dr. Dornfeld László – Keleti Arthur – Barsy Miklós – Kilin Józsefné – Berki Gábor – dr. Pintér István

Műhelymunkák

A virtuális tér geopolitikája

Tanulmánykötet

2016/1. szám

Geopolitikai Tanács Közhasznú Alapítvány – Budapest, 2016
w w w . c g e o p o l . h u

Szerkesztette: Pintér István

A kötetben publikált tanulmányok
a szerzők önálló véleményét tartalmazzák,
így az abban foglaltak nem tekinthetők
a Geopolitikai Tanács hivatalos álláspontjának.

Idézés: Szerző neve (2016) A cikk címe. In: PINTÉR, István: A virtuális tér geopolitikája. Geopolitikai Tanács Műhelytanulmányok, 2016/1. p. oldalszám.HU ISSN 1788-7895. ISBN 978-963-9816-34-3.

Citation: Name of the author (2016) Name of the article. In: PINTER, Istvan: Geopolitics of the Virtual Space. Council on Geopolitics Working Papers, 2016/1. pp.
HU ISSN 1788-7895. ISBN 978-963-9816-34-3.

Tartalom

DR. DORNFELD LÁSZLÓ*

(dlaci120@gmail.com)

A kibertér főbb nemzetközi és nemzeti szabályozásai

Lektorálta: ERDŐS ANDRÉ

* A szerző a Miskolci Egyetem Állam és Jogtudományi Karának I. évfolyamos doktorandusza, témavezetője Dr. habil. Róth Erika egyetemi docens

Absztrakt

A kibetérben található fenyegetések elleni fellépés mind állami, mind nemzetközi szinten egyre erősödik. Az egyes szereplők egyre szervezettebb formában igyekeznek fellépni a bűnözők ellen, gyakran egymást segítve. Az eredményes együttműködést nehezíti azonban az, hogy az érintett felek eltérő szabályozási rendszerek megvalósulásában érdekeltek, amely kibertérrel kapcsolatos politikájuk fontos részét képezi. A két fő modell az Egyesült Államok és az Európai Unió által támogatott több érdekelt fél bevonásával történő, és a Kína és Oroszország által pártolt nemzeti szuverenitáson alapuló multilaterális szabályozás. A tanulmány célja, hogy feltárja az ezek között húzódó különbségek okait és a szabályozások fontosabb fejlődési irányait.

Kulcsszavak: kibertér: kiberbűnözés, szabályozás

Abstract

The willingness of countering threats that are present in cyberspace is growing both on national and on international levels. The actors are trying to step up more organically against the involved criminals, often cooperating with each other. However there is an obstacle in the way of successful international cooperation – the actors are interested in implementing different types of legal regimes which is an integral part of their individual policies. The two main models are the multi-stakeholder approach supported by the US and the EU and the regime based on national sovereignty promoted by China and Russia. The main goal of this study is to unfold what are the causes of this difference and to give a review over the most important tendencies of the evolution of the legal regimes.

Keywords: cyberspace, cybercrime, regulation

Bevezetés

Mikor az internet még csak a hadsereg számára elérhető technológiaként létezett, nem volt szükség szabályozás kidolgozására a területen. A jogellenes használatuktól való félelem még akkor is igen jelentéktelen volt, amikor a hálózatok többségét nagy cégek működtették. Azonban ahogy a civil szektor és a lakosság számára is széles körben hozzáférhetővé vált a technológia, a helyzet gyökeresen megváltozott. Az e-kereskedelemben új szabályozás vált szükségessé, az államok működését pedig az e-közigazgatás kiépítése tette gördülékenyebbé. A felhasználók számának növekedésével a kiberbűnözés jelentette fenyegetés is jelentősen megnőtt. Hamarosan a hadseregekben is felismerték, hogy az internet segítségével emberveszteség nélkül okozhatnak súlyos károkat az ellenségnek, és ennek elérésére hamarosan az egyszerű polgárok is képessé váltak, mint mutatja azt például az Észtország internetes infrastruktúrája elleni oroszpárti hackertámadás 2007 áprilisában. (Jensen, 2015, p. 276.)

A kibertér információbiztonságát érő összes jelentősebb eddigi fenyegetés nemzetközi vonatkozásokkal rendelkezett. Az államok egyre inkább felismerték, hogy egyedül nem képesek gátat szabni ennek az új jelenségnek. Éppen ezért – bírjanak bármilyen felfogással is a kiberteret illetően – a nemzetközi együttműködés szükségessége vitathatatlanná vált. (Zhang, 2013, p. 123.) Ebből a körülményből következik, hogy a kibertérrel kapcsolatos szabályozási modellek nemzetközi érvényesítésére az államok egyre nagyobb hangsúlyt helyeznek. A jelentősebb szereplők nemzeti szinten az Egyesült Államok, Kína és Oroszország, míg szupranacionális és nemzetközi szinten az Európai Unió és az ENSZ.

A jelenlegi szabályozásban fontos szerep jut még az iparban érdekelt nagy multinacionális cégeknek (pl. Google, Apple, Microsoft), amelyek saját szabályaik szerint járnak el számos kérdésben, így például egyes – akár politikai – tartalmak eltávolításáról saját belátásuk szerint döntenek. Sokan kritizálták a Facebookot, amikor idén májusban egy volt alkalmazottjuk a sajtónak arról nyilatkozott, hogy a népszerű hírek kiválasztásánál a szerkesztőcsapat tudatosan mellőzte a konzervatív honlapokat. (Lakner, 2016) Ez jól mutatja, hogy a nagy cégek milyen jelentős befolyással lehetnek a szolgáltatásaikat használók véleményének formálására. Mivel az alapvető jogok – így a szólásszabadság

is – csak az állam és az egyén kapcsolatában értelmezhetők, az államihoz hasonló jogosultságokat gyakorló cégek korlátozás nélkül dönthetnek tartalmak sorsáról.

Az egyes szabályozási modellek számos kisebb-nagyobb jelentőségű kérdésben eltérnek egymástól, mint például a szolgáltatók szerepe és bevonása, a jogsértő tartalom kiszűrésének a módszerei, az interneten folyó kommunikáció ellenőrzése stb. Ezek mindegyikét lehetetlen lenne ennek a tanulmánynak a keretei között tárgyalni, ezért a főbb irányvonalakra és kérdésekre fogok a következőkben koncentrálni. Célom, hogy bemutassam a világon található jelentősebb szabályozási megoldásokat, és ezek fejlődési tendenciáit.

1. Egyesült Nemzetek Szervezete

Az ENSZ kiberteret érintő szabályozásának kidolgozásával a Közgyűlés több határozatban is foglalkozott. Az 1998-ban Oroszország javaslatára elfogadott 53/70. sz. közgyűlési határozat a kiberteret érő új fenyegetésekkel kapcsolatban fogalmazott meg ajánlást a tagállamok számára. 2006-ban a 60/45. sz. határozat a főtitkár számára egy nemzetközi, kormányzati szakértőből álló csapat összehívását írta elő, amelynek feladata volt jelentést készíteni az információbiztonságot fenyegető létező és potenciális veszélyekről. A jelentés 2010-re készült el. Fontos szerepet tölt be a szabályozásban a Nemzetközi Távközlési Egyesület (ITU), amelynek 191 tagállama és 700-nál is több ágazati tagja van (köztük például az Európai Bizottság), működési területét pedig gyors ütemben terjeszti ki az internetre is. (Sofaer – Clark – Diffie, 2010, pp. 187–188.) 1988-ban Melbourne-ben a Távíró- és Telefonszolgáltatók Világkonferenciáján (WATTC-88) fogadták el a nemzetközi távközlési szabályozást (International Telecommunication Regulations, ITR), amely azóta sem változott. A szabályozás célja a határokon átnyúló telekommunikációs forgalmat biztosító rendszerek együttműködő képességének (interoperabilitás) és összekapcsolódásának megkönnyítése. Többek között olyan kérdéseket érint, mint a díjazás és számvitel, felelősség vagy adóztatás. Ugyanakkor olyan időszakban született, amikor az internetszolgáltatók jelentős része állami tulajdonban volt, és mára

időszerűvé vált felváltása és szabályainak az új kihívásokhoz való igazítása. (Internet Society, 2011)

2003-ban és 2005-ben Genfben és Tuniszban a szervezet megtartotta az Információs Társadalom Világcsúcsát (World Summit on the Information Society, WSIS), amelyen a tagállamok amellett foglaltak állást, hogy a szervezet legyen a fellépés vezetője az új információs és kommunikációs technológiák biztonsága, és az ezek iránti bizalom kiépítésében. Számos egyeztetést követően ezen cél elérése érdekében 2007. május 17-én létrehozták a Globális Kiberbiztonsági Menetrendet (*Global Cybersecurity Agenda*, GCA), amelynek célja, hogy keretet biztosítson a kiberteret fenyegető növekvő fenyegetés elleni nemzetközi fellépés koordinálásához. A GCA fontosnak tartja, hogy minden érdekelt fél egyesített erőfeszítése révén valósuljanak meg célkitűzései. (Sofaer – Clark – Diffie, 2010, p. 186–187.) Az Egyesült Államok Kormányzati Ellenőrzési Hivatalának 2010. júliusi jelentése rámutat, hogy egyetlen központi szereppel bíró szerv híján a kiberbiztonságban résztvevő nemzetközi szervezetek nagy száma akadályozhatja a nemzetközi koordinációt. A jelentés rámutat, hogy a hálózatbiztonsági vészhelyzeteket elhárító csoportokkal (*Computer Emergency Response Team*, CERT) való állami együttműködés számos nehézséggel bír, és a szervezetek egy része – mint például az ENSZ által létrehozott Globális Reagálóközpont (Global Response Center) – nem képes arra, hogy minden résztvevő előnyére szolgáló, legitimitással bíró globális biztonsági szolgáltatást nyújtson. (Sofaer – Clark – Diffie, 2010, p. 186.)

2011 szeptemberében Kína, Oroszország, Kazahsztán, Kirgizisztán, Tádzsikisztán és Üzbegisztán javaslatot terjesztettek az ENSZ Közgyűlés elé a kiberbiztonság megteremtése érdekében, amelyben hangsúlyos szerepet kapott a nemzeti szuverenitás részét képező kiberszuverenitás, vagyis a kormányok azon joga, hogy határaikon belül korlátok nélkül ellenőrizhessék az adatforgalmat. (Jong-chen, 2015) Ezen országok képviselői közös levélben kérték az ENSZ főtitkárát, hogy a sanghaji együttműködés részeként elfogadott nemzetközi magatartási kódexet a Közgyűlés 66. ülésszakán hivatalos dokumentumként terjessze a megjelentek között. (Zhang 2013, p. 126.) Változtatásokat követően Oroszország és Kína 2015 januárjában ismét benyújtotta a magatartási kódexet a főtitkárnak, ami jól mutatja, hogy nem tettek le annak nemzetközi elfogadtatásának szándékáról. (Grisby, 2015)

2012-ben a Dubajban tartott nemzetközi távközlési világkonferencián (WCIT) Oroszország, Kína, Brazília és India olyan javaslattal álltak elő, ami jóval nagyobb szerepet szánt volna az internet szabályozásában az ITU-nak. A kibertér szabályozásában a nemzeti szuverenitás elvét valló országok részéről ez azért különösen lényeges, hiszen így végső soron az államok jutnak szélesebb beleszólási lehetőséghez. (Eichensehr, 2015, p. 331.) Az Egyesült Államok élesen ellenezte a javaslatot, azon az alapon, hogy abban csak vertikális módú irányítás valósulna meg, és a többi érdekelt fél nem kerülne bevonásra. Mások azt emelték ki, hogy ezzel a világpolitikai érdekeknek rendelnék alá egy nagyon gyorsan fejlődő technikai terület szabályozását, amely megbénítaná a döntéseket. Megint mások a beterjesztő országokban működő, szabad információáramlást korlátozó internetszabályozás alapján fogalmaztak meg kritikát. (Sasso 2012; Rosenzweig 2012, p. 414.)

Oroszország javaslata az internetet egyértelműen az ITU szabályozása alá rendeli, és egyúttal a domainnevek kiosztását felügyelő ICANN nem kormányzati szervezet pozícióját is gyengíti. A javaslat ugyanis egyenlő jogokat biztosított volna ezen a területen a tagállamoknak. A világkonferencia eredménye felemás volt: egyrészt az Egyesült Államok és szövetségesei sikerrel akadályozták meg az ITU vagy az ENSZ domainnevek elosztásába történő bevonását, és a szerződésbe belefoglaltattak egy nyilatkozatot, amely szerint annak hatálya nem terjed ki a tartalomszabályozás kérdéseire. Másrészt azonban elfogadásra került az orosz javaslat módosított változata, és ezt a határozatot az egyezményhez csatolták. Eszerint „minden kormányzatnak egyenlő szerepet és felelősséget kell biztosítani a nemzetközi internetszabályozásban", ami igen távol áll a nyugati küldöttségek által szorgalmazott minden érdekelt bevonásával működő modelltől. Összesen nyolcvankilenc ország – köztük Oroszország, Kína, Dél-Afrika, számos afrikai és arab ország – írta alá az új egyezményt, míg az Egyesült Államok, az EU tagállamok, Kanada, Ausztrália, Új-Zéland és India nem. (Eichensehr, 2015, pp. 333–335.)

Az amerikai küldöttség vezetője, Terry Kramer nagykövet öt indokot nevezett meg az elutasítás okaként. Az első, hogy a javaslat a közreműködő ügynökség (*operating agencies*) helyett az elismert közreműködő ügynökség (*recognized operating agencies*) kifejezést használta. Az első megnevezés a hagyományos telekommunikációs közszolgáltatásokat nyújtókat jelöli, amely-

be nem tartoznak bele az internetszolgáltatók, a magán- és kormányzati hálózatok. Az amerikai vélekedés szerint amennyiben ezekre is kiterjed az egyezmény, úgy az internet állandó figyelés alá vehető. A második ok a spamek tilalma, amely az amerikai álláspont alapján a kifejezés egyik formája, ezért a véleményszabadság védelme alá tartozik. A harmadik ok a hálózatbiztonsági kérdések felvetése, amely a nagykövet szerint nem az ITR szabályozási körébe tartozó kérdés. Kifejtette továbbá, hogy egyetlen kormányzat vagy nemzetközi szervezet sem irányíthatja az internetet és dönthet annak fejlődési irányáról, így az ENSZ sem. Utolsóként azt említette, hogy bár az előzetes megbeszélések során Hamadoun Touré biztosította arról, hogy internettel kapcsolatos kérdések nem lesznek a megbeszélésen, ezek mégis előkerültek. Kramer szerint ugyan az amerikai küldöttség jóhiszeműen próbált hozzáállni ezekhez, a többi küldöttség által tett, oda nem illő javaslatok alaposan megváltoztatták a megbeszélés jellegét. (Popescu, 2012)

2014-ben a dél-koreai Puszanban tartott Meghatalmazotti Konferencián szintén több internettel kapcsolatos javaslat került benyújtásra. Például Oroszország javasolta, hogy az ITU kezdje meg az IP-címek kiosztását, amelyet jelenleg nem kormányközi szervezetek végeznek, az arab államok pedig a kormányok internetre vonatkozó döntési lehetőségét növelték volna. India javaslata a belföldi internetforgalmat az államhatárokon belül tartotta volna, így az azon túli címek eléréséhez külön csatlakozásra lett volna szükség. (Dickinson 2014) Az Egyesült Államok és partnerei azonban sikeresen megakadályozták ezek mindegyikének elfogadását, így a status quo fennmaradt.

Ebben az évben Zhao Houlin, egy kínai állampolgár lett az ITU új főtitkára, aki korábban hét évig a szervezet főtitkárhelyetteseként tevékenykedett. Az ő irányítása alatt jelentősen megváltozott a megbeszélések hangneme a szervezet 2015-ös világkonferenciáján, amely már korántsem olyan konfrontatív, mint 2012-ben volt. Ezzel sikeresen kivívta az amerikaiak dicséretét is. (Austin, 2016, p. 174)

2. Egyesült Államok

2.1. Az amerikai szabályozás

Az Egyesült Államok kétféle módon közelít a kiberbiztonság kérdéséhez: egyrészt nemzeti érdekei védelmében saját belső védelmét megerősítette új törvények elfogadásával és betartatásával, másrészt nem amerikai állampolgárok és más államok esetén jelentős lépéseket tesz az információk gyűjtésére. Ez utóbbi akkor derült ki, mikor Edward Snowden 2013-ban nyilvánosságra hozta az NSA működésével és feladatával kapcsolatos adatokat. (Zhang 2013, p. 121.) A biztonságpolitikai szakértők azt javasolják, hogy a nemzeti jogszabályok segítsék elő a támadásokról szóló információk megosztását, az állami szervek működjenek együtt a magánszektorral, valamit államilag támogatott kutatások segítségével építsenek ki gyors és effektív védelmet a kibertámadások ellen. Ugyanakkor ezek a módszerek hatástalanok olyan esetekben, amikor a támadók olyan külföldi országból származtak, amelyben az USA nem tudja a jogszabályait érvényre juttatni. (Sofaer – Clark – Diffie, 2010, p. 184.)

Az USA elsők között ismerte fel a kibertér fenyegetései elleni állami fellépés szükségességét. A későbbi számítógépes csalással és visszaéléssel foglalkozó törvény (*Computer Fraud and Abuse Act*, a továbbiakban CFAA) előkészítése már 1976-tól elkezdődött, és a Kongresszus 1984-ben fogadta el, ekkor még egy másik törvény részeként. Az elkövetkező két évtizedben nyolc alkalommal módosították a jogszabályt, amelyek fokozatosan kiterjesztették hatályát. Míg kezdetben csak a „szövetségi érdekeltségű" számítógépek elleni támadást büntették, a 2008-as módosítás eljutott oda, hogy a világ összes számítógépét a szabályozás alá vonja. (Dornfeld 2015, pp. 69–71.) Ezt számos egyéb szabályozás is követte, mint például az információszabadságról (*Freedom of Information Act*), a számítógépes biztonságról (*Computer Security Act*), a gyermekek online magánéletének védelméről (*Children's Online Privacy Protection Act*), a biztonságos közhálózatokról (*Secure Public Networks Act*), a titkosított kommunikációról (*Encrypted Communications Privacy Act*), a telefonos vásárlók védelméről (*Telephone Consumer Protection Act*) stb. szóló törvények. Ennek a jelentős méretű joganyagnak köszönhetően az Egyesült Államok szabályozása az egyik legrészletesebben kimunkált a világon.

A törvényeken kívül számos elnöki rendelet is született, egyes fontos kérdések szabályozásával kapcsolatban. 2011-et követően sok vita folyt az amerikai törvényhozásban a kritikus infrastruktúra védelmét illetően, amelyek azonban nem vezettek eredményre. Végül 2013. február 12-én Obama elnök, egy amerikai erőmű leállását eredményező kibertámadást követően kiadta a kritikus infrastruktúra kibervédelmének javításáról szóló 13636. számú elnöki rendeletet, amelyben a Nemzeti Szabványügyi és Technológiai Intézetet (*National Institute for Standards and Technology*, NIST) bízta meg a kritikus infrastruktúra többségét birtokló magánszektorral való együttműködés részleteinek kialakításával. (Wiley Rein, 2013; White House, 2013) 2015. április 1-jén született meg a 13694. számú elnöki rendelet, amely olyan természetes és jogi személyekkel szemben teszi lehetővé pénzügyi szankciók alkalmazását, akik súlyos nemzetbiztonsági kockázatot jelentő kibertevékenységekben vesznek részt, kereskedelmi titkokat szivárogtatnak ki vagy ezekben bármilyen segítséget nyújtanak. Feltétel, hogy ezen elkövetők teljesen vagy jelentősen az Egyesült Államok területén kívül működjenek. Bár a rendelet nem mondja ki, elsődlegesen a Kínából és Oroszországból érkező – amerikai feltételezések szerint államilag támogatott – támadásokra adott válaszlépésként értelmezhető, főleg, mivel ezeknek az államoknak nincs kiadatási egyezményük az USA-val.

Az internetsemlegesség – melynek általános kérdéseit az EU-val foglalkozó fejezetben részletezem – fontos szabályozási kérdésként merült fel, és Barack Obama választási programja részévé is tette az elképzelést. 2002-ben a Szövetségi Távközlési Bizottság (*Federal Communications Commission,* FCC) úgy döntött, hogy az internetszolgáltatók nem telekommunikációs szolgáltatást nyújtanak, így nem is vonatkoznak rájuk a telekommunikációs törvényben a közös szállítókkal kapcsolatban megfogalmazott kötelező szabályok. A 2005-ben kiadott internetes szabályozási nyilatkozatban négy internetszabadsági alapelv került meghatározásra. Ez a felhasználók jogait tartalmazza, így: a törvénybe nem ütköző tartalmakhoz való szabad hozzáférés, a választásuk szerinti alkalmazások futtatása, az eszközeik közötti összeköttetés, valamint a szolgáltatók közötti verseny. (Walthall, 2010, pp. 21–22.) Az ezt követő években az FCC kiállt az internetsemlegesség mellett. Miután 2007-ben kiderült, hogy a Comcast internetszolgáltató megakadályozza vagy jelentősen

lassítja a BitTorrent feltöltéseket, a szervezet 2009 októberében törvényalkotási javaslattal állt elő az ilyen gyakorlat megakadályozása érdekében. Ennek folytatásaként 2010 decemberében kiadták az internet szabadságának megőrzéséről szóló utasítást, amely kompromisszumos megoldásként továbbra is engedélyezte a forgalomirányítási technikák használatát, ha azok nem valósítanak meg megkülönböztetést, illetve blokkolást vagy feltorlódást. (Null, 2011, pp. 461–462.) A Verizon azonban megtámadta a döntést, és a Szövetségi Fellebbviteli Bíróság 2014. január 14-én megszületett ítéletében (740 F.3d 623 (D.C. Cir. 2014)) úgy határozott, hogy az FCC-nek nincs hatásköre a szabályozás meghozatalára, mivel az internetszolgáltatók nem tekinthetők közös szállítóknak. A szervezet nem támadta meg a bíróság döntését, ehelyett 2015. február 26-án olyan döntést hozott, amely mégis az 1934-es kommunikációs törvény és az 1996-os telekommunikációs törvény alá tartozónak mondta ki az internetszolgáltatókat. Az FCC ezt követően április 13-án adta ki új, a szabad internet megőrzéséről és elősegítéséről szóló utasítását. A szabályozást a szolgáltatók érdekvédelmi szervezetei megtámadták, de 2016. június 14-én a Szövetségi Fellebbviteli Bíróság ezt elutasította. Az érdekeltek azonban nem nyugodtak bele a döntésbe, így az internetsemlegességgel kapcsolatos vita várhatóan a Legfelsőbb Bíróságon és a Kongresszusban fog folytatódni. (Npr, 2016)

A bűnüldözés érdekei és az amerikai Alkotmányban (különösen annak első, negyedik és ötödik kiegészítésében) lefektetett alapvető jogok összeütközése megjelenik a kiberbűnözéssel kapcsolatos ügyekben is. Az ötödik kiegészítés tartalmazza az önvádra kötelezés tilalmát, ami azt jelenti, hogy a terhelt nem kötelezhető a saját bűnösségét alátámasztó írásbeli vagy szóbeli vallomás megtételére. A bírói gyakorlat alapján ez nem vonatkozik a tárgyi bizonyítékokra – a szolgáltatásukra már viszont igen – és az önként tett kijelentésekre, így azokra sem, amiket a terhelt az interneten tett közzé, akár nyilvános, akár zárt csoportban. Érdekes kérdésként merül fel, hogy amennyiben valaki titkosítással védi az illegális tartalmat a számítógépén, úgy az kötelezhető-e a jelszó átadására. 2007-ben Sebastian Boucher gyermekpornográfia birtoklásával kapcsolatos ügyében a szövetségi bíróság úgy ítélte meg, hogy az Alkotmány tiltásába ütközne, amennyiben a vádlottat kötelezik a kód megadására. Másabb lenne azonban egy hasonló ügy kimenetele, amennyiben a kódot a terhelt egy naplófájlba menti le. Ez ugyanis nem tekinthető vallo-

másnak, így nem esik az ötödik kiegészítés védelme alá. (Brenner, 2011, pp. 115–118.) A tartalomszabályozás terén a szövetségi kormány nem hozhat kormányszintű szabályozást, mivel az az Alkotmány első kiegészítésébe ütközne, így elsősorban az intézményi szinten megvalósuló szűrést támogatják. Ebben az esetben a felhasználóitól magasabb, de az államitól alacsonyabb szinten (pl. a munkáltató, az iskola vagy a könyvtár) döntik el, hogy mely tartalmak nem elérhetők. (Parti, 2010, p. 99.) Ez alól kivételt az obszcén tartalmak, és különösen a gyermekpornográfia jelentenek, amelyek nem élvezik az első kiegészítésben foglalt védelmet. A gyermekek online védelméről szóló 1998-as törvény (*Child Online Protection Act*) azt kívánta megakadályozni, hogy a kiskorúak számukra károsnak ítélt tartalmakhoz férjenek hozzá az interneten. A törvényt vizsgáló bíróságok megállapították, hogy a törvény korlátozásai számos ponton nem voltak megfelelőek, így például túlzottan tág fogalmakat használt, és az egyes tartalmak károsságát nem azok kontextusával együtt értelmezték. 2008-ban a 3. Fellebbviteli Bíróság ezért alkotmányellenesnek nyilvánította. (Lamut, 2008)

A szabályozás egységes érvényesülését szolgálja, hogy bár főszabályként a szövetségi kormánynak csak korlátozott bűnügyi hatásköre van, kizárólagos hatáskörrel bír a tagállamközi és államközi kereskedelemben, és így gyakorlatilag a számítógépeket és hálózatokat érintő ügyekben is. (Borisevich et al. 2012, p. 278.) Ugyan az Egyesült Államok 50 tagállamának és a fővárosnak a kiberfenyegetésekkel kapcsolatos szabályozása nagymértékben konzisztens a szövetségivel, előbbiek alkalmazása számos nehézséget okozna és áttekinthetetlen, szövevényes rendszert alkotna. (Brenner, 2011, p. 85.) A szövetségi szabályozás fontosságából következik, hogy a bírói gyakorlatnak – különösen a szövetségi Legfelsőbb Bíróság ítéleteinek – fontos szerepe van a jogszabályok értelmezésében és fejlesztésében. (Dornfeld 2015, pp. 71–73.)

Intézményi szinten elnöki bizottságot hoztak létre a kritikus infrastruktúra védelmére, amelynek feladata a kiberbiztonság irányítása és koordinálására, valamint 2008-ban létrejött az Átfogó Nemzeti Kiberbiztonsági Kezdeményezés (*Comprehensive National Cyber-security Initiative*). (Zhang 2013, p. 123.) Az USA Belbiztonsági Minisztériumán belül működik a Nemzeti Kiberbiztonsági Részleg (*National Cyber Security Division*), amely a fenyegetésekre való reagálással és a kockázatkezeléssel foglalkozik. A kibertámadások elhá-

rításáért a hadseregen belül működő Kiberparancsnokság felel. (Levin – Ilkina, 2013, p. 19.)

2.2. Kiberdiplomácia: új tényező az amerikai külpolitikában

Az Egyesült Államok külpolitikájában egyre hangsúlyosabb szerepet kap az új kiberfenyegetésekkel szembeni nemzetközi együttműködés kialakítása, valamint az internetszabályozás alapelveinek a megfogalmazása. Az ország a több érdekelt bevonásával működő (*multi-stakeholder*) rendszer elképzelését támogatja, vagyis az ipar szereplői, a civil társadalom, a tudományos élet képviselői és az egyének bevonásával megvalósuló szabályozást, amelyet alapvető fontosságúnak ítél. A megoldás támogatásában nemcsak a szabadságjogok szélesebb érvényesülése játszik közre, hanem az a tény is, hogy a számítástechnikai cégek és a működésben szerepet játszó nem kormányzati szervek – mint például az ICANN – amerikai kötődéssel bírnak. (Eichensehr, 2015, pp. 346-347.)

Az Egyesült Államok Kormányzati Ellenőrzési Hivatalának 2010. júliusi jelentése szerint akkor még nem volt egységes stratégia a nemzetközi fellépés céljait illetően, és az egységes irányítás is hiányzott, így ekkor inkább csak ad hoc kapcsolatfelvételekről lehetett beszélni. (Sofaer – Clark – Diffie, 2010, pp. 184–185.) Ez a szemlélet jól megmutatkozott az ITU nemzetközi távközlési szabályozásának (ITR) megújítása kapcsán, amelyet az Európai Unió már szükségtelennek ítélt, az Egyesült Államok azonban 2008-ban kiemelt fontosságúnak nyilvánított. A tárgyalások során képes volt érdekeit jelentős mértékben érvényesíteni, és csak az általa jónak ítélt javaslatokat megtartani, a végén azonban mégis teljes amerikai diplomáciai kudarcként került kommunikálására a folyamat, és a 2012-es egyezménytervezet megbukott. (http://www.internetgovernance.org, 2012)

2010-ben Hillary Clinton külügyminiszter beszélt a kibertér és az emberi jogok kapcsolatáról, és F. D. Roosevelt elnök hét évtizeddel korábbi kijelentését alapul véve a „kapcsolódás szabadságát" az ötödik szabadságként fogalmazta meg.[1] Élesen elítélte azokat az országokat, amelyek cenzúrázzák az

1 Az 1941. január 6-án megfogalmazott gondolat szerint négy alapszabadság illeti meg a világ minden lakosát. Ezek: szólásszabadság, vallásszabadság, a nélkülözéstől való szabadság és a félelemtől való szabadság. Az emlegetett ötödik szabadság digitális alapjogként való kezelése az ENSZ hasonló irányú törekvésével vethető össze. A 2003-as WSIS zárójelentése úgy fogalmaz, hogy mindenkinek lehetőséget kell biztosítani az információs társadalomban való részvételre. (WSIS, 2003)

internet tartalmát, és beszélt hazája aktív fellépéséről az ilyen gyakorlat ellen. (Crook, 2010) 2011-ben az Obama-adminisztráció ismételten megerősítette az internetszabadság fontosságát az amerikai külpolitikában. (Fidler 2012) Ez előre jelezte az Egyesült Államok aktív fellépését az elkövetkező időszakban. Ebből a szempontból kiemelkedő jelentőségű volt a 2011-es év, amikor elfogadták az ország kibertérre vonatkozó nemzetközi stratégiája, valamint több bilaterális egyezmény megkötésére is sor került, amelyekkel a későbbiekben részletesen is foglalkozom.

A kiberstratégia megerősítette azt, hogy az Egyesült Államok az alapjogok érvényesülését tartja bármilyen internetszabályozás alapjának. A szólásszabadságon kívül ez magában foglalja a magánélet védelmének biztosítását és az információ szabad áramlását. A dokumentum második fejezete kifejezetten a diplomáciai célokra koncentrál, amelyek között szerepel a kibertérrel kapcsolatos alapelvek terén konszenzus kialakítása a nemzetközi közösséggel. Ennek módja elsősorban bi- és multilaterális egyezmények kötése, valamint a magánszektor képviselőivel való szoros kapcsolattartás. A dokumentum kitér a kiberfenyegetések elleni fellépésre is, és fenntartja az Egyesült Államok számára a jogot, hogy egy állam részéről érkező kibertámadásra akár gazdasági szankciókkal vagy fegyveresen is válaszoljon. (White House, 2011)

A 2011-ben megkötött kétoldalú megállapodások sorában az elsők között volt a február 4-én bejelentett közös kanadai-amerikai akcióterv, amelyben fontos szerepet kap a kiberbiztonsághoz kapcsolódó együttműködés létrehozása és a digitális kritikus infrastuktúra védelme. Ezekhez kapcsolódóan Kanada vállalta, hogy ratifikálja az Európa Tanács Számítástechnikai bűnözésről szóló egyezményét (a továbbiakban Budapesti Egyezmény) is, amellyel bővebben az Európáról szóló részben foglalkozom. (http://actionplan.gc.ca/2011) Ugyanezen évben kiegészítésre került az 1951-ben megkötött ANZUS-paktum is,[2] amely ezután már a kibertérben indított, a részes felek „területi integritását, politikai függetlenségét vagy biztonságát" fenyegető támadás esetén is előírja az Egyesült Államoknak és Ausztráliának a közös fellépést. (Sullivan

2 ANZUS: Ausztrália, Új-Zéland és Egyesült Államok Biztonsági Egyezménye, 1951. szeptember 1-jén írták alá az érintett államok. 1986-ban, egyéves vitát követően az Egyesült Államok felfüggesztette kötelezettségvállalásait Új-Zélanddal szemben, és azóta csak éves bilaterális találkozókra (AUSMIN) kerül sor Ausztráliával.

2014; Levin – Ilkina, 2013, p. 5.) 2011. május 25-én együttműködésről szóló megállapodás született az Egyesült Királyság kormányával is, amelynek részleteivel a brit szabályozásról szóló fejezetben foglalkozom. (www.gov.uk, 2011) Ugyanezen év július 19-én Indiával közös szándéknyilatkozatot írt alá Lute amerikai helyettes államtitkár, amely a kiberbiztonsággal összefüggő kritikus információk cseréjét irányozta elő. (http://www.dhs.gov, 2011) Ennek folytatásaként 2015. augusztus 11-12-én megbeszélésre került sor az amerikai és indiai kormánydelegációk között, ahol a korábbiakon túl felmerültek a kiberbűnözéssel szembeni fokozott fellépés, az internetszabályozás és a kibertérben történő állami viselkedési normák kérdései is. (White House Statement, 2015) Az Egyesült Államok, Kanada, az Egyesült Királyság, Ausztrália és Új-Zéland közötti multilaterális hírszerzési együttműködést Öt Szem (*Five Eyes*) néven is emlegetik. Az Edward Snowden által kiszivárogtatott információk szerint ez egy „szupranacionális hírszerző ügynökség, amely nem felelős a részes országok saját jogszabályainak", működési elve pedig az, hogy egymás állampolgárait figyelik meg, ezzel kerülve meg az ezt korlátozó törvényeket. Ezen kívül más szövetséges országok, illetve az ENSZ tisztségviselőinek lehallgatásáról is derültek ki információk. (Ellis, 2014, p. 178.)

Az Egyesült Államok nemcsak a baráti országokkal igyekszik a kibertér szabályozásának jövőjét alakító egyezményeket kötni, hanem azon államokkal is, melyekkel alapvető nézetkülönbség van a szabályozás alapját illetően. 2013 júniusában Oroszországgal született megállapodás, amelyben a felek kötelezettséget vállaltak, hogy a nemzetbiztonságot érintő incidensekről valós idejű kommunikációt folytatnak közvetlenül egymással. (Eichensehr, 2015, p. 364.)

Kínával kapcsolatban sokkal kevésbé egyértelmű az amerikai viszony. Hillary Clinton 2010-es kijelentése elsősorban a kínai módszer kritikája volt, melyet éles diplomáciai válasz követett Peking részéről. (Crook 2010) Xi Jinping elnök 2013-as hivatalba lépésekor küldött gratulációjában Obama elnök egyúttal felvette a kiberbiztonság kérdését, amely a másik fontos töréspont a két állam között. Xi későbbi amerikai látogatása alkalmával is utalt az amerikai elnök azon internetes betörésekre, amelyek szerinte Kínából indultak – amit a kínai vezetés tagadott –, és az amerikai kormányzaton kívül számos nyugati vállalat számára is súlyos károkat okoztak, elsősorban ipari kém-

kedéssel. A kérdésben azonban nem közeledett a két fél álláspontja. (Lee, 2014, p. 951) 2015. szeptember 24-25-én Xi elnök ismételt amerikai látogatása során a két ország számos ügyben, így a kiberbiztonság kérdésében is egyezményt kötött. Ebben a felek megegyeztek arról, hogy fellépnek a területükről elkövetett kiberbűncselekmények ellen, és ezek eredményéről szükség esetén tájékoztatják egymást. Ezen kívül létrehozásra kerül a kiberbűnözés elleni fellépés és a kapcsolódó kérdésekkel foglalkozó magas szintű kapcsolattartási mechanizmus. Egyúttal a felek ígéretet tettek arra, hogy nem hajtanak végre vagy támogatnak tudatosan olyan cselekményeket, amelyek üzleti titkok és szellemi tulajdon lopására irányulnak. (White House Fact Sheet, 2015)

Az Egyesült Államok a Mandiant biztonsági cég 2013-as jelentése óta nyíltan a kiberbetörések egyik fő forrásának nevezi Kínát. A dokumentum szerint a kínai Népi Felszabadító Hadsereg 61398. számú egysége áll a nagyszámú támadás mögött. Az amerikaiak gyakran egyoldalú igénye Kínával szemben a kibertámadások mérséklésére valószínűleg nem segíti a feszültségek enyhülését, hiszen maga az amerikai kormányzat is érintett volt bizonyos kiberháborús eszközök alkalmazásában. Snowden 2013-as szivárogtatását követően kiderült, hogy az Egyesült Államok 2011-ben 231 támadást hajtott végre Oroszország, Kína, Irán és Észak-Korea ellen. (Eichensehr, 2015, p. 319.) A leghírhedtebb ilyen akció azonban korábbra tehető: 2007-ben kezdődött meg az az izraeli-amerikai közös hadművelet, amelynek keretében kártevő szoftverrel fertőzték meg az iráni atomkutatásban urándúsításra használt centrifugákat. (Moore, 2013, p. 226.) A Stuxnet névre hallgató vírus húszszor összetettebb kódolással készült, mint más kártevők, és szinte teljesen hibamentes. Úgy írták meg, hogy a rendszerbe jutást követően képes legyen teljesen önállóan működni. További különlegessége, hogy úgy képes megváltoztatni az érintett rendszerek működését, hogy közben mindent rendben lévőnek mutat a kezelőszemélyzet felé. Terjedéséhez úgynevezett nulladik napi sebezhetőségeket használt ki, és a gyárakban, erőművekben, valamint a kritikus infrastruktúráknál (pl. forgalomirányító rendszerekben) használt Siemens programozható logikai vezérlőket fertőzte meg. Tényleges célpontjai csak bizonyos, megadott azonosítószámmal ellátott típusok voltak, amelyeket elsősorban Iránban gyártottak. 2010 júniusában jelenlétét számos ilyen helyen fedezték fel. A kártevő az év novemberéig az iráni centrifugák ötödét rongálta meg, ezzel több hónapos leállásra kényszerítve

az iráni atomprogramot. (Sipos, 2016, p. 29.) A 2016. július 8-án megjelent *Zero Days*[3] című dokumentumfilm amellett érvel, hogy a korábban tagadott amerikai–izraeli kormányérintettség egyértelmű a bizonyítékok fényében. Emellett szól például a kártevő kifinomultsága, továbbá az, hogy a célba vett rendszerek megfertőzése, azok internettől való elzártsága miatt csakis személyi közreműködéssel történhetett. A támadók az iráni urándúsító üzem beszállítóit fertőzték meg először, és rajtuk keresztül juttatták be a Stuxnetet. További jel a támadás állami tervezettségére, hogy a kártevő támadása idején számos vezető iráni atomtudós merénylet áldozata lett. A dokumentumfilmben megszólaltatott amerikai és izraeli személyek alapján a Stuxnet létrehozásának kezdeményezője George W. Bush elnök volt, aki el akarta kerülni a nyílt fegyveres konfliktust Iránnal, ugyanakkor az iráni nukleáris kapacitás kiépülését is meg akarta akadályozni. Belső források szerint a kártevő fejlesztésében részt vett az NSA, a CIA, az amerikai hadsereg Kiberparancsnoksága, a Moszad és a kiberháborúra specializálódott izraeli 8200-as egység. A kódban elhelyeztek egy záró dátumot is, amely csak néhány nappal esik Barack Obama elnöki beiktatása elé, és többek szerint ez is a Bush-adminisztráció érintettségét mutatja a kártevő elkészítésében. Ugyanakkor a támadásokra már Obama elnök kellett, hogy engedélyt adjon, mivel – mint az a Snowden által kiszivárogtatott anyagok között lévő elnöki rendeletből kiderül – támadó kibertevékenységet csak az elnök utasítása alapján lehet folytatni. A leállás dátuma és a támadások közötti időintervallumban a kártevő kódja fejlesztésre került. Ezt azonban már a gyors eredményeket akaró izraeliek saját maguk végezték el, és a változtatások azt eredményezték, hogy a kártevő elterjedt az egész világon, és létezése nyilvánosságra került.

Kínával kapcsolatban ugyanakkor más hangok is vannak, amelyek az együttműködés helyett a szankciós politikát javasolják. 2006-ban a Kongresszus egyik képviselője javaslatot tett a globális online szabadságról szóló törvény (*Global Online Freedom Act*, GOFA) elfogadására, aminek oka az amerikai információs magáncégek és a kínai kormány közötti együttműködés vitás megítélése volt. Újabb javaslatok kidolgozására került sor 2007-ben, 2009-ben és 2011 áprilisában, illetve decemberében. Ezek közül a 2007-es

3 Az alkotás címe (nulladik napok) az olyan számítástechnikai sebezhetőségekre utal, amelyeket a támadón kívül senki más nem fedezett még fel, ezért javítani sem tudták azokat.

javaslat jutott legtovább a jogalkotási eljárásban, mivel az a Kongresszus elé került, miután Christopher Smith republikánus képviselő benyújtotta azt. A javaslatot rajta kívül 3 republikánus és 4 demokrata képviselő támogatta. A szavazásra bocsáthatóságról az Energiaügyi és Kereskedelemi, valamint a Jogi Bizottság döntött, amelyek elutasították annak Kongresszus elé terjesztését. (GovTrack, 2016; Congress, 2016) Ennek a változatnak három fő sarokpontja volt: éves jelentések készítése az egyes országokban tapasztalható internetkorlátozásokról, a leginkább korlátozó országok megjelölése és végül a rendszer fenntartásához szükségesnek ítélt technikai javak ezen helyekre történő exportjának korlátozása. (Fidler, 2012) Véleményem szerint egy ilyen lépés megtétele egyértelműen a hidegháborús COCOM-lista[4] felélesztését jelentené, és jelentősen rombolná az államok közötti bizalmat, ellehetetlenítve a közös nevezőre jutást.

3. Európa

3.1. A közösségi szabályozás kezdetei

Európában az 1990-es években kezdett el kialakulni a kibertér szabályozása, egyszerre nemzeti és nemzetközi szinten. Az utóbbi formálásában a legaktívabbak az Európa Tanács és az Európai Unió voltak. Az internethozzáféréssel rendelkező háztartások aránya világviszonylatban is kiemelkedően magas az EU tagállamokban, az Eurostat (2015) adatai szerint 2014-ben átlagosan 78%-os volt. A jelentős számú felhasználó mellett a másik fontos tényező, ami a szabályozás alakulását befolyásolta, az e-kereskedelem jelentőségének felismerése volt. Az Unió JOIN/2013/01 sz. európai kiberstratégiájának preambuluma évi 500 milliárd euróra becsülte azt a gazdasági növekedést, amit az egységes digitális piac kialakítása jelentene. A stratégiában megfogalmazásra kerül az a felismerés is, hogy ennek alapja a felhasználói bizalom megteremtése.

A bizalom megteremtésének egyik fontos eszköze a kiberbűnözés elleni fellépés erősítése. Ennek terén az európai jogharmonizáció 1989-ben kez-

4 COCOM-lista: a hidegháború nyugati blokkjába tartozó országainak a keleti blokk államaival szemben bevezetett gazdasági embargója, amely megtiltotta csúcstechnológiai termékek ide történő exportját.

dődött el, amikor az Európa Tanács kibocsátotta a számítógépekkel kapcsolatos bűncselekményekről szóló R (89) 9. számú Miniszteri Bizottsági ajánlást, amelyben a kriminalizálandó cselekményeket határozták meg a jogalkotó számára egy minimum, illetve egy fakultatív listába foglalva. Ennek előkészítése már 1985 óta folyt egy szakértőkből álló bizottságban, amelynek zárójelentésében foglalt tanulságait az ajánlás részévé tették. Hat évvel később került megalkotásra az információs technológiával összefüggő büntető eljárásjogi problémákról szóló R (95) 13. ajánlás, amelyben alapvető eljárásjogi kérdések kerültek tisztázásra. (Walden, 2004)

2001. november 23-án került elfogadásra az Európa Tanács Számítástechnikai bűnözésről szóló egyezménye (a korábban már említett Budapesti Egyezmény), amely jelentős előrelépés volt, hiszen míg az ajánlások végrehajtása teljesen opcionális, ennek ratifikációjával a részes államok kötelezettséget vállalnak annak érvényre juttatására. A szerződést 2001-ben 35 ország írta alá, köztük olyan Európa Tanácson kívül államok, mint az Egyesült Államok, Kanada, Japán és Dél-Afrika, ám az egyezmény ratifikációja több országban is várat még magára. (Buono, 2012, p. 336.) 2012-re harminchat ország ratifikálta a szerződést, köztük az Egyesült Államok, rajtuk kívül pedig további tizenöten aláírták, de még nem ratifikálták, mint pl. Kanada, Dél-Afrika és Svédország. (Borisevich et al. 2012, p. 272.) A Budapesti Egyezmény lefektette a kibertér szabályozásának azon minimumát, amelyet a nyugati világ egyöntetűen elfogad. Jól mutatja ezt az is, hogy a Brit Nemzetközösség 54 igazságügyi minisztere támogatta az Egyezmény mintájára megalkotott a számítógépes és számítógépes környezetben elkövetett bűncselekményekről szóló LMM (02) 17. modelltörvényt. (Walden, 2004, p. 324.) Más szervezetekben is az Egyezmény alapján képzelik el a kiberbűncselekményekkel kapcsolatos szabályozás megalkotását, így például a Karib-tengeri Közösségben (Project Cybercrime, 2014) és a Délkelet-ázsiai Nemzetek Szövetségében (ASEAN, 2008).

Az Európa Tanács ezt követően is részt vett a kibertér szabályozásának alakításában, továbbá számos, az igazságszolgáltatásban dolgozók részére szóló továbbképzést szervez. (Council of Europe, 2016) 2012-ben – az Európai Unióval közös CyberCrime@IPA projekt kereti között –, az angol Nigel Jones felügyeletével kezdődtek el a munkálatok az elektronikus bizonyításról szóló

útmutató elkészítésén. Ennek célja azon országok bírói, ügyészi és rendőrei munkájának segítése, melyek még csak most dolgozzák ki a kiberbűnözés elleni fellépésről szóló stratégiájukat. A dokumentum még ebben az évben elkészült és június 7-én az Octopus konferencián, amelyen 80 ország, nemzetközi szervezetek, a magánszektor és a tudományos élet szakértői voltak jelen. (Electronic Evidence, 2016)

3.2. Az Európai Unió kiberbiztonság megteremtésére irányuló lépései

A kiberbűnözéssel kapcsolatos európai jogharmonizációra az Európai Unió keretei között is sor került. Az Unió szupranacionális szabályozásában hangsúlyos szerep jutott a kiberbűnözés elleni közös fellépés megteremtésének. Az 1992-ben elfogadott Maastrichti Szerződés alapján létrejött hárompilléres rendszerben a kiberbiztonság a második pillért jelentő közös kül- és biztonságpolitika, a kiberbűncselekményekkel kapcsolatos szabályozás pedig a harmadik pillér, a bel- és igazságügyi együttműködés része lett. Ez a két terület sok vonatkozásban hasonlított egymásra, ami abból fakadt, hogy mindkettő az államközi együttműködés szintjén valósult meg. Az ezekkel kapcsolatos döntések meghozatalához – néhány végrehajtó jellegű szabályt kivéve – a tagállamok Európai Tanácsban lévő állam- és/vagy kormányfőinek egyhangú döntésére volt szükség, valamint az Európai Bizottság meg kellett ossza kezdeményezési jogát a tagállamokkal, és a Parlamentnek mindössze korlátozott konzultatív jogkör jutott. Továbbá az EU nem fogadhatott el közvetlen hatályú szabályozást, és az EU Bírósága nem vizsgálhatta a megszületett másodlagos jogforrások érvényességét, valamint szerződésekkel való összeegyeztethetőségét. (Chalmers 2014, p. 53.)

Az 1999-ben hatályba lépett Amszterdami Szerződés fontos, harmadik pillért érintő újítása volt a kerethatározatok bevezetése, amely lényegét tekintve közvetlen hatály nélküli irányelv volt. (Peers 2011, pp. 272–273.) Ilyen formában került sor a kibertérre vonatkozó legtöbb jogforrás elfogadására. Fontos lépés volt a 2005//222/IB kerethatározat elfogadása, amely a Budapesti Egyezmény megoldásait vette át. A 2007-ben Észtország ellen oroszpárti hackerek által elkövetett kiterjedt kibertámadás tapasztalatai nyomán került sor a 2008/114/EK irányelv elfogadására, amely a kritikus infrastuktúra ki-

jelölésével és védelmével foglalkozik. A Lisszaboni Szerződés 2009-es hatályba lépéséig ezen rendelkezések végrehajtásának eszközrendszere csak igen nehezen volt biztosítható. A hárompilléres rendszer számos problémával és hiányossággal küzdött, többek között a tagállamoknak széles jogköröket biztosító szabályozásból eredő uniós intézményrendszer elégtelen mozgásteréből és a másodlagos jogforrások tagállamok általi helytelen átültetéséből következően. A Lisszaboni Szerződés elfogadása jelentős változásokat hozott, így a Tanácsban a döntéshozatalhoz már nincs szükség egyhangúságra, csak minősített többségre; bővültek a Parlament jogalkotási lehetőségei, és a Bíróság is minden jogkörét gyakorolhatja. (Buono, 2012, p. 336.; Chalmers, 2014, p. 583.)

A Szerződés után kezdődött meg az addigi másodlagos uniós jogforrások újragondolása, és a kiberbűnözéssel kapcsolatos EU szabályozás új alapokra helyeződött mind jogi, mind politikai szinten. A 2005-ös kerethatározat eddigre már elavulttá vált, mivel elfogadásakor a jogalkotó még nem ismerte fel a nagyméretű kibertámadásokban rejlő veszélyeket, valamint a botnetek megjelenése is új kihívást jelentett, melyet a jogforrás nem volt képes kezelni. (Buono, 2012, pp. 338.) Az ennek felváltására elfogadott 2013/40/EU irányelv már kriminalizálta a botnetek előállítását, árusítását, használatra történő beszerzését, behozatalát és forgalomba hozatalát is, valamint a bűnüldöző szervek szorosabb együttműködésére tett javaslatot az információs rendszerek ellen elkövetett bűncselekmények esetén. Fontos újítása az irányelvnek, hogy 10-11. cikke lehetővé teszi a jogi személyek felelősségének a megállapítását, és velük szemben különleges szankciók alkalmazását irányozza elő, mint az elkövetésre használt létesítmények bezárása vagy a bíróság által elrendelt felszámolás.

A tartalomszabályozás kérdései egységes uniós szabályozás hiányában elsősorban tagállami hatáskörbe tartoznak. Közülük számosan, így például Németország, az Egyesült Királyság és Magyarország is jogrendje részévé tette az internetblokkolást. (Parti, 2010) Kivételt képez a gyermekpornográfia, amely kapcsán a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló 2011/93/EU irányelv 25. cikke előírja a tagállamoknak, hogy az ilyen tartalommal bíró vagy azt terjesztő honlapokat azonnal távolítsák el, ami történhet a hozzáférés meggátolásával is.

Szintén nincs egységes, szupranacionális szintű szabályozás azzal kapcsolatban, hogy a titkosítással védett, feltehetően jogsértő tartalomhoz tartozó jelszó gyanúsítottól történő megszerzése az önvádra kötelezés tilalmába ütközik-e. A 2016. május 10-11-én Dublinban megtartott *Fighting Cybercrime: Between Legal Challenges and Practical Difficulties* című konferencián tartott előadásában Philippe van Linthout belga vizsgálóbíró is érintette a kérdést. Ő az ittas vezetéshez hasonlította az esetet: az intézkedés alá vont sofőr sem tagadhatja meg, hogy alávesse magát a szondáztatásnak vagy vérvételnek. A belga büntetőtörvénykönyv egy, míg a francia kódex három évig terjedő szabadságvesztéssel rendeli büntetni azt, aki megtagadja a feloldáshoz szükséges jelszó átadását a hatóságoknak. Utóbbi szerint a büntetés mértéke öt évig terjedő szabadságvesztés, ha a titkosított információ segítségével más bűncselekményt lehetett volna megelőzni. Ez sem jelent azonban megoldást: a VeraCrypt már képes úgy titkosítani adatokat, hogy maga a felhasználó sem ismeri az azt feloldó jelszót. Rainer Franosch hesseni első ügyész elmondta, hogy éppen ezért olyan esetekben, amikor félő, hogy a gyanúsított ezzel az eszközzel fog élni, kommandósok segítségével fogják el.

3.3. Az uniós jog egyéb internetre vonatkozó szabályozásai

A kiberbiztonságon túl számos más kérdésben is az európai szabályozás egységesítésére törekszik az Unió. Ezek közül a legfontosabbak az e-kereskedelem, az elektronikus tartalomszolgáltatás és az adatvédelem területén született másodlagos jogforrások. Ennek kiépítésében lényeges cél volt a telekommunikációs piac liberalizációja és összehangolása, amely néhány – a nemzeti viszonyokhoz történő jobb igazítás érdekében meghagyott – kivétellel meg is történt. Számos fogyasztói szolgáltatás ára csökkent ennek köszönhetően, ám ezen intézkedések nem váltották be a hozzájuk fűzött reményeket, és nem nőtt jelentősen a befektetések mértéke. Hogy az egyes nemzeti szabályozások különbségéből adódó nehézségeket megszüntessék, a Tanács és a Parlament COM(2013) 627 számmal javaslatot tett az elektronikus hírközlés egységes európai piacáról szóló rendelet elfogadására. Ez az Európa 2020 stratégia részét képező uniós Digitális Menterend legelső pillére. (Bartóki-Gönczy, 2014, pp. 3–4.)

A 44/2001/EK rendelet elfogadása fontos lépés volt annak érdekében, hogy megszűnjenek az interneten kötött szerződésekkel kapcsolatos bizonytalan-

ságok. A rendelet ugyanis bizonyos feltételek fennállása esetén lehetőséget teremt arra, hogy az így kötött fogyasztói szerződések esetén a fogyasztók lakóhelyükön perelhetőek legyenek, illetve indíthassanak pert. (Erdős, 2014, pp. 84–86.) Hasonlóan lényeges volt a fogyasztók jogairól szóló 2011/83/EU irányelv, amely számos rendelkezéssel igyekszik a digitális piac iránti bizalmat megteremteni. Így például a kereskedő a vásárlás előtt köteles meghatározott információkról (mint pl. a termék lényeges tulajdonságai, az elfogadott fizetési módok stb.) tájékoztatást adni, valamint a vásárláshoz vezető gombnak is egyértelműen tükrözni kell funkcióját. A szerződés másolatát vagy visszaigazolását a fogyasztó számára papíron vagy más adathordozón biztosítani kell. Továbbá az áru minőségét szavatolja az, hogy a fogyasztó 14 napon belül indoklás nélkül elállhat a szerződéstől. Ezek a rendelkezések mind arra szolgálnak, hogy a felhasználókat ne lehessen silány termékek árusításával megtéveszteni, és aláásni az internet iránti közbizalmat, amelynek erősítése az EU egyik igen fontos politikája.

Fontos még megemlíteni az internetsemlegesség kérdését is, hiszen az elvet támogatók szerint az internetet nyitottsága és könnyű elérhetősége tette sikeressé, és szerintük ezeket a feltételeket a megfelelő verseny érdekében jogi eszközökkel kell biztosítani. Ugyanakkor mivel az internet hozzáférésért fizetni kell, az azonos feltételek nem érvényesülnek, és a hálózatok jelenlegi kapacitása is véges. Ez utóbbi miatt jelent meg a szolgáltatók részéről a forgalomirányítási technikák alkalmazása, amely ugyanakkor lehetőséget teremtett arra, hogy bizonyos szolgáltatásokat ne vagy ne egyenlő minőségnek nyújtsanak a felhasználók részére. (Mester, 2012, pp. 149–150.) Az ezzel kapcsolatos vita az EU-ban 2009-ben kezdődött el, amikor a korábbi szabályozási keretet felülvizsgálták. (Bartóki-Gönczy, 2014, p. 12.) 2011-ben a Parlament és a Tanács COM (2011) a 222. sz. közös közleményében kiállt a semleges és nyitott internet mellett. Az ezt érő fenyegetések közé sorolta az adatforgalom blokkolását és gátolását, valamint az adatkérések feltorlódását és az átláthatóság hiányát. A Bizottság 2015. június 30-án kelt IP/15/5265 sajtóközleményében jelentette be, hogy döntés született a roaming díjak eltörléséről, valamint a nyílt internet támogatásáról. Ennek értelmében a felhasználók szabadon eldönthetik, milyen tartalmakhoz férnek hozzá, és ezt sem blokkolni, sem lassítani nem lehet, továbbá a fizetett prioritizálás is tiltott lesz. Vagyis min-

den adatforgalmat egyformán kell kezelni, ami alól csak pontosan meghatározott – biztonsági jellegű – kivételek lehetnek. Ugyanakkor a javaslatot számos kritika érte, amelyek szerint homályos és pontatlan megfogalmazásai kiskapukat biztosítanak a szabályozás megkerülésére. Az ezzel kapcsolatos módosító javaslatok mindegyikét leszavazták a Parlamentben. (Price, 2015)

Nagy változásokra került sor az uniós adatvédelmi szabályozásban is. A személyes adatok kezeléséről szóló 95/46/EK irányelv rendelkezései alapján személyes adatot csak akkor lehet harmadik országba továbbítani, ha az ottani védelem szintje megfelelő. Az irányelv lehetőséget biztosít a Bizottság számára, hogy az megállapítsa a megfelelő védelmi szint meglétét egy országban, ekkor nem kell alkalmazni a különleges korlátozásokat az ide irányuló adattovábbítások esetén. A Bizottság a védett adatkikötőről szóló 2000/520/EK határozatában elismerte az Egyesült Államok Kereskedelmi Minisztériuma által kiadott biztonságos kikötőkre (*Safe Harbor*) vonatkozó alapelveket mint a védelem megfelelő szintjét. Ez a döntés olyan feltételek mellett is lehetővé tette az amerikai cégek számára a személyes adatok továbbítását, amelyeknél a szabályozás lényeges eltérései miatt egyébként nem lett volna lehetőség. Az Unió által meghatározott három alapelvnek (adatvédelmi politika átláthatósága, biztonságos kikötő alapelveinek a vállalati adatvédelmi politikába építése és hatósági végrehajtás) meg kellett felelni.

Az EU intézményei számára mindig is fontos kérdés volt az adatvédelmi szabályok maradéktalan betartása, és ezek elégtelensége esetén fellépett. Így például a Bíróság 2006 májusában a C-317/04 és C-318/04. egyesített ügyekben formai okok miatt megsemmisítette az USA és az Európai Közösség közti személyes adatok továbbításáról szóló megállapodást, amely a terrorizmus elleni küzdelem részeként született meg. 2014 májusában a C-131/12. ügyben a Bíróság úgy határozott, hogy a keresőmotorok működtetői felelősek a külső honlapokon fellelhető személyes adatok kezeléséért, és az érintettek közvetlenül megkereshetik őket, hogy töröljék a róluk információt tartalmazó linket a találati listáról. (Lehóczki, 2015, p. 94.)

Éppen ezért váltott ki heves reakciókat Edward Snowdennek az amerikai hírszerzés működését felfedő 2013-as kiszivárogtatása. Az Unióban, és különösen Németországban, jelentős megrendülést okoztak azok a hírek, miszerint az NSA korlátlan hozzáféréssel bír a kibertérben található személyes adatok-

hoz. (Lehóczki, 2015, p. 93.) A Bizottság az ügyre reflektálva két közleményt is megfogalmazott a kérdésben 2013 novemberében: a COM(2013) 846 a bizalom helyreállításával, a COM(2013) 847 pedig a rendszer vizsgálatával foglalkozott. Utóbbi során a Bizottság jelentős hiányosságokat talált, amelyek orvoslására 13 pontból álló ajánlást fogalmazott meg. A biztonságos kikötő végét azonban a Bíróság a C-362/14 számú, Schrems-ügyben hozott ítélte jelentette. Schrems osztrák állampolgárként az ír adatvédelmi hatósághoz nyújtott be panaszt, mivel a Facebook európai leányvállalata itt működik, és innen továbbítják az amerikai szerverekre a feltett tartalmat, ezt azonban elutasították. Az ír legfelsőbb bíróság az EU Bírósághoz fordult előzetes döntéshozatali kérelemmel, amely 2015. október 6-án hozott ítéletében érvénytelennek mondta ki a Bizottság 2000/520/EK határozatát, ezzel véget vetve a biztonságos kikötő rendszerének. Az ítélet nem csak az ezt követő adattovábbításra, de a már ott tárolt adatokra is vonatkozik, hiszen a határozatot visszamenőlegesen is érvénytelennek kell tekinteni. (Lehóczki, 2015, pp. 95–98.)

A személyes adatok védelméről szóló COM(2012) 11 rendelet javaslatát négy év vita után, 2016. április 15-én fogadták el a 95/46/EK irányelv felváltására. Az uniós jogalkotó célja ezzel az volt, hogy az adatvédelmet megnehezítő gyors technológiai fejlődésre választ adjon. Az új szabályozás gazdaságilag is fontos, hiszen remények szerint növeli az internetes kereskedelembe vetett bizalmat.

3.4. Az EU kiberteret érintő politikája: több érdekelt bevonása

Az Európai Unió a kibertér szabályozásával kapcsolatban igyekszik minél aktívabb külpolitikát folytatni, és aktívan részt venni a kiberbiztonsággal kapcsolatos nemzetközi diskurzusban. A 2012-es ITU nemzetközi távközlési világkonferencián való részvétel kapcsán a Tanács COM(2012) 430 határozatában úgy fogalmazott, hogy a nemzetközi távközlési szabályozás (ITR) bármely módosítása összhangban kell, hogy legyen az uniós vívmányokkal, és segítenie kell az Unió céljainak elérését. 2014-ben a Tanács következtetései a kiberdiplomáciáról című 9967/4/14. számú dokumentumban sor került a kibetérrel kapcsolatos nemzetközi politika hat uniós pillérének meghatározására. (Dancă 2015, p. 95.) A dokumentumban olyan EU-s értékek jelennek meg, mint az emberi jogok védelme a kibertérben, a hatályos nemzetközi

jog alkalmazása a nemzetközi biztonság területén és a több érdekelt bevonásával működő szabályozási modell támogatása. A Tanács számos célt is megfogalmaz ebben, mint például az EU versenyképességének és jólétének fokozása, a kiberkapacitás-építés és -fejlesztés, valamint a nemzetközi partnerekkel való szorosabb együttműködés.

Intézményi szinten is megfigyelhető ennek a szabályozási modellnek az alkalmazása. Az 526/2013/EU rendelet – felváltva a 460/2004/EK rendeletet – újragondolta az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (European Network and Information Security Agency, ENISA) feladatköreit, és jelentősen kibővítette azokat. Fontos szerep jut a szervezet számára a hálózat- és információbiztonsággal kapcsolatos – mind az uniós szervezetekkel, mind a harmadik országokkal történő – együttműködés kiépítésében. Ennek részeként az ENISA és az Európai Közös Kutatóközpont 2010-ben megtartotta első páneurópai kiberbiztonsági gyakorlatát, a „Kiber Európa 2010"-et, amely a tagállamok közötti szorosabb együttműködést volt hivatott elősegíteni. (Zhang, 2013, p. 124.)

Az Európai Bizottság COM (2012) 140 közleményében beszámolt az Europolon belül egy új szervezet létrehozásáról, amelynek feladata kifejezetten a kiberbűncselekményekkel kapcsolatos bűnüldözési feladatok összehangolása. Ez 2013. január 1-jén kezdte meg működését Hágában Europol Számítástechnikai Bűnözés Elleni Európai Központ (European Cybercrime Centre, EC3) néven. A nyomozásokban való segítségnyújtáson kívül számos más tevékenységet is ellát, így például információt gyűjt, és elemzi a kiberbűnözés alakulását, segít a tagállamoknak a kapacitásépítésben, valamint kapcsolatot teremt a bűnüldöző szervek és a magánszektor, valamint a tudományos élet között. (Buono, 2012, pp. 340–342.) A szervezeten belül működik egy rendőri különítmény is Kiberbűnözés Elleni Közös Munkacsoport (Joint Cybercrime Action Taskforce, J-CAT) néven, amelyben négy unión kívüli ország – Egyesült Államok (FBI, USSS), Kanada, Ausztrália és Kolumbia – is képviselteti magát. Ennek feladata a kulcsfontosságú kiberfenyegetések – így például az online csalás, botnetek és gyermekek szexuális kizsákmányolása – elleni fellépés. (Europol, 2014)

Politikai szinten nagyon lényeges a 2015 áprilisában elfogadott európai biztonsági stratégia (COM (2015) 185.), amely számos kihívás mellett foglal-

kozik a kiberbűnözés elleni fellépéssel is. A dokumentum kiemeli a harmadik országokkal megkötött kölcsönös jogi segítségnyújtási megállapodások fontosságát. Az Uniónak a harmadik államok közül tízzel van stratégiai partneri megállapodása (USA, Kanada, Mexikó, Brazília, Dél-Afrika, India, Kína, Japán, Dél-Korea és Oroszország), amelyek közül az Egyesült Államokkal való együttműködés a kiberbiztonság területén a leginkább elmélyült. (Dancă, 2015, p. 96.) A biztonsági stratégia kiberbűnözéssel foglalkozó fejezete külön nevesíti az EU–USA kiberbiztonsággal és számítástechnikai bűnözéssel foglalkozó munkacsoportot a támogatandó nemzetközi kezdeményezések között. Ennek fontosságát mutatja, hogy az USA-val való együttműködést már a két évvel korábbi kiberbiztonsági stratégia is szorgalmazta, amely az EU legfőbb partnereként tekint az Egyesült Államokra. (Fahey, 2014, p. 47.) Az EU ugyanakkor nem kíván együttműködni sem Kínával, sem Oroszországgal a kiberbiztonság területén, sőt politikailag motivált támadásaik miatt a biztonságot gyengítő tényezőként tekint rájuk. Ennek a hozzáállásnak az egyik oka, hogy az orosz–uniós viszony jelentősen megromlott a kelet-ukrajnai konfliktus kitörése óta. (Dancă, 2015, p. 96.)

3.5. Egyesült Királyság: a különutas politika

Az Egyesült Királyság igen korán nemzeti joga részévé tette a kiberbűnözés elleni fellépést. Az 1990-ben elfogadott számítógépes visszaélésről szóló törvény (*Computer Misuse Act*) három magatartást kriminalizált: engedély nélküli hozzáférés a számítógéphez, engedély nélküli hozzáférés további bűncselekmények elkövetésének szándékával és a számítógépes adatok engedély nélküli módosítása. 2006-ban a rendőrségi és igazságszolgáltatási törvény (*Police and Justice Act*) kisebb mértékben kiegészítette a jogszabály szövegét. 2000-ben fogadták el a vizsgálati hatáskörök szabályozásáról szóló törvényt (*Regulation of Investigatory Powers Act*), melynek rendelkezései szerint az elektronikus kommunikáció határozat nélkül is lehallgatható, amennyiben a résztvevők legalább egyike beleegyezett ebbe. A 2012-ben előterjesztett javaslat a hírközlési adatokról szóló törvényről (*Communications Data Bill*) kötelezte volna a szolgáltatókat arra, hogy 12 hónapra megőrizzék a felhasználók böngészési előzményeit, valamint felhatalmazta az államot arra, hogy monitorozza az internetes kommunikációt, és a mobiltelefonok használóját

azonosító adatokhoz hozzáférhessen. A javaslatot a liberális demokraták élesen ellenezték annak lehetséges alapjogsértő következményei miatt, amely végül nem került elfogadásra. (Levin – Ilkina, 2013, p. 18.) 2015-ben a kormányzó konzervatív párt átdolgozott formában, jóval szigorúbb előírásokkal újra benyújtotta azt. (BBC, 2015) A feladatok ellátásra két specializált szervezetet hoztak létre: a Kiberbiztonsági Irodát (*Office of Cyber Security*) és a Kiberbiztonsági Műveleti Központot (*Cyber Security Operations Centre*). Előbbi a különböző kiberbiztonsági tervek koordinálását, míg utóbbi a jelentősebb kormányzati és nem kormányzati információs rendszerek védelmét látja el. (Zhang, 2013, p. 125.)

Az Egyesült Királyság kiberbiztonsággal kapcsolatos politikáját az teszi különutassá, hogy a kormány a Lisszaboni Szerződést csak jelentős engedmények árán ratifikálta, és ezek között volt az igazságügyi és belügyi együttműködést érintő uniós jogszabályokból való kimaradás lehetősége, amellyel azóta is él. (Egedy, 2013) Másik hasonló engedmény volt annak kimondása, hogy a közös kül- és biztonságpolitikára vonatkozó rendelkezések nem érintik a tagállamok hatásköreit külpolitikájuk kialakításában. Mindezek miatt kijelenthetjük, hogy az Unióból történő kilépésről szóló június 23-i népszavazás eredménye érdemben nem fogja megváltoztatni a kiberbiztonság területén eddig folytatott brit politikát.

2010-ben megszületett a Stratégiai Védelmi és Biztonsági Felülvizsgálat, egy évvel később pedig elfogadták a nemzeti biztonsági stratégiát, amely a terrorizmust, a kibertámadást, a katonai krízist és a természeti katasztrófákat tartja a legjelentősebb biztonsági fenyegetéseknek. (Zhang, 2013, p. 125.) 2011 novemberében pedig nyilvánosságra hozták az ország kiberbiztonsági stratégiáját, amely 2015-ig elérendő célként tűzte ki a kiberbűnözés megállítását; az Egyesült Királyság online érdekeltségeinek határozottabb védelmét; egy nyitott, stabil és színes kibertér létrehozását és az ezek biztosításához szükséges kapacitás kiépítését. A program megvalósítására 650 millió fontot költöttek. Ez jól mutatja, hogy az ország elsősorban a kiberbűnözés letörésében érdekelt – amely felmérések szerint évi 27 milliárd fontos veszteséget okoz a brit gazdaságnak –, és elsősorban erre koncentrál, nem a kibertámadások elleni védekezésre. (Levin – Ilkina, 2013, pp. 16–17.)

Nemzetközi szinten az Egyesült Királyság aktívan részt vesz a kibetér szabályozásáról folyó diskurzusban. 2011-ben David Cameron brit miniszterelnök és Barack Obama amerikai elnök közös közleményt adtak ki a kiberbiztonság terén történő együttműködésről. Eszerint a két ország összehangolja kutatás-fejlesztési tevékenységét, az információtechnológiák fejlődése kapcsán rendszeres együttműködést alakít ki a kapacitásépítésben résztvevő szervek között, a kiberbűnözés elleni fellépéshez szükséges eszközök számát növeli, a magánszektorral és a kereskedelmi partnerekkel szoros együttműködést hoz létre. További fontos pont még, hogy az Egyesült Királyság bejelentette csatlakozását a Budapesti Egyezményhez, és kifejezte szándékát annak ratifikációjára. (www.gov.uk, 2011) Az együttműködések terén érdemes továbbá megemlíteni az Egyesült Királyság-Kína Internet Keresztasztalt, amelynek célja a kommunikáció erősítése és a közös bizalom kiépítése. Szemben tehát az EU-val, az Egyesült Királyság partnerként tekint Kínára. (Zhang, 2013, p. 125.)

3.6. Oroszország

Oroszország gyakran a legnagyobb hackerpopulációval rendelkező országként élt a köztudatban. Olyan támadások fűzhetők oroszok nevéhez, mint az 1995-ös Levin-ügy, amelynek során mintegy hárommillió dollárt loptak el az amerikai Citibank ügyfeleitől. (Warren – Streeter, 2005, pp. 41–42) De hasonlóan nagy visszhangot váltott ki a Target amerikai cégcsoport rendszereibe történő 2013-as betörés, amely szintén az Orosz Föderációból indult ki. (McDougal, 2015, p. 55.) Az orosz hackerek nagy száma azonban nem véletlen: a hidegháború vége felé a hírhedt KGB számos számítógépes specialistát képezett ki, illetve használt fel a COCOM-listán szereplő nyugati szoftverek illegális beszerzése érdekében. A keleti blokk felbomlása után sok, ilyen kapcsolatokkal rendelkező volt államvédelmi ügynök csatlakozott a szervezett bűnözéshez. (Warren – Streeter, 2005, pp. 121–122)

Az orosz jogrendszer a kiberbűncselekmények esetén a szövetségi szerveknek biztosít elsőbbséget és általános illetékességet, míg a helyi adminisztráció csak korlátozott jogkörökkel bír. (Borisevich et al., 2012, p. 278.) Az 1996-os büntetőtörvénykönyv 272. szakasza bünteti a számítógépes információhoz való illetéktelen hozzáférést. A törvények védik a szellemi alkotásokat, és a Btk. komoly büntetéseket tartalmaz ezek megsértésének esetére. Ettől is

súlyosabb büntetés jár abban az esetben, ha valaki kártékony programokat terjeszt az interneten. A probléma gyökerei nem a törvényekben, hanem azok betartatásában keresendők: az orosz rendőrség gyakran hezitál fellépni az ilyen ügyekben, és ha meg is teszik, akkor is gyakran igen alacsony büntetéseket szabnak ki a bíróságok. (McDougal, 2015, pp. 56–58.) Egyes orosz régiókban a látencia mértéke az információkhoz való illetéktelen hozzáférés esetén meghaladhatja a 80%-ot is. (Borisevich et al., 2012, p. 285.)

A felderítésért a Belügyminisztérium „K" osztálya felelős, amelynek adatai alátámasztják a növekvő számú elkövetést. 2012 első felében 5956 kiberbűncselekmény ügyében indult nyomozás, amely 11%-kal több az előző év hasonló időszakához képest. A Group-IB orosz biztonságtechnikai cég szerint a fentebb említett okokon kívül ebben az is közrejátszik, hogy az egyes csoportok együttműködnek egymással a minél nagyobb profit érdekében. Ugyanakkor az orosz hatóságok keményen fellépnek a gyermekpornográfiával szemben: 2011-ben a „szornyak" (сорняк) névre keresztelt akció során szerzett bizonyítékok alapján 131 büntetőeljárás indult meg. A program eredményeként egy 24 országot magában foglaló együttműködés jött létre. A 2000-ben született Orosz Föderáció Információbiztonsági Doktrínája a kibertámadásoktól való védelmet tekinti elsődleges célnak. (Levin – Ilkina, 2010, pp. 30-31.)

Akárcsak más államokban, az orosz hadseregnek is van kiberháborúra szakosodott hadereje, amely azonban a kémkedés helyett inkább katonai célok elérése fókuszál. Nyugati vélemények szerint ők voltak felelősek az Észtország ellen 2007-ben ért kibertámadásokért, a 2008-as orosz–grúz konfliktus során grúz kormányzati weboldalakat elérhetetlenné tevő, és a 2014 óta tartó ukrán válság során az ukrán kormány elleni akciókért. (Muir, 2014, pp. 78–79.) Oroszország azonban ezen esetekben tagadta az érintettségét, és egyszerű internetes aktivisták tevékenységének tudta azt be. Ugyanakkor semmiféle hajlandóságot nem mutatott abban, hogy az észt hatóságokkal együttműködve felkutassa az elkövetőket. (Jensen, 2015, p. 278.) A 2010-ben született új katonai doktrína egyértelműen a hadsereg feladatának tartja a kiberbiztonság biztosítását, valamint jelentős katonai fenyegetésként értékeli az ország információs infrastruktúrája elleni támadásokat. (Levin – Ilkina, 2010, p. 31–32.)

Oroszország a nemzetközi színtéren nyíltan támogatja a nemzeti szuverenitáson alapuló szabályozás szükségességét. Az ITU 2012-es világkonferen-

ciáját megelőzően, 2011 júniusában Vlagyimir Putyin miniszterelnök kijelentette, hogy országának célja az, hogy a szervezeten keresztül nemzetközi irányítás alá vonja az internetet. (Eichensehr, 2015, p. 332.) Bár az ország már hosszú ideje Kína szövetségese az internetszabályozás nemzetközi kérdéseiben a hasonló célok miatt, Muir rámutat, hogy közöttük az együttműködés korántsem problémamentes. A két ország között régóta vannak geopolitikai feszültségek (például Szibéria hovatartozását illetően), és az egyéb politikai kérdések körüli viták a kibertér kapcsán folyó együttműködést is ellehetetleníthetik. A szerző véleménye szerint, mivel a Krím-félsziget annektálását követő nyugati szankciók még jobban kiszolgáltatták az orosz gazdaságot Kínának, az oroszok érdekeltek lehetnek a kínaiak meggyengülésében. (Muir, 2014, pp. 88–90) A 2015-ben kötött orosz-kínai bilaterális kiberegyezmény megkötése azonban azt mutatja, hogy ezek a törésvonalak korántsem olyan jelentősek a két ország között.

4. Ázsia

4.1. Kína modellje: az ellenőrzés elsődlegessége

Kelet-Ázsia legnagyobb és a világ második legnagyobb gazdaságaként Kína kibertérre alkalmazott szabályozásának áttekintése különösen fontos. A kínai modell régóta áll tudományos kutatások fókuszában, a nyugati szerzőket elsősorban az ország által alkalmazott szigorú szabályok és az információáramlást gátló, illetve annak ellenőrzésére szolgáló rendszerek érdeklik elsősorban. (Lee, 2014, p. 953.) Austin három időszakra osztja Kína kibertérrel kapcsolatos politikáját: a 2005-ig tartó lassú kezdetet a kiberháborút középpontba helyező elképzelés követte, és 2014 februárjától tör az ország a Xi Jiping elnök által „kiberhatalom"-nak nevezett státuszra. (Austin, 2016, p. 171.)

Az ország a Nyugatnál jóval később, csak az ezredforduló környékén ismerte fel az internet hatalmas gazdasági jelentőségét, és 1994-ben indultak meg a fejlesztések. (Gao, 2011, p. 353.) Emellett nagy szerepet játszott a döntésben annak rossz emléke is, hogy Kína milyen súlyosan meggyengült a XX. századra az ipari fejlesztések elhanyagolása miatt. Ekkor indult a kínai internethasználók száma robbanásszerű növekedésnek, ami az 1997-es egymilliós számról

2001-re huszonkét millióra nőtt. (Hachigian, 2001) Ez a tendencia a China Internet Network Information Center (2015) éves felmérései alapján tovább folytatódik napjainkig is: 2005-ben 111 millió, 2010-ben 457 millió, 2015 elején 649 millió kínai rendelkezett internethozzáféréssel, mely utóbbi a teljes lakosság 49%-át jelenti. Bár ez a lakosságszámhoz viszonyítva arányaiban kevésnek tűnhet, a látszat csal, hiszen már majdnem annyi kínai használja az internet lehetőségeit, mint ahányan az EU-ban és az Egyesült Államokban együttvéve. Ez a világ legnagyobb digitális piacává teszi az országot, ahogy azt már évekkel korábban megjósolták. (Blythe, 2007, p. 1.)

Az internet kínai térhódításánál az államot vezető Kínai Kommunista Párt (CPC) kezdettől fogva ügyelt arra, hogy politikai vezető szerepét biztosítsa. Az új, erősen decentralizált médiát jóval nehezebb ellenőrizni, mint a tradicionális kommunikációs csatornákat. A kormányzat központi, tartományi és helyi szervei ezek ellenére támogatták az internetelérés folyamatos kiterjesztését. (Hachigan, 2001) Az évek során számos olyan jogszabály született, amely a politikai helyzet fenntartását szolgálja. A 33/1997. sz. közbiztonsági minisztériumi rendelet például felsorolja, milyen típusú információkat tilos létrehozni, másolni, keresni és terjeszteni az interneten, és a kilenc elemből álló felsorolás többsége politikai bűncselekményt takar (pl. a szocialista államrend megdöntésére irányul). (Gao, 2011, p. 355.)

Ezen szabályok betartatására a CPC-nek a világ legkifinomultabb, internet ellenőrzésre szolgáló rendszerét sikerült kiépítenie, ami véget vetett azon nyugati reményeknek, hogy az internet elterjedése Kínában a többpártrendszeri változások fontos elősegítője lesz. (Lee – Liu, 2012, p. 127.) Kínában a tartalom szűrése a gyakran nagy tűzfalnak is nevezett Aranypajzs projekt keretei között történik. Az internetszolgáltatók szerepe ebben a rendszerben elsősorban formális, és csak az infrastuktúra működtetésére terjed ki. 2009-ben ennek kiegészítésére előírták, hogy minden számítógép otthoni szűrő szoftverrel együtt kerüljön értékesítésre, amely a gyermekeket hivatott megvédeni a központilag nem kívánatosnak ítélt szexuális, vallási és politikai tartalmaktól. A rendelkezés nagy tiltakozást váltott ki, így végül elálltak a tervtől. (Parti, 2010, p. 99.)

A kínai kormányzat is hamar felismerte a nemzetközi együttműködés szükségességét a kibertéren fenyegető új kihívások leküzdésében, és ezzel kapcsolatban saját elképzelést dolgozott ki. Ez különösen azért fontos számukra,

mert a nyugati szabályozást egyfajta kiberhegemóniaként értékelik, amely közvetlenül veszélyezteti a CPC hatalmát. (Gady, 2014) Mint Austin rámutat, bár Kína normameghatározó ország szeretne lenni a nemzetközi színtéren, jelenleg elsősorban csak normakövető szerepet játszik. (Austin, 2016, p. 172.) Jól mutatja a kínai elképzelést a szuverén államok szabályozásban betöltött szerepéről az a nyilatkozat, amely szerint csak ezeknek „van meg a felelősségük és joguk ahhoz, hogy megtegyék a szükséges intézkedéseket a honi kibertér és a kapcsolódó infrastruktúra fenyegetésektől, zavaroktól, támadásoktól és szabotázstól való védelme érdekében." (Jensen, 2015, p. 297.)

A Sanghaji Együttműködési Szervezet tagállamai államfőinek 2007-es találkozóján közös akciótervet fogadtak el, amelyben megállapodtak azokról az alapelvekről, amelyeket a számítógépes rendszerekkel szembeni kibertámadások elleni fellépésben kívánnak alkalmazni. A fő különbség a Kína, Oroszország, Kazahsztán, Kirgizisztán, Tádzsikisztán és Üzbegisztán által elfogadott dokumentum és a Budapesti Egyezmény között, hogy ez a részes államok számára teljes rendelkezési jogot biztosít a rendszerek és a bennük tárolt adatok felett, beleértve a politikailag veszélyesnek ítélt tartalmak elleni fellépés lehetőségét. (Sofaer – Clark – Diffie, 2010, p. 186.) 2014-ben Kína – a nemzeti szuverenitáson alapuló szabályozási elképzelése népszerűsítése érdekében – Wuzhenben megrendezte első internetes világkonferenciáját. Ennek hivatalos dokumentumában, a wuzheni kiáltványban megpróbálták meggyőzni a nyugati megjelenteket a kínai elképzelések helyességéről, de az álláspontok nem közeledtek egymáshoz. (Gady, 2014)

2015-ben a Sanghaji Együttműködési Szervezet tagjai módosították a korábbi nemzetközi magatartási szabályokra vonatkozó javaslatukat, amelyben megerősítették, hogy az államok szuverén joga politikai döntéseket hozni az internettel kapcsolatos közpolitikai kérdésekben. Egyúttal előírták, hogy minden részes állam köteles más államok szuverenitását, területi integritását és politikai függetlenségét tiszteletben tartani. Ez egyértelműen jelzi, hogy a nevezett államok által kívánatosnak tartott internetszabályozás a kormány ellenőrzése alatt áll. (Jong-Chen, 2015) Az ország 2015-ben bilaterális egyezményt is kötött Oroszországgal az információbiztonsággal kapcsolatos kérdésekről, amely a szoros együttműködés és információcsere mellett politikai jellegű kérdéseket is tartalmaz, így pl. a nemzetközi szervezetekben a szabá-

lyozással kapcsolatos hasonló elképzelések előmozdítását. (Kulikova, 2015) Alekszandr Szalinkov, az Információbiztonsági Intézet vezetője szerint az egyezmény szövege 70%-ban megegyezik a sanghaji együttműködés részeként elfogadott korábbi dokumentuméval, és az újdonság benne a belső szuverenitás védelmének fontosságát taglaló rész. (Roth, 2015) A nyugati elemzők szerint az elfogadásának oka az eddigi együttműködés megerősítése volt, amelynek végső célja a nemzeti szuverenitáson alapuló internetszabályozás multilaterális elfogadtatása. Austin egyúttal rámutatott, hogy az egyezmény 4. cikke nem tiltja a feleknek az egymással szembeni kiberkémkedést és a kiberháborús készülődést. (Gady, 2015) Mivel a szöveg az információs infrastruktúrát érő „jogellenes" beavatkozásokat zárja ki, ez úgy értelmezhető, hogy a tilalom csak békeidőre szól. (Austin, 2016, p. 178.) Akárcsak az orosz-kínai, az amerikai-kínai egyezmény sem tiltja az államtitkok megszerzésére irányuló internetes kémkedést. Ugyanakkor különbséget jelent, hogy az utóbbi tilalmazza a szellemi tulajdon és a kereskedelmi titkok kikémlelését.

Ugyanakkor Austin egy 2014-es amerikai jelentés alapján azon a véleményen van, hogy az eltérő alapkoncepciók ellenére számos kérdésben több a hasonlóság a kínai és az orosz megközelítésben, mint a különbség. Így például Kína támogatja a belügyekbe történő beavatkozás tilalmának kiterjesztését a kibertérre, valamint az internetszabályozás demokratizálását, amely megszüntetné az USA jelentős befolyását a domainnevek elosztását intéző ICANN-ben. A két ország véleménye megegyezik az állami felelősség szabályainak, a háborúindítás jogának és a hadijognak a kibertérben történő alkalmazásában is. (Austin, 2016, p. 176.)

4.2. Dél-Korea

Világviszonylatban Dél-Korea lakossága rendelkezik a legnagyobb arányú szélessávú internetelléréssel. (Leitner, 2009, p. 84) Szabályozásának sajátos jellegét az adja, hogy a koreai háború 1953-as fegyverszüneti lezárása óta nem tudott békeszerződést kötni északi szomszédjával. Utóbbi nem csak konvencionális és – egyes feltételezések szerint – nukleáris fegyverekkel jelent fenyegetést az országra, de a kibertérben is. Észak-Korea internetes kapacitását mutatja, hogy nem csak dél-koreai állami intézmények és hadsereg rendszerei,

de az északi vezetőről paródiafilmet készítő Sony ellen is sikerrel hajtottak végre támadást, jelentős kárt okozva a cégnek. Déli becslések szerint az ország a harmadik legnagyobb kiberháborús támadóerővel rendelkezik a világon. Ugyanakkor tompítja ezt az, hogy gyengén kiépített internetes infrastruktúrája miatt ennek az apparátusnak más államok hálózataira és botnetjeire van szüksége akciói végrehajtásához, ez pedig jelentősen behatárolja mozgásterüket. (Siers, 2014)

Dél-Korea azért is különleges, mert az internetes névtelenség kapcsán igen sajátos szabályozást vezetett be. A nyugati típusú demokráciák általában támogatják az anonimitást, mint például az Európa Tanács 2003-as, az internetes kommunikáció szabadságáról szóló deklarációjában vagy az Egyesült Államok Legfelsőbb Bírósága több ítéletében. 2007-ben azonban ezzel ellentétes szabályozás mellett foglalt állást Dél-Korea kormánya, ahol világviszonylatban is egyedülálló megoldásként az Információs és Kommunikációs törvény módosításával bevezetésre került az ún. „valódi nevet igazoló rendszer". Ezzel létrejött a nyugati demokratikus országok közül a leginkább korlátozó jellegű rendszer.

Lényege az volt, hogy a leglátogatottabb – kezdetben minden napi háromszázezernél, később minden napi százezernél több egyedi látogatóval rendelkező – weboldalat üzemeltető szolgáltatót köteleztek arra, hogy az őket felkereső felhasználókat egy közintézmény honlapjára irányítsák, ahol személyi igazolványszámuk segítségével azonosítaniuk kellett magukat, mielőtt tartalmat tehettek közzé. Az adatokat megőrizték, hogy egy esetleges későbbi büntetőeljárás során felhasználhassák őket. (Leitner, 2009, pp. 84.) A szabályozás szigorúsága összefüggött politikai tényezőkkel, így elsősorban a 2008-as Egyesült Államok elleni tüntetéssel, amelynek oka az amerikai marhahús importtilalmának feloldása volt. Az ekkori online tiltakozások szolgáltattak okot arra, hogy a törvény hatályát jelentősen kiterjesszék. (Leitner, 2009, pp. 92.) Politikailag motivált cenzúrára már korábban is volt példa az országban: a Nemzetvédelmi Törvény kriminalizálja az államellenes véleménynyilvánítást, például Észak-Korea nyilvános dicséretét vagy támogatását. Ezen rendelkezés alapján 2004-ben 31 északpárti weboldalt blokkoltak az országban, amelynek következtében azonban több ezer vétlen honlap is elérhetetlenné vált. (Leitner, 2009, p. 95.)

2012-ben a dél-koreai Alkotmánybíróság megsemmisítette a jogszabályi rendelkezést. Véleményük szerint a valós adatok felfedése előzetes cenzúrához vezetett, súlyos beavatkozást jelentett a felhasználók magánéletébe – hiszen ez alapján visszakövethető volt, mely weboldalakat látogatják –, és egyúttal szükségessége sem nyert bizonyítást, mivel a rendszer nehezen betartatható és kevéssé hatékony volt. A szabályozás egyéb buktatói már korábban kiderültek, így például az összegyűjtött és tárolt adatok védelmének nehézségei, hogy ahhoz illetéktelenek ne férjenek hozzá, illetve a rendszer fenntartásának magas költsége. (Ramstad, 2012)

5. Összefoglalás

Mint az előzőekben bemutattam, számos elképzelés létezik a kibertér szabályozásával kapcsolatos kérdésekben, egymástól különböző mértékű eltérésekkel. Két modell képe rajzolódik ki előttünk: a Nyugat által támogatott több érdekelt bevonásával működőé, valamint a Kína és Oroszország által forszírozott nemzeti szuverenitás alá rendelőé. Előbbi rendszerben az állam a keretet és a kényszerítőerőt biztosítja az internet biztonságában érdekeltek számára, míg a szabályozásban nagy teret kapnak az ágazat szereplői, valamint pontosan szabályozott a katonai felhasználás is. Utóbbi rendszerben az államhatalom monopóliummal bír az internetszabályozás minden kérdésében – különösen a tartalomszabályozásban –, a szolgáltatók és más szereplők pedig csupán a központi hatalom végrehajtóiként jelennek meg. Ezt a rendszert nevezik multilaterálisnak is, mivel az államok között kötött szerződéseken alapulnak a keretei, a katonai felhasználás pedig nem szabályozott vagy részben nem megengedett. (Eichensehr, 2015, p. 321) Mindkét szabályozásnak megvannak a maga előnyei és hátrányai, így például a több érdekelt bevonásával működő rendszer ugyan nagyobb információszabadságot biztosít, másrészről viszont a lobbitevékenység erősen érvényesül a kialakításában és a kiberbiztonság is sokkal nehezebben megvalósítható.

Ezen különbségek a nemzetközi dokumentumokban és diplomáciában is tetten érhetőek. A nemzeti szuverenitás alapú szabályozás pártján állók olyan megoldást támogatnak, amely a többnyire amerikai érdekeltségű nem kor-

mányzati szervek helyett a nemzetközi szervezeteknek – és így az azokban részes államoknak – biztosít nagyobb befolyást. Egy ilyen megoldás azonban elfogadhatatlan a másik modell követői számára, hiszen nem az együttműködésen alapul, hanem vertikális irányítást valósít meg. A 2001-es Budapesti Egyezmény számukra nemcsak a nyugati értékek támogatása miatt vonzó, de azért is, mert csak a szabályozás közös minimumát adja meg, annak kivitelezését pedig az egyes részes államok körébe utalja. Az Egyesült Államok és az Európai Unió folyamatos támogatásának köszönhetően az Egyezmény még sokáig az együttműködés alapját fogja képezni a nyugati államok között. Vagy, ahogy Ian Walden professzor fogalmazott Dublinban: ez marad Az Egyezmény.

Ezen indokok mellett az egyes államok politikai érdekeinek ismerete is fontos az eltérések megértéséhez. Ezek nemcsak aktuálpolitikai jellegűek, hanem mélyebben gyökereznek: egy pontos keretekkel rendelkező szabályozás nemcsak az érdekérvényesítő képességének korlátozása és a Five Eyes-hoz hasonló kezdeményezések megnehezítése miatt nem szimpatikus az Egyesült Államoknak, de az angolszász jogi tradícióknak megfelelő informális együttműködést is ellehetetlenítené. Ezzel szemben a minden érdekelt bevonásának megvalósítása kikezdené a CPC gondosan körbebástyázott hatalmát Kínában. Rajtuk kívül sok ingadozó állam is akad, például India, amely sokáig a nyugati elképzelést támogatta, de újabban szembefordult ezzel, ami jól tetten érhető az ITU puszani meghatalmazotti konferenciáján benyújtott javaslatukban. (Eichensehr, 2015, p. 335.)

A fentebb részletezett modellek azonban ritkán érvényesülnek tisztán. A nyugati demokratikus és autoriter megoldások sok területen – mint például a tartalomszűrés terén – lassú közeledést mutatnak egymáshoz, hiszen sok helyen az állami büntetőjogi igény érvényesítése céljából szélesebb körben alkalmazni kezdték az állami szűrést. (Parti, 2010, p. 99.) A felosztást árnyalja, hogy míg Kína mellett Nagy-Britannia is a kiberbűnözés elleni fellépést tekinti prioritásnak, addig a többi nyugati állam és Oroszország a kibertámadásokkal szembeni védekezést. (Levin – Ilkina, 2010, p. 35.)

Véleményem szerint ezen jogi és politikai okok miatt nem várható a közeljövőben konszenzus a két modell követői között, ugyanakkor a gyakorlat azt mutatja, hogy lassan zajlik az arra érdemesnek tartott megoldások átvétele

egymástól. Amíg a mostanihoz hasonló együttműködés van a modellek jelentős képviselői között, addig ez a folyamat biztosan folytatódni fog.

Irodalomjegyzék

Könyvek

WARREN, Peter – STREETER, Michael (2005): Az internet sötét oldala. Budapest, HVG. 256 p. ISBN 963-7525-815

Könyvrészletek

AUSTIN, Greg (2016) International Legal Norms in Cyberspace: Evolution of China's National Security Motivations. In: OSULA, Anna-Maria – RÕIGAS, Henry. International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn, NATO CCD COE. p. 171–201. ISBN 978-9949-9544-7-6

BRENNER, Susan W. (2011) Cybercrime Law – A United States Perspective. In: CASEY, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. USA, Academic Press. p. 85–122. ISBN 978-0-12-374268-1

CHALMERS, Damian (2014) Eu Criminal Law. In: CHALMERS, Damian – DAVIES, Gareth – MONTI, Giorgio. European Union Law: Cases and Materials. New York, Cambridge University Press. p. 581–629. ISBN 978-0-521-12151-4

DORNFELD, László (2015) A kiberbűncselemények szabályozásának története az Egyesült Államokban és Európában. In: SZABÓ Miklós. Studia Iurisprudentiae Doctorandorum Miskolciensium. Tomus 16. Miskolc, Gazdász-Elasztik Kft. p. 67–86. ISSN 1588-7901

PEERS, Steve (2011) EU Justice and Home Affairs Law. In CRAIG, Paul – DE BÚRCA, Gráinne. The Evolution of EU Law. New York, Oxford University Press. p. 269–298. ISBN 978-0-19-959296-5

SOFAER, Abraham D. – CLARK, David – DIFFIE, Whitfield (2010) Cyber Security and International Agreements. In: CLARK, David. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and

Developing Options for U.S. Policy. Washington D. C., The National Academies Press. p. 179–206. ISBN 978-0-309-16035-3

Folyóiratcikkek

BARTÓKI-GÖNCZY, Balázs (2014) Towards a Single Market for Telecoms. European Networks Law and Regulation Quarterly, 2. évf. 3. sz., p. 3–16. ISSN 2197-4454

BLYTHE, Stephen E. (2007) China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of e-Commerce. Chicago-Kent Journal of Intellectual Property, 7. évf. 2. sz., p. 1–32. ISSN 1559-9493

BORISEVICH, Galina – CHERNYADYEVA, Natalya – FROLOVICH, Evelina – PASTUKHOV, Pavel – POLYAKOVA, Svetlana – DOBROVLYANINA, Olga – GRIFFITH Keeling, Deborah – LOSAVI, Michael M. (2012): A Comparative Review of Cybercrime Law and Digital Forensics in Russia, the United States and Under the Convention on Cybercrime of the Council of Europe. Northern Kentucky Law Review, 39. évf. 2. sz., p. 267–326. ISSN 0198-8549

BUONO, Laviero (2012) Gearing Up the Fight Again Cybercrime in the European Union: A New Set of Rules and Establishment of the European Cybercrime Centre (EC3). New Journal of European Criminal Law, 4. évf. 3. sz., p. 332–343. ISSN 2032-2844

CROOK, John R. (2010) Secretary of State Addresses Human Rights and the Internet. The American Journal of International Law, 104. évf. 2. sz., p. 291–294. ISSN 0002-9300

DANCĂ, Dana (2015) Cyber Diplomacy – A New Component of Foreign Policy. Journal of Law and Administrative Sciences, 2. évf. 3. sz., p. 91–97. ISSN 2392-8298

EGEDY Gergely (2013) Brit kilépés? Polgári Szemle, 9. évf. 1–3. sz., ISSN 1786-6553

EICHENSEHR, Kristen E. (2015) The Cyber-Law of Nations. Georgetown Law Journal, 103. évf. 2. sz., p. 317–380.

ELLIS, Mark S. (2014) Losing Our Right to Privacy: How Far is Too Far? Birkbeck Law Review, 2. évf. 2. sz., p. 173–190. ISSN 2052-1316

ERDŐS István (2014) Az elektronikus kereskedelem hatása Az Európai Unió fogyasztói szerződésekkel kapcsolatos egyes joghatósági szabályainak alakulására. Iustum Aequum Salutare, 9. évf. 2. sz., p. 81–94. ISSN 1787-3223

FAHEY, E. (2014) The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security. European Journal of Risk Regulation, 5. évf. 1. sz., p. 46–60. ISSN 1867-299X

FISH, Eric (2009) Is Internet Censorship Compatible with Democracy? Legal Restrictions of Online Speech in South Korea. Asia-Pacific Journal on Human Rights and the Law, 10. évf. 2. sz., p. 43–96. ISSN 1388-1906

GAO, Henry (2011) Google's China Problem: A Case Study on Trade, Technology and Human Rights under the GATS. Asian Journal of WTO & International Health Law and Policy, 6. évf. 1. sz., p. 351–387. ISSN 1819-5164

HACHIGIAN, Nina (2001) China's Cyber-Strategy. Foreign Affairs, 80. évf. 2. sz., p. p. 118–133. ISSN 0015-7120

JENSEN, Eric Talbot (2015) Cyber Sovereignty: The Way Ahead. The Texas International Law Journal, 50. évf. 2. sz., p. 275–304. ISSN 0163-7479

LEE, Jyh-An – LIU, Ching-Yi (2012) Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China. Minnesota Journal of Law, Science & Technology, 13. évf. 1. sz. p. 125–151. ISSN 1552-9533

LEE, Jyh-An (2014) The Red Storm in Uncharted Waters: China and International Cyber Security. University of Missouri – Kansas City Law Review, 82. évf. 4. sz. p. 951–966. ISSN 0047-7575

LEHÓCZKI Balázs (2015) Európai Bíróság: Az Egyesült Államok „biztonságos kikötő" adatvédelmi rendszere nem biztosítja az uniós polgárok alapjogainak tiszteletben tartását. Acta Humana, 3. évf. 6. sz., p. 93–98. ISSN 0866-6628

LEITNER, John (2009) Identifying the Problem: Korea's Initial Experience with Mandatory Real Name Verification on Internet Portals. Journal of Korean Law, 9. évf. 4. sz., p. 83–85. ISSN 2213-4476

MCDOUGAL, Trevor (2015) Establishing Russia's Responsibility for Cyber-Crime Based on Its Hacker Culture. International Law & Management Review, 11. évf. 2. sz., p. 55-80. ISSN 1555-5070

MESTER Máté (2012) Hálózatsemlegesség az Európai Unióban: veszélyben az internet? Infokommunikáció és Jog, 9. évf. 51. sz., p. 149–154. ISSN 1786-0776

MOORE, Stephen (2013) Cyber Attacks and the Beginnings of an International Cyber Treaty. North Carolina Journal of International Law and Commercial Regulation, 39. évf. 1. sz., p. 224–257. ISSN 0743-1759

MUIR, Lawrence L. (2014) Combatting Cyber-Attacks Through National Interest Diplomacy: A Trilateral Treaty with Teeth. Washington and Lee Law Review Online, 71. évf. 1. sz., p. 73–106. ISSN 0043-0463

NULL, Eric (2011) The Difficulty with Regulating Network Neutrality. Cardozo Arts & Entertainment Law Journal, 29. évf. 2. sz., p. 459–493. ISSN 0736-7694

PARTI Katalin (2010) „10 dolog, amit utálok benned", avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán. Infokommunikáció és Jog, 7. évf. 38. sz., p. 97–103. ISSN 1786-0776

ROSENZWEIG, Paul (2012) The International Governance Framework for Cybersecurity. Canada-United States Law Journal, 37. évf. 2. sz., p. 405–414. ISSN 0163-6391

SIERS, Rhea (2014) North Korea: The Cyber Wild Card. Journal of Law & Cyber Warfare, 3. évf. 4. sz., p. 1–12.

SIPOS Zoltán (2016) A kibertér biztonságával kapcsolatos alapvető kérdések áttekintése. Honvédségi Szemle, 144. évf. 1. sz., p. 27–36. ISSN 1216-7436

WALDEN, Ian (2004) Harmonising Computer Crime Laws in Europe. European Journal of Crime, Criminal Law & Criminal Justice, 12. évf. 2. sz. p. 321–336. ISSN 0928-9569

WALTHALL, Howard (2010) The New Neutrality Debate: An IP Perspective. Landslide, 3. évf. 1. sz., p. 21–25. ISSN 1942-7239

ZHANG, Xinbao (2013) Establishing Common International Rules to Strengthen the Co-Operation of Cyber Information Security. China Legal Science, 12. évf. 1. sz., p. 121–139. ISSN 2095-4867

Elektronikus tartalmak

ACTIONPLAN (2011) Beyond the Border;

Letöltve: http://actionplan.gc.ca/en/content/beyond-border (Utolsó letöltés: 12/01/2015)

ASEAN (2008) EU-ASEAN Workshop on Cybercrime Legislation in the ASEAN Member States;

http://www.asean.org/uploads/archive/apris2_old/file_pdf/Press%20Releases/EU-ASEAN%20Workshop%20on%20Cybercrime%20Legislation%20in%20the%20ASEAN%20Member%20States.pdf (Utolsó letöltés: 14/06/2016)

BBC (2015) Theresa May says ‚contentious' parts of web surveillance plan dropped;
Letöltve: http://www.bbc.com/news/uk-34691956 (Utolsó letöltés: 19/02/2015)

CHINA INTERNET NETWORK INFORMATION CENTER (2015) Statistical Report on Internet Development in China;
Letöltve: http://www1.cnnic.cn/IDR/ReportDownloads/201507/P020150720486421654597.pdf (Utolsó letöltés: 04/01/2016)

CONGRESS (2016) H.R.275 – Global Online Freedom Act of 2007;
Letöltve: https://www.congress.gov/bill/110th-congress/house-bill/275/actions (Utolsó letöltés: 14/05/2016)

COUNCIL OF EUROPE (2016) Trainings on cybercrime and electronic evidence;
Letöltve: http://www.coe.int/en/web/cybercrime/trainings (Utolsó letöltés: 14/06/2016)

DICKINSON, Samantha (2014) How will internet governance change after the ITU conference?
Letöltve: http://www.theguardian.com/technology/2014/nov/07/how-will-internet-governance-change-after-the-itu-conference (Utolsó letöltés: 04/03/2016)

ELECTRONIC EVIDENCE (2016) Electronic Evidence Guide;
Letöltve: http://ic4mf.org/wp-content/uploads/2013/11/2ndDay-p08-2013-11-07-COE-Electronic-Evidence-Guide-IC4MF.pdf (Utolsó letöltés: 12/06/2016)

EUROPOL (2014) Joint Cybercrime Action Taskforce (J-CAT)
Letöltve: https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat (Utolsó letöltés: 15/01/2016)

EUROSTAT (2015) Information society statistics – households and individuals;
Letöltve: http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals (Utolsó letöltés: 10/01/2016)

FIDLER, David P. (2012) The Internet, Human Rights, and U.S. Foreign Policy: The Global Online Freedom Act of 2012;

Letöltve: https://www.asil.org/insights/volume/16/issue/18/internet-human-rights-and-us-foreign-policy-global-online-freedom-act (Utolsó letöltés: 29/02/2016)

GADY, Franz-Stefan (2014) The Wuzhen Summit and Chinese Internet Sovereignty;

Letöltve: http://www.chinausfocus.com/peace-security/the-wuzhen-summit-and-chinese-internet-sovereignty/ (Utolsó letöltés: 10/06/2016)

GADY, Franz-Stefan (2015) Have China and Russia Agreed Not to Attack Each Other in Cyberspace?;

Letöltve: http://thediplomat.com/2015/05/have-china-and-russia-agreed-not-to-attack-each-other-in-cyberspace/ (Utolsó letöltés: 10/06/2016)

GOV.UK (2011) US – UK cyber communique; Letöltve: https://www.gov.uk/government/publications/us-uk-cyber-communique (Utolsó letöltés: 04/03/2016)

GOVTRACK (2016) H.R. 275 (110th): Global Online Freedom Act of 2007;

Letöltve: https://www.govtrack.us/congress/bills/110/hr275 (Utolsó letötés: 14/05/2016)

GRISBY, Alex (2015) Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?

Letöltve: http://blogs.cfr.org/cyber/2015/01/28/will-china-and-russias-updated-code-of-conduct-get-more-traction-in-a-post-snowden-era/ (Utolsó letöltés: 10/06/2016)

HOMELAND SECURITY (2011) United States and India Sign Cybersecurity Agreement;

Letöltve: https://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement (Utolsó letöltés: 12/01/2016)

INTERNET GOVERNANCE (2012) ITU Phobia: Why WCIT was derailed;

Letöltve: http://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/ (Utolsó letöltés: 28/02/2016)

INTERNET SOCIETY (2011) Background: International Telecommunication Regulations

Letöltve: http://www.internetsociety.org/background-international-telecommunication-regulations (Utolsó letöltés: 21/02/2016)

JONG-CHEN, Jing de (2015) Spotlight on Cyber V: Data Sovereignty, Cybersecurity and Challenges for Globalization;
Letöltve: http://journal.georgetown.edu/data-sovereignty-cybersecurity-and-challenges-for-globalization/ (Utolsó letöltés: 15/01/2016)
KULIKOVA, Alexandra (2015) China-Russia Cyber-security Pact: Should the US be Concerned?;
Letöltve: http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned (Utolsó letöltés: 04/03/2016)
LAKNER Dávid (2016) Amit az üzenőfal elbír – Cenzorszerepben a Facebook?;
Letöltve: http://mno.hu/media/amit-az-uzenofal-elbir-cenzorszerepben-a-facebook-1345499 (Utolsó letöltés: 12/06/2016)
LAMUT, Anna (2008) Third Circuit Holds Child Online Protection Act Unconstitutional;
Letöltve: http://jolt.law.harvard.edu/digest/internet/aclu-v-mukasey (Utolsó letöltés: 12/06/2016)
LEVIN, Avner – ILKINA, Daria (2013) International Comparison of Cyber Crime; Letöltve: http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf (Utolsó letöltés: 10/01/2016)
NPR (2016) U.S. Appeals Court Upholds Net Neutrality Rules In Full;
Letöltve: http://www.npr.org/sections/thetwo-way/2016/06/14/471286113/u-s-appeals-court-holds-up-net-neutrality-rules-in-full (Utolsó letöltés: 15/06/2016)
POPESCU, Adam (2012) 5 Reasons Why The U.S. Rejected The ITU Treaty
Letöltve: http://readwrite.com/2012/12/14/5-reasons-why-the-us-rejected-the-itu-treaty (Utolsó letöltés: 02/03/2016)
PRICE, Rob (2015) The European Parliament just dealt a major blow to net neutrality.
Letöltve: http://www.businessinsider.com/european-parliament-net-neutrality-vote-2015-10 (Utolsó letöltés: 05/03/2016)
PROJECT CYBERCRIME (2014) Cybercrime Model Laws;
Letöltve: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf (Utolsó letöltés: 14/06/2016)

SASSO, Brendan (2012) House to examine plan for United Nations to regulate the Internet;
Letöltve: http://thehill.com/policy/technology/229653-house-to-examine-plan-to-let-un-regulate-internet (Utolsó letöltés: 02/03/2016)
SULLIVAN, Clare (2014) Cybersecurity and the ANZUS Treaty: The Issue of U.S.-Australian Retaliation;
Letöltve: http://journal.georgetown.edu/cybersecurity-and-the-anzus-treaty-the-issue-of-u-s-australian-retaliation/ (Utolsó letöltés: 10/01/2016)
RAMSTAD, Evan (2012) South Korea Court Knocks Down Online Real-Name Rule;
Letöltve: http://www.wsj.com/articles/SB10000872396390444082904577606794167615620 (Utolsó letöltés: 30/01/2016)
ROTH, Andrew (2015) Russia and China Sign Cooperation Pacts;
Letöltve: http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=1 (Utolsó letöltés: 10/06/2016)
WHITE HOUSE (2011) International Strategy for Cyberspace;
Letöltve: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Utolsó letöltés: 10/01/2016)
WHITE HOUSE (2013) Cybersecurity — Executive Order 13636;
Letöltve: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636 (Utolsó letöltés: 12/06/2016)
WHITE HOUSE STATEMENT (2015) Joint Statement: 2015 United States--India Cyber Dialogue;
Letöltve: https://www.whitehouse.gov/the-press-office/2015/08/14/joint-statement-2015-united-states-india-cyber-dialogue (Utolsó letöltés: 10/01/2016)
WHITE HOUSE FACT SHEET (2015) FACT SHEET: President Xi Jinping's State Visit to the United States;
Letöltve: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (Utolsó letöltés: 10/06/2016)
Wiley Rein (2013) Combating Cyber-Terrorism: President Issues Executive Order on Improving Critical Infrastructure Cybersecurity;
Letöltve: http://www.wileyrein.com/newsroom-articles-2621.html (Utolsó letöltés: 10/06/2016)

WSIS (2003) Final Report of the Geneva Phase of the Summit WSIS-03/GENEVA/DOC/0009 (rev. 1);
Letöltve: http://www.itu.int/net/wsis/documents/listing.asp?lang=en&c_event=s|1&c_type=o| (Utolsó letöltés: 28/04/2016)