. december 21.

³⁹ *Commonwealth Cyber Declaration*. 2018. április 20.

megfogalmazásának igényét, amelyet az Egyesült Királyság anyagilag is támogat, 15 millió fonttal hozzájárulva a rögzített célok megvalósításához.⁴⁰

Zárógondolatok

Az előző fejezetben már hivatkoztam az egyes államok kiberpotenciálját rangsoroló Globális Kiberbiztonsági Indexre. Az index alapján a világ vezető kiberhatalma az Egyesült Királyság, a harmadik helyen pedig Franciaország található. A harmadik vizsgált állam, Németország a 26. helyet szerezte meg.⁴¹ Igen érdekes ugyanakkor, hogy az ötödik vizsgált terület, az együttműködés vonatkozásában az angolok igen jó pontot értek el, míg a diplomáciai nagyhatalomnak számító Franciaország jelentős lemaradásban van. Az európai kiberbiztonság vizsgálata azonban nem ér véget a három nagy állam bemutatásával. Számos üdítő példa létezik arra, hogy kis országok milyen nagy sikereket tudnak elérni a kiberbiztonság területén. Az index ezt is visszatükrözi, ugyanis a 4. helyen Litvánia, az 5. helyen pedig Észtország áll az összesített világgrangsorban. Mindez természetesen nem véletlen: elég, ha arra gondolunk, hogy ezeket az államokat érte elsőként olyan horderejű kibertámadás a 2000-es évek vége felé, amely a kiberkérdéseket az államok biztonsági agendájának élvonalába emelte. Mindkét állam magasabb részpontszámot ért el az együttműködés területén, mint a három vezető nagy állam. Ez az eredmény jól jelzi, hogy a kis államok milyen nagy hangsúlyt helyeznek a kiberdiplomácia fontosságára, és a békés diplomáciai eszközök használatát előrébb valónak tartják a hard kapacitásoknál. Az európai térség pedig valamennyi részkérdés tekintetében magasan a világ előtt jár, így az együttműködés vonatkozásában is, amely talán alapul szolgálhat egy békés kibertér alapjainak lerakásához.

Felhasznált irodalom

Analysis: Untangling the Web of Multi-Level Cyber Diplomacy. 2018. Online: www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/may/analysis-untangling-the-web-of-multi-level-cyber-diplomacy/.

⁴⁰ *Analysis: Untangling the Web of Multi-Level Cyber Diplomacy.*

⁴¹ *Global Cybersecurity Index.* 2018.

- Európai kiberdiplomáciai helyzetkép – Franciaország, az Egyesült Királyság és Németország
ANSSI/BSI Common Situational Picture. 1. 2018. 1. –2018. július. www.ssi.gouv.fr/uploads/2018/07/bilateral-french-german-it-security-situation-report.pdf.
- Appel de Paris pour la confiance et la sécurité dans le cyberspace.* 2018. november 12. Online: www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf.
- Burgess, Christopher: *Dissectiong China's Global Bilateral Cybersecurity Strategy.* 2016. Online: <https://securityboulevard.com/2017/10/dissecting-chinas-global-bilateral-cybersecurity-strategy/>.
- Chazan, Guy: German Cyber Security Chief Backs 5G 'No Spy' Deal over Huawei. *Financial Times*, 2020. február 28. Online: www.ft.com/content/5a0fe826-3b34-11e9-b856-5404d3811663.
- Commonwealth Cyber Declaration.* 2018. április 20. Online: https://thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf.
- Cyber Policy: Multilateral Solutions for the Future.* Federal Foreign Office, 2019. szeptember 25. Online: www.auswaertiges-amt.de/en/aussenpolitik/themen/multilateralism-cyber/2250332.
- Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans la cyberspace.* Liste des soutiens à l'appel de Paris (actualisé le 14 novembre 2018). Online: www.diplomatie.gouv.fr/IMG/pdf/soutien_appel_paris_cle8e5e31.pdf.
- Cyber Security Strategy for Germany 2016.* Federal Ministry of the Interior. Online: www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.
- Défense et sécurité des systèmes d'information: Stratégie de la France.* 2011. Online: www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.
- Dinard Declaration on the Cyber Norm Initiative.* 2019. április 6. Online: www.diplomatie.gouv.fr/IMG/pdf/g7_dinard_declaration_on_cyber_initiative_cle4e553d.pdf.
- Fact Sheet: U.S. – United Kingdom Cybersecurity Cooperation.* The White House, Office of the Press Secretary. 2015. január 16. Online: <https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation>.
- Global Cybersecurity Index.* UN ITU, 2019. Online: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
- Initiative pour des normes dans le cyberspace. Synthèse des enseignements tirés et des bonnes pratiques.* 2019. augusztus 26. Online: www.diplomatie.gouv.fr/IMG/pdf/fr_synthesis_cyber_norm_initiative_cle025b33.pdf.
- Joint Statement on U.S.–Germany Cyber Bilateral Meeting.* 2016. március 24. Online: <https://2009-2017.state.gov/r/pa/prs/ps/2016/03/255082.htm>.

- La diplomatie française à l'ère numérique*. Consulat Général de France à Ekaterinbourg, 2019. május 29. Online: <https://ru.ambafrance.org/La-diplomatie-francaise-a-l-ere-numerique>.
- La France et la cybersécurité* (é. n.). Online: www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/.
- La Revue Stratégique de Cyberdéfense*. SGDSN, 2018. február 12. Online: www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.
- La stratégie nationale pour la sécurité de la numérique 2015*. Online: www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf.
- Laudrain, Arthur P. B.: *France's New Offensive Cyber Doctrine*. 2019. február 26. Online: www.lawfareblog.com/frances-new-offensive-cyber-doctrine.
- Livre Blanc. Défense et sécurité nationale 2013*. Online: www.defense.gouv.fr/content/download/206186/2286591/file/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf.
- Molnár Dóra: Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia. *Hadmérnök*, 12. (2017), II. különszám „KÖFOP”. 136–148. Online: http://hadmernok.hu/170kofop_09_molnar.pdf.
- National Cyber Security Strategy 2016–2021*. United Kingdom, HM Government, 2016. november 1. Online: www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
- Parameswaran, Prashanth: *Singapore–Germany Cyber Cooperation in Focus with Introductory Visit*. 2018. augusztus 14. Online: <https://thediplomat.com/2018/08/singapore-germany-cyber-cooperation-in-focus-with-introductory-visit/>.
- Rapport d'Information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (I) sur la cyberdéfense*. Par le Sénateur M. Jean-Marie Bockel. Sénat Session extraordinaire de 2011–2012. Enregistré à la Présidence du Sénat le 18 juillet 2012. Online: www.senat.fr/rap/r11-681/r11-6811.pdf.
- Rogusky, Przemyslaw: *France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I*. 2019. szeptember 24. Online: <http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/>.
- Roy-Chaudhury, Rahul: *India–UK Cybersecurity Cooperation: The Way Forward*. 2019. november 22. Online: www.iiss.org/blogs/analysis/2019/11/sasia-india-uk-cyber-security-cooperation.
- Second Edition of the Franco–German Common Situational Picture*. 2019. május 21. Online: www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/D-F-Reports/Common_Situational_Picture_2019.pdf?__blob=publicationFile&v=2.

Európai kiberdiplomáciai helyzetkép – Franciaország, az Egyesült Királyság és Németország

Troisième dialogue stratégique France-États-Unis en matière de cybersécurité (Paris, 22 janvier 2020). 2020. Online: www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/lutter-contre-la-criminalite-organisee/la-france-et-la-cybersecurite/actualites-et-evenements-lies-a-la-cybersecurite/article/troisieme-dialogue-strategique-france-etats-unis-en-matiere-de-cybersecurite-22.

The 4th Japan–UK Bilateral Consultations on Cyberspace. Japan–UK Joint Press Release, 2018. március 16. Online: www.mofa.go.jp/press/release/press4e_001960.html.

The 5th Japan–UK Bilateral Consultations on Cyberspace. 2020. január 31. Online: www.mofa.go.jp/press/release/press4e_002766.html.

The Making of UK Strategy towards China. 2019. április 4. Online: <https://publications.parliament.uk/pa/cm201719/cmselect/cmfaif/612/61210.htm>.

The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World. 2011. november. Online: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

Three Priorities for Cyber Diplomacy under the German OSCE Chairmanship 2016. Berlin, German Institute for International and Security Affairs, Berlin, 2015. november 11. Online: www.swp-berlin.org/en/point-of-view/three-priorities-for-cyber-diplomacy-under-the-german-osce-chairmanship-2016/.

UK–China Joint Statement 2015. Foreign and Commonwealth Office, 2015. október 22. Online: www.gov.uk/government/news/uk-china-joint-statement-2015.

UK–Poland Cyber Cooperation Commitment. 2017. december 21. Online: www.gov.uk/government/publications/uk-poland-cyber-co-operation-commitment-joint-statement/uk-poland-cyber-co-operation-commitment.

U.S.–U.K. Cyber Agreement Opens Doors for Both Nations. DoD News, 2016. szeptember 18. Online: www.defense.gov/Explore/News/Article/Article/937878/us-uk-cyber-agreement-opens-doors-for-both-nations/.

US–UK Cyber Communiqué. 2011. május 25. Online: www.gov.uk/government/publications/us-uk-cyber-communique és https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62647/CyberCommunique-Final.pdf.