Debreceni Jogi Műhely 2021. (XVIII.) 3-4.
Debreceni Egyetem, Állam- és Jogtudományi Kar, Debrecen
(University of Debrecen, Faculty of Law, Debrecen)
DOI 10.24169/DJM/2021/3-4/4

Kerekes László

PhD hallgató
Debreceni Egyetem, Marton Géza Állam- és Jogtudományi Doktori Iskola

„GODOTRA VÁRVA...” EGY EGYSÉGES KIBERBŰNÖZÉS ELLENI EGYEZMÉNY KODIFIKÁCIÓJÁNAK KIHÍVÁSAI

Debreceni Jogi Műhely, 2021. évi (XVIII. évfolyam) 3-4. szám (2022. február 15.)

DOI 10.24169/DJM/2021/3-4/4

Abstract: Ever since computers have existed, there has been a category of cybercrime. And because of the existence of cybercrime, international legislatures are trying to regulate this burning issue. This topic is not unknown to me. I wrote my dissertation on the anomaly of the Dark Web, which I carried on in my dissertation, where I examined the phenomenon of cybercrime on the international stage.

In my research, I examined how it is possible that there will be no single international cyber security convention in 2021. There are several reasons for this: it is a delicate issue – it has to do with state foreign policy; conceptual uncertainties – the current legal position is not uniform on certain issues either; different practices of legal entities – different states and IGOs; over-regulation – there are currently so many conventions and organizations that the issue is already opaque.

Keywords: cybercrime, codification

Absztrakt: Amióta léteznek számítógépek, azóta létezik a számítógépes bűnözés kategóriája. És mivel létezik számítógépes bűnözés, a nemzetközi- nemzeti jogalkotó szervek próbálják kialakítani a megfelelő szabályozást eme égető kérdésre. Ezen téma nem ismeretlen számomra. Tudományos diákköri dolgozatomat a Dark Web anomáliájáról írtam, ezt tovább vittem szakdolgozatomba, ahol pedig is a kiberbűnözés jelenségét vizsgáltam a nemzetközi porondon.

Kutatásomban azt vizsgáltam, hogyan lehetséges, hogy 2021-ben nincs egy egységes nemzetközi kiberbiztonsági egyezmény. Ennek több oka is van: kényes kérdés – ugyanis összefügg az állami külpolitikával; fogalmi bizonytalanságok – a jelenlegi jogtudományi álláspont sem egységes bizonyos kérdésekben; jogalanyok eltérő gyakorlata – az egyes államok valamint IGO-k gyakorlata eltérő; túlszabályozottság – jelenleg olyan sok egyezmény, szervezet foglalkozik a kérdéssel, hogy már már átláthatatlan a téma.

Kulcsszavak: kiberbűnözés, kodifikáció

A modern ember számára a számítógépes bűnözés egyre nagyobb fenyegetést jelent. Ez egyrészt magában foglalja az új bűncselekmények megjelenését, valamint már létező bűncselekmények modernizációját. Mivel világunk egyre jobban függ a technológiától égetően szükséges megtalálnunk a választ eme kihívásra. Jól mutatja a téma fragmentált jellegét, hogy magának a cybercrime-nak sincs egységes fogalma. Itt meg kell említeni Európa Tanács 2001-es Számítástechnikai bűnözésről szóló Egyezményét. Ezen egyezmény úttörő volt abban a tekintetben, hogy modellt biztosított a kiberbűnözéssel kapcsolatos nemzeti jogszabályok megfogalmazásához (1139/*2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági stratégiájáról, Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013.évi L. törvény*) valamint megadta a nemzetközi együttműködés alapjait.

Debreceni Jogi Műhely 2021. (XVIII.) 3-4.
Debreceni Egyetem, Állam- és Jogtudományi Kar, Debrecen
(University of Debrecen, Faculty of Law, Debrecen)
DOI 10.24169/DJM/2021/3-4/4

Amint az lenni szokott, a kiberbűnözés megjelenése egyúttal a jogalkotók figyelmét is ráirányította a joghézag meglétére. Számos nemzetközi egyezmény, valami helyi kiberstratégia született azzal a céllal, hogy visszaszorítsa és szabályozza a kérdést. Azonban egy egységes, Egyesült Nemzetek által elfogadott nemzetközi szerződés a mai napig nem jött létre.

Dolgozatomban azt vizsgálom miért nem jött létre napjainkig, 2021-ig egy egységes kiberbiztonságot szabályozó nemzetközi kódex. Éppen ezért a tanulmányt három nagyobb egységre tagolom. Az elsőben bevezetést nyújtok a kiberbiztonság-bűnözés eddigi eredményeiről, felsorolom a jelentősebb nemzetközi egyezményeket, illetve intézményeket. A másodikban elemzem miért tekinthető kényes kérdésnek a kiberhadviselés, bemutatom az elmúlt évek legnagyobb kibertámadásait, valamint bemutatom néhány állam gyakorlatát. A harmadikban a meglévő fogalmi bizonytalanságokat vizsgálom, például, hogy lehet, hogy 2021-ben nincs egy egységes cybercrime fogalom. Végezetül összegzem az addig leírtakat. Mindezek során főleg leíró és összehasonlító módszert használok, mely során felhasználom a meglévő releváns szakirodalmat, valamint a joganyagot.

1. A kiberbűnözés visszaszorítására tett eddigi nemzetközi összefogás: nemzetközi dokumentumok és intézmények

Ezen fejezetben azokat a fontosabb nemzetközi dokumentumokat illetőleg intézményeket vázolom fel, melyek dolgozatom témája szempontjából relevánsak.

Az Egyesült Nemzetek keretében megvalósuló együttműködés kereteit a következő dokumentumok alkotják. (SORBÁN, 2015, p.348)

„Az Egyesült Nemzetek Kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről” (SORBÁN, 2015, p.348) Ezen dokumentum nem határozta meg a számítógépes bűncselekmény fogalmát, azonban megjelöli azok tulajdonságait. Továbbá nem határolta el egymástól a számítógépes bűncselekmény, és a számítógéppel kapcsolatos bűncselekmény fogalmát. (SORBÁN, 2015, p.348) *„Az Egyesült Nemzetek Közgyűlésének 55/63 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról”* (SORBÁN, 2015, p.350) Ezen határozat prevenciós jellegű intézkedéseket tartalmazott az információs technológiák jogellenes felhasználását megelőzendő. (SORBÁN, 2015, p.350)

„Az Egyesült Nemzetek Közgyűlésének 56/121 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról” (SORBÁN, 2015, p.350) A Közgyűlés 2002-ben fogadta el ezt a határozatot. Ebben a Szervezet sürgeti a tagállamok közötti együttműködést, ugyanakkor felhívja a tagállamokat arra, hogy az információs technológiákkal való visszaélések visszaszorítására koncentráló nemzeti jogszabályok, politikák és gyakorlat kialakításakor vegyék figyelembe a nemzetközi és regionális szervezetek munkáját és eredményeit. (SORBÁN, 2015, p.350)

Az Európa Tanács is felfigyelt az új információ technológiai jelenségekre

„A Miniszteri Bizottság R (89) 9 számú ajánlása a számítógéppel kapcsolatos bűnözésről” (SORBÁN, 2015, p.350) Az Európa Tanács Miniszteri Bizottsága 1985-ben szakértői bizottság felállításáról döntött, amelynek a feladata a számítógépes bűncselekmények jogi vonatkozásainak feltárása volt. Ennek nyomán a Miniszteri Bizottság ajánlást adott ki a számítógépes bűncselekményeket illetően. A dokumentum összesen tizenkét tényállást különböztet meg, amelyeket két csoportra oszt: az első egy úgynevezett „minimumlista” mely 8 tényállást, a második egy opcionális lista mely 4 tényállást tartalmaz. (SORBÁN, 2015, p.350) *„A Miniszteri Bizottság R (95) 13 számú ajánlása a büntetőeljárás információs technológiával kapcsolatos problémáiról”* (SORBÁN, 2015, p.350) 1995-ben a Miniszteri Bizottság újabb ajánlást fogadott el, amely hét pontban foglalja össze azokat a problémákat, amelyek a büntetőeljárás során felmerülhetnek, amennyiben informatikai bűncselekményekről van szó. (SORBÁN, 2015, p.350) *„A Számítástechnikai bűnözésről szóló egyezmény és a kiegészítő jegyzőkönyvek”* (SORBÁN, 2015, p.350) Ezen egyezmény úttörő volt abban a tekintetben, hogy modellt biztosított a kiberbűnözéssel kapcsolatos nemzeti jogszabályok megfogalmazásához, valamint megadta a nemzetközi együttműködés alapjait. (SORBÁN, 2015, p.350)

DOI 10.24169/DJM/2021/3-4/4

Európai Unió:

„Az Európai Parlament és a Tanács 2000/31/EK irányelve a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól" Az irányelv nagyrészt nem büntetőjogi jellegű, de érdemes megemlíteni, hogy a dolgozatom szempontjából releváns rendelkezéseket tartalmaz. Az irányelv bizonyos feltételek teljesülése esetén mentesíti a közvetítő szolgáltatókat, mivel tevékenységük többnyire egyszerű továbbításra vagy adattárolásra korlátozódik, nem feltétlenül ismerik a tárolt információ tartalmát, így jogsértést, és a tartalomszolgáltatókkal ellentétben nem viselnek szerkesztői felelősséget. Által. A mentesülés egyik feltétele azonban, hogy a közvetítő szolgáltató a jogsértő adatot a tudomásszerzést követően haladéktalanul törölje. (SORBÁN, 2015, p.351) *„A Tanács 2001/413/IB számú kerethatározata a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről „A* kerethatározat harmonizációs kötelezettséget ír elő a tagállamoknak a nevezett bűncselekményekkel kapcsolatos büntetőjogi szabályozást illetően. A határozat kimondja *„ezeket a magatartásokat valamennyi tagállamban bűncselekménynek kell minősíteni, és az ilyen bűncselekményeket elkövető vagy azokért felelősséggel tartozó természetes és jogi személyekkel szemben hatásos, arányos és visszatartó erejű szankciókat kell előírni."* (SORBÁN, 2015, p.353) *„A Tanács 2005/222/IB kerethatározata az információs rendszerek elleni támadásokról „2005* februárjában az Európai Unió Tanácsa kerethatározatot fogadott el az információs rendszerek elleni támadásokról. Ez a dokumentum az információs rendszer kifejezést használja a korábban használt számítógépes rendszer kifejezés helyett. (SORBÁN, 2015, p.353) *„Az Európai Parlament és a Tanács 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról „Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról"* (SORBÁN, 2015, p.350) Továbbá 2013-ban az Unió megalkotta önálló kiberbiztonsági kódexét

A NATO Tallini Kézikönyv néven adott ki kiberbiztonsággal kapcsolatos joganyagot, továbbá Cyber Defence Management Authorityt és Cyber Defence Management Boardot állított fel, valamint gyorsreagálású csoportokat azaz RRT-ket működtet. (Sorbán, 2015, p.353) Az OECD államok a szervezet 1037.ülésén fogadták el *Útban a biztonságkultúra felé* címmel azt a dokumentumot, melyek a biztonságos környezet megteremtéséhez szükséges 9 alapelvet tartalmazza. (GYARAKI, 2020, p.199) A FIRST egy 1990-ben alakult nemzetközi szervezet, mely oktatási, szervezeti, kereskedelmi és biztonsági kérdésekre szakosodott. Az EBESZ 1202-es döntésében 16 bizalomépítő intézkedést hozott létre, melyekre a részes államoknak ügyelniük kell. Az Interpol Digital Crime Centert, Cyber Fusion Centert, valamint Digital Forensic Laboratoryt működtet. A G8 államok 2000-ben fogadták el az *Okinawa Chartát*, amely az információs társadalom chartája lett. (GYARAKI, 2020, p.200)

Meglátásom szerint a kodifikációt hátráltatja a már meglévő intézményrendszere a kibertér és a kiberbiztonság szabályozásának. Ugyanis annyira fragmentált, már-már kaotikus, ami nem túl szerencsés az egységes szabályozás megvalósításának. Lássuk hogyan is néz ez ki.

Amennyiben az Európai Uniót vizsgáljuk látható mennyi intézménye foglalkozik ezzel. *Az Európai Kiberbűnözés Elleni Munkacsoportot* 2010-ben hozták létre. A szakértői csoport az Europol, az Eurojust és az Európai Bizottság képviselőiből, valamint a tagállamok kiberbűnözéssel foglalkozó osztályainak vezetőiből áll. A szakértői csoport segíteni foga számítástechnikai bûnözés elleni küzdelem egységes európai megközelítésének kialakításában és elõmozdításában, és foglalkozni fog az információs technológia bűnözési célú felhasználása jelentette kihívásokkal. (Sorbán, 2015, p.356) Az *EMPACT* program lényegében az Európai Unió égisze alatt létrehozott, a transznacionális szervezett bûnözés elleni hatékony fellépést szolgáló missziórendszer, amelyet számos különbözõ prioritáson (például számítógépes bûnözés, embercsempészet, szintetikus kábítószerek, illegális bevándorlás stb.) jelöltek ki az EMPACT-nak. Nemzeti szakértők az Europol segítségével. A számítástechnikai bûnözés prioritása keretében a cél a kiberbûnözés és az internet bûnözési célú felhasználása elleni küzdelem. A prioritások között szerepel a hitelkártyás bűnözés, a kibertámadások elleni küzdelem és a gyermekek online szexuális kizsákmányolása. (Sorbán, 2015, p.357) Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.) az *Európai Hálózat- és Információbiztonsági Ügynökség* létrehozásáról Az Európai Hálózat- és Információbiztonsági Ügynökséget 2004-ben hozták létre a magas szintű hatékonyság és eredményesség biztosítása érdekében. a kiber- és információbiztonság, valamint a kiber- és információbiztonsági kultúra fejlesztése az uniós polgárok, a fogyasztók, a vállalkozások és a közszektorbeli szervezetek javára, ezzel is elősegítve a belső piac zavartalan

DOI 10.24169/DJM/2021/3-4/4

működését. (Sorbán, 2015, p.359)

Ezeken túlmenően a már korábban említett ENSZ dokumentumokon kívül nem rendelkezik olyan intézményi háttérrel, inkább a tagállamokra bízza azok megoldását. (GYARAKI, 2020, p.205) Az EBESZ is rendelkezik kiberstratégiával, valamint az Interpol is működtet információtechnológiai bűnözés elleni akciócsoportokat. Továbbá számos állam rendelkezik kiberbiztonsági stratégiával, például az Egyesült Államok, Németország, Egyesült Királyság, Kína, vagy akár Magyarország. Hazánk viszonylatában is számos dokumentum és intézmény lát el kiberbiztonsági feladatokat. Ez felsorolás jelleggel: Nemzeti Védelmi Stratégia, Nemzeti Kiberbiztonsági Stratégia, Információvédelmi törvény, Kibervédelmi Intézet, valamint a Magyar Honvédség Kiberszemlélője.

Meglátásom szerint érdemesebb lenne az intézmények nagy számát redukálni, elkerülve ezzel az esetleges hatásköri összeütközéseket, valamint növelné az átláthatóságot mind a szakemberek, mind a laikusok felé.

2. Kényes kérdés

A digitális forradalom minden más mellett a hadviselést is átalakította. Általánosságban elmondható, hogy azokat a kiberhadműveletekben az államok jellemzően kémkedési, diszruptív vagy destruktív céllal, közvetlenül, vagy harmadik fél, például hacker csoportok bevonásával indítják. A támadások leggyakoribb célpontjai az ellenséges államok kritikus infrastruktúrái, ipari-egészségügyi szektorai, valamint védelmi ágazatainak informatikai rendszerei. Emellett elterjedtek még a közösségi médiában megvalósuló a civil társadalom megfélemlítésére alkalmas tevékenységek. Tágabb értelemben tehát a kiberhadviselés körébe tartozik minden olyan kibertérben végrehajtott támadás, amelynek a támadó ország számára katonai vagy politikai értelemben hasznosítható eredménye van.

Tekintsük át az utóbbi évek legfontosabb kibertámadásait. Ennek során Berki Gábor kutatásaira támaszkodom. A legelső dokumentált kibertámadást a Tamil Tigrisek követték el 1997-ben. 1999-ben szerb hackerek NATO-szervereket támadtak Szerbiában és DDoS-t használtak arra, hogy e szerverek egy részét átmenetileg elérhetetlenné tegyék, valamint behatoltak a kormányzati webhelyekre, ahol propagandaüzeneteket helyeztek el. (BERKI, 2016, p.266)

Az első kibertámadás egy ország ellen 2007-ben történt. 2007. április 27-én zavargások törtek ki Észtországban a Szovjetunió hősei emlékművének lerombolása miatt Tallinban, ahol az IT-kultúra igen fejlett volt, beleértve a digitális menedzsmentet is. Az első támadás napokkal a parlament, a kormányhivatalok, a minisztériumok, a bankok, a telefontársaságok és a médiacégek szerverei elleni első tüntetés után történt. A célpontok kiválasztása, a támadások koordinációja, a pontos végrehajtás és a hatékonyság azt mutatja, hogy ezeket a támadásokat szervezett erők és külföldi intézmények támogatták. Szakértői jelentések szerint a támadás egy orosz szerverről indult, amit természetesen az orosz hatóságok cáfoltak. A támadott szerver természetéből adódóan azonban egyértelmű, hogy a támadás célja egyértelműen a balti államok kritikus információs infrastruktúrájának letiltása volt. Az ország legfontosabb, online forgalmat irányító szerverei nap mint nap összeomlottak, ezért sok közintézménynek átmenetileg le kellett kapcsolódnia az internetről. Egyes szakértők szerint az Észtország elleni kibertámadások által okozott gazdasági veszteségek sokkal súlyosabbak, mint azok a kereskedelmi szankciók, amelyekkel Oroszország a válság első heteiben fenyegetett. Szakértői jelentések szerint orosz hackerek botnetet hoztak létre, amelyben az orosz gépeken kívül 178 ország számítógépeit toborozták, hogy tudtuk nélkül hajtsanak végre támadásokat. (BERKI, 2016, p.267)

A 2008 augusztusában kitört orosz-grúz háborúnak is volt kiberhadviselésre visszavezethető aspektusa. (BERKI, 2016, p.267) Az emigrációba vonult grúz kormány amellett, hogy sorra jelentette meg a virtuális támadásokról szóló közleményeit, azt állította, hogy Oroszország ellenőrzése alá vonta Grúzia internetforgalmát. (www.georgiamfa.blogspot.com, 2008) A hacker-akciók ugyanis az állam kormányzati weboldalai ellen indultak, amelyeket k megbénítottak, valamint a tartalmukat kicserélték. Az orosz hackerek Mihail Szakasvili elnök ellen indítottak lejáratő hadjáratot.

Figyelmet érdemelnek azok a támadások, melyek kritikus infrastruktúra ellen irányulnak. Ide tartoznak: áramszolgáltatók, erőművek vagy más létfontosságú rendszerek. (BERKI,2016, p.268) Gondoljunk csak bele, mi történik akkor, amikor egy elkövető behatol a paksi atomerőmű számítógépes rendszerébe, ahol olyan

DOI 10.24169/DJM/2021/3-4/4

változtatásokat hajt végre, hogy ennek következtében annak fontos alkatrészei károsodást szenvednek és mindezt Magyarország alkotmányos rendjének megzavarása céljával teszi; egyebek mellett a rombolás bűntettét is elköveti, amint erről Ibolya Tibor is vélekedik. (IBOLYA, 2012, p.9)

Több olyan támadás is volt már a világon (Brazília, Törökország), ahol kibertámadás következtében állt le az áramszolgáltatás. (BERKI, 2016, p.268) 2015 decemberében regisztráltak ilyen jellegű támadást Ukrajnában, melynek következtében hétszázezer embert érintő áramszünet következett be. (BERKI, 2016, p.268) 2016 januárjában a kijevi repülőtér számítógépes rendszerében találtak olyan kódokat, amelyek a repülés biztonságának veszélyeztetésére alkalmasak voltak. (BERKI, 2016, p.268)

A kritikus infrastruktúrák, valamint az ipari folyamatirányító rendszereket támadó rosszindulatú kódok az utóbbi években hatalmas fejlődésen estek át. (BERKI, 2016, p.268) Legnagyobb figyelmet kapó példája ezeknek a programoknak a VirusBlokAda cég 2010-ben kifejlesztett vírusa, amely a Stuxnet nevet kapta. (BERKI, 2016, p.268) A vírus célja az iráni urándúsító centrifugák tönkretétele és a dúsítás ellehetetlenítése volt. Ezt a célt sikeresen teljesítette, hiszen legalább 1000 centrifugát tett használhatatlanná a Natanzban lévő dúsítóban és legalább két évvel vetette vissza az atomprogramot. (BERKI, 2016, p.268)

2016-ban több állam, köztük az Egyesült Államok, Franciaország és az Egyesült Királyság megvádolta Oroszországot, hogy a kibertéren keresztül avatkozott be a választási folyamataiba. 2019-ben Izrael megsemmisítette a Hamasz egyik épületét, ahonnan feltehetőleg kibertámadást hajtottak végre Izrael ellen. A 2020-as évben kibertámadás érte az USA pénzügyminisztériumának szervereit, valamint Magyarország Kormányának weboldalát is.

A kiberhadviselés mellett azonban, mint az állami külpolitika eszközeként megjelent a kiberdiplomácia. A kiberdiplomácia nem más, mint diplomáciai erőforrások, eljárások felhasználása a nemzeti érdekek érvényesítése érdekében a kibertérben. (Nyáry, 2020, p.332) Érdekes sajátosság, hogy míg az állami külpolitika főbb irányvonalait egy általános stratégiai dokumentum tartalmazza, addig a kiberdiplomáciai célokat egy kiberstratégia tartalmazza. Ez részben magyarázható a speciális témákkal, mint például kiberbiztonság-kiberbűnözés, stratégiai bizalomépítés, internet szabadság, valamint a szuverenitás kérdése is. Személyzete valós diplomatákból áll, valamint felölelhet bilaterális, vagy multilaterális viszonyt. (Nyáry, 2020, p.33.)

A kiberdiplomáciai folyamatok megindulásának első állomása 2011, amikor is az Egyesült Államok elfogadta az International Strategy for Cyberspace névre keresztelt dokumentumot. Ez volt az első kormányzati dokumentum, mely önálló tématerületnek tekintette a kibertér nemzetközi összefüggéseit. (Nyáry, 2020, p.334) Ezen felül néhány problémás területet azonosít úgy mint, hálózatvédelem, internetkormányzás, internet szabadsága. Mindezeken túlmenően a stratégia a keretrendszer megalkotása mellett megalkotta a megvalósítási intézményrendszert is, ugyanis létrehozta az Egyesült Államok Külügyminisztériumának Kibertérügyi Koordinátori Hivatalát.

2013-ban Japán is megalkotta kiberdiplomáciai stratégiáját, mely a Nemzetközi Kiberbiztonsági Együttműködési Stratégia nevet kapta. 2015-ben az Európai Unió Tanácsa elfogadta az Európai Tanácsi Következtetést a Kiberdiplomáciáról, mely mérföldkő abban az értelemben, hogy először használta a kifejezést az unió intézményrendszerében. (Nyáry, 2020, p.334) A stratégia alkotást követően több államban is felállítottak a külügyminisztérium kötelékében működő kiberdiplomáciával foglalkozó részleget, mint például Belgiumban.

Láthatjuk ezek alapján, hogy a digitalizáció az eddigi hagyományos kereteket megtörte és új tartalommal bővítette. Vagyis a kooperációs szándék megvan, azonban új és izgalmas keretek jelentek meg az állami érdekek érvényesítésére.

A kodifikáció egy másik visszahúzó komponense az az államok eltérő gyakorlata és viszonyulása a kibertérhez. Ezt legegyszerűbben Kína, Oroszország és az Egyesült Államok példáján keresztül lehet megérteni.

Kína viszonya a kibertérhez elég sajátosan alakult, főleg, hogy a gazdasági fejlődés katalizátora az információtechnológia mellett az internet elterjedése volt. (KOVÁCS, 2018, p.105) 2013-ban egy ENSZ szakértői csoport jelentése megállapította, hogy a kibertér szabályozására az ENSZ Alapokmánya és a hatályos nemzetközi jog minden további nélkül alkalmazható, azonban Kína és még pár közép-ázsiai ország

DOI 10.24169/DJM/2021/3-4/4

egy önálló kiberbiztonságot szabályozó magatartási kódexet nyújtott az ENSZ plénuma elé. A dokumentum célja, hogy *„az információs térben azonosítsa az államok jogait és felelősségét, előmozdítsa a konstruktív és felelősségteljes magatartásukat, valamint fokozza együttműködésüket az információs térben jelentkező közös fenyegetések és kihívások kezelésében"* (KOVÁCS, 2018, p.105) A kódex 13 pontban rögzítette a csatlakozó államok kötelezettségeit, köztük a belügyekbe való beavatkozás tilalmát. Ez abban a fényben is érdekes, hogy a kódexhez Oroszország is csatlakozott, aki többé-kevésbé bizonyítottan 2016-ban több állam választásába is beavatkozott. A dokumentum kiadására azért kerülhetett sor, mivel az abban érdekelt államok nagyon érzékenyek a kibertér szabályozására, annak a szabályozása a szuverén feladata kellene, hogy legyen. Ez Kínára levetítve annyit jelent, hogy a felhasználók irányítását az államnak kell végeznie, valamint a kibertér szuverenitása az állam szuverenitását is meghatározza. (KOVÁCS, 2018, p.105)

Éppen ezért Kína webes cenzúrát állított fel, mely többek között olyan tartalmakat tilt, mint Tibet függetlenedése, tajvani kormányzati weboldalak vagy pornográf tartalmak. Eme konstrukció elnevezése a Kínai Nagy Tűzfal, melynek Aranypajzs nevű része felel az internetes tartalmakért. Éppen ezért hatalmas mennyiségű információtechnológiai szakember felügyeli a még több felhasználó tevékenységét. (KOVÁCS, 2009, p.25)

Ezek után jutunk egy 1999-ben a Kínai Népi Felszabadítási Hadsereg két tisztje által kiadott könyvig, aminek címe Korlátlan hadviselés. Ez a könyv fektette le a Kína által korlátlan hadviselésként alkalmazott módszert, amit a kibertérben is alkalmaz. Sajátosan ázsiai gondolkodásmódot tükröz, európai szemmel nehezen megérthető, de lefektette a kínai kiberhadviselés alapjait. (KOVÁCS, 2009, p.25)

Ez alapján látható, hogy Kína már rég folytat a kibertérben katonai tevékenységeket. 2008-ban készült jelentés alapján már 2002 óta voltak olyan támadások, melyek Kínának tudhatóak be. (KOVÁCS, 2018, p.111) 2013-ban egy újabb független jelentés készült, mely több mint 20 ATP-t, azaz fejlett technológiával fennálló folyamatos támadásra képes hackercsoportot azonosított melyek Kínához köthetőek. Ezek közül az ATP1-ről nem mást állít a jelentés, minthogy az nem más, mint a Kínai Népi Felszabadítási Hadsereg 61398. számú egysége. Vagyis, a kiberműveleteket teljes mértékben alárendelték a katonai irányításnak. (KOVÁCS, 2018, p.111)

Ezt követően nézzük meg Oroszország jelenlétét a kibertérben. Ezt nagyon jól összefoglalja Clapper, az NSA igazgatójának nyilatkozata 2016-ban *„Oroszország esetében egyre inkább növekvő kibertéri jelenlét feltételezhető abból kiindulva, hogy készek a kritikus infrastruktúrákat támadni, illetve kiberkémkedési műveleteket folytatni, még akkor is, ha észlelték őket, vagy ha nagyobb nyilvános ellenőrzés alatt állnak. Az orosz kiberműveletek valószínűleg az USA érdekeltségeit célozzák a stratégiai céljaik elérésének támogatására. Információgyűjtést folytatnak az orosz döntéshozatal támogatása érdekében az ukrán és a szíriai válságok során, a katonai és politikai célkitűzések támogatására pedig befolyásolást végeznek, valamint a kiberkörnyezetet folyamatosan készítik elő a jövőbeni tevékenységekre."* (www.dni.gov, 2016)

Az orosz kiberjelenlét sokban hasonlít a kínaira, megvannak a kijelölt támadási irányai. Többek között a Kaukázus, Kelet-Európa, valamint a NATO és EBESZ. Mindezeket ATP-kel is elősegítik. Az egyik csoport az ATP28, illetve a Fancy Bear nevet kapta. Ők főleg phishing műveleteket hajtottak végre, valamint fake domain neveket alkottak egyes weboldalakhoz. (KOVÁCS, 2018, p.134) Meg kell említeni Oroszország szabályozása kapcsán a Geraszimov-doktrína néven elhíresült publikációt. Ezen dokumentumot Valerij Geraszimov hadseregtábornok, az orosz fegyveres erők vezérkari főnöke jelentette meg 2013-ban és hatást gyakorolt az orosz haderő fejlesztésére, valamint elméleti kérdéseket is fejteget. (HOLECZ, 2017, p.13.) Amint azt Geraszimov írta *„A fegyveres konfliktusok modern eszközeinek lényegét befolyásoló másik tényező a modern automatizált/robotizált eszközök és a mesterséges intelligencia területén folytatott kutatások katonai célú felhasználása. Míg ma repülő drónjaink vannak, a holnap csatatereit sétáló, kúszó, ugró és repülő robotok töltik majd meg. A közeljövőben az is lehetséges, hogy teljesen robotizált alegységeket hoznak létre, amelyek képesek lesznek önállóan katonai műveletek végrehajtására."* (HOLECZ, 2017, p.16.)

Egy másik csoport az ATP29 nevet, illetve a Cozy Bear nevet kapta, feltehetőleg polgári kötődésűek voltak és leginkább adatlopási műveleteket hajtottak végre. (KOVÁCS, 2018, p.135)

Ezt követően tekintsük át az Egyesült Államok jelenlétét a kibertérben a kiberbiztonsági stratégián keresztül, ehhez Kovács László tábornok úr kutatását hívom segítségül. Az Egyesült Államok Védelmi Minisztériuma (DoD) 2015 áprilisában alkotta meg az ország kiberbiztonsági stratégiáját. A stratégia három olyan

DOI 10.24169/DJM/2021/3-4/4

nemzetbiztonsági szempontból is jelentős területre épít, amely a DoD tekintetében a legfontosabb feladatokat jelenti a kibertérben: *„a DoD hálózatainak, számítógépeinek és adatainak védelmére; az Egyesült Államok és annak érdekeinek védelmére a súlyos következményekkel járó kibertámadásokkal szemben; valamint a katonai műveletek kibertámogatására."* (KOVÁCS, 2018, p.154) A dokumentum többször is megnevezi az Egyesült Államok Kiberparancsnokságát (USCYCOM) mint *„a különböző, a stratégiában kiemelt területek felelős szervezetét."* (KOVÁCS, 2018, p.159) Az első feladat, amelyet a stratégia a USCYCOM-ra helyez, a legfontosabb kibertéri műveleteknél szerepel. Ez nem mást, mint *„a szembenálló fél hálózati vagy egyéb, a kibertérben működő rendszerei elleni tevékenységet jelenti."* (KOVÁCS, 2018, p.159) Ezzel párhuzamosan rendkívül érdekes annak meghatározása, hogy ez a tevékenység, amely akár offenzív tevékenység is lehet, de kiterjedhet a kibertéren kívül eső tartományokra: *„Az Egyesült Államok Cyber Command tevékenysége arra is irányulhat, hogy – adott esetben más amerikai kormányhivatalokkal együttműködve – kiberműveleteket hajtson végre más területeken fennálló stratégiai fenyegetések elrettentése vagy felszámolása érdekében."* (KOVÁCS, 2018, p.159)

A fort madei Kiberparancsnokság az egyik alapvető fontosságú hivatal az Egyesült Államok olyan katonai szervezetei között, amelyek elsődleges feladata a kibertér folyamatainak ellenőrzése, illetve irányítása. (KOVÁCS, 2018, p.160) A parancsnokság legfőbb küldetése: *„A műveletek vezetése és a Védelmi Minisztérium hálózatainak védelme érdekében tervezi, koordinálja, integrálja és szinkronizálja a – különböző tevékenységeket, valamint előkészíti és elrendelés esetén vezeti a katonai kibertér teljes spektrumában a műveleteket annak érdekében, hogy azok minden területen megvalósulhassanak, és hogy biztosítsák az USA és a szövetségesek cselekvési szabadságát a kibertérben, és megfosszák attól a szemben álló felet."* (KOVÁCS, 2018, p.160)

Az Egyesült Államok Hadseregének Kiberparancsnoksága, a Haditengerészeti Kiberparancsnokság és a Tengerészgyalogság Kiberparancsnoksága az Egyesült Államok Kiberparancsnokságának alárendeltjei. Bár jogi kapcsolatban áll a Nemzetbiztonsági Minisztériummal, a Coast Guard Cyber Command közvetlen támogatást nyújt az Egyesült Államok Kiberparancsnokságának. (KOVÁCS, 2018, p.160) Emellett a Nemzeti Kiberbiztonsági és Kommunikációs Integrációs Központ a Nemzetbiztonsági Minisztérium égisze alatt működik, és szövetségi szintű incidenskezelési és ellenőrzési feladatokat lát el a nap 24 órájában, a hét minden napján. Ezen túlmenően a szervezet kapcsolatot biztosít a szövetségi kormány, a titkosszolgálati közösség, valamint a bűnüldöző szervek hálózati és kommunikációs szervezetei között. (KOVÁCS, 2018, p.160) Az NCCIC a köz-továbbá magánszféra között információmegosztási feladatokat is ellát, amely során feladatai sebezhetőségekre, incidensekre, biztonsági eseményekre reagálás, illetve azok elhárítása vagy bekövetkezésük esetén azok következményeinek enyhítése. (KOVÁCS, 2018, p.161) Az NCCIC-nek alárendelten működik a US-CERT, amelynek feladata elemzéseket végezni a nemzeti hálózatokat veszélyeztető támadásokkal kapcsolatban, illetve az Ipari Irányító Rendszerek CERT-je, amely szövetségi és tagállami szinten egyaránt felelős a kritikus infrastruktúra ágazatokban a kiberbiztonság fenntartásáért. (KOVÁCS, 2018, p.161)

A fentebb felvázolt államok gyakorlata is kedvezőtlen hatással lehet agy esetleges jövőbeni nemzetközi egyezmény kodifikálására. Véleményem szerint túl „kényelmes" tevékenység ahhoz, hogy felhagyjanak vele.

3. A fogalmi bizonytalanságok kérdése

Először is fontos tisztázni, hogy van különbség kiber, elektronikus és digitális jelző között. (Mártonffy, 2020, p.308) A kiber főleg a biztonsági kérdésekre fókuszál, az elektronikus jelző leginkább gazdasági szférára utal, a digitális pedig vállalati és állami szektorokra utal.

Magának a cybercrimenak sincs egy egységes fogalma, nézzük hogyan alakult ennek a meghatározása az évek során. Az 1986-os OECD jelentés elemezte és rendszerezte az európai tapasztalatokat, ezzel irányt mutatva a bűncselekmények feltérképezéséhez és azok megismeréséhez. (Deres, 2016, p.244) 1989-ben az Európa Tanács megfogalmazta *„9. számú ajánlását, mely a számítógéppel kapcsolatos bűncselekményekről szól."* (DERES, 2016, p.244) A Tanács egy szakértői testületet is felállított, ám ez kerüli a számítógépes bűncselekmény meghatározását, ehelyett az online térben elkövethető bűncselekményeket határozza meg. 1997-ben a G-8 fórum megalapítja a high-tech bűnözés elleni alcsoportját, továbbá elfogadja a számítógépes bűnözés elleni harc 10 alapelvét.

DOI 10.24169/DJM/2021/3-4/4

Következő lépcsőfok volt az Európa Tanács 2001-es Számítástechnikai bűnözésről szóló Egyezménye. Ezen egyezmény úttörő volt abban az értelemben, hogy modellt biztosított a kiberbűnözéssel kapcsolatos nemzeti jogszabályok megfogalmazásához, valamint megadta a későbbi nemzetközi együttműködés kereteit. Az egyezmény a bűncselekményeket a következőképp kategorizálta: „*számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények; számítógéppel kapcsolatos bűncselekmények; számítástechnikai adatok tartalmával kapcsolatos bűncselekmények; szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények; számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények."* (DERES, 2016, p.244)

Azonban az egyezmény nem tartalmaz több tényállást, így pl.: kiberterrorizmus. Az Európai Parlament és Tanács 2011-ben hozta meg irányelvét „*A gyermekek bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről."* (DERES, 2016, p.245) Ezen dokumentum büntetni rendelte a groomingot, vagyis a gyermekekkel történő szexuális céllal zajló internetes kapcsolatfelvételt. 2013-ban hozta meg az Európai Parlament és Tanács „*Az információs rendszerek elleni támadásokról szóló irányelvét."* (DERES, 2016, p.245) Ennek célja, hogy *„a bűncselekmények tényállására és szankcióikra vonatkozó szabályok megállapítása révén közelítse a tagállamok büntetőjogát az információs rendszerek elleni támadások terén, és hogy javítsa a tagállamok illetékes hatóságai, így a rendőrség és az egyéb bűnüldözési szolgálatok, valamint az Unió illetékes szakosított ügynökségei és szervei közötti együttműködést."* (DERES, 2016, p.244)

Az egyes nemzetközi szerveken túlmenően a jogtudomány is megkísérelt választ találni a kérdésre. A Jaburek- Schmölzer (JABUREK-SCHMÖLZER, 1985, p.20) szerzőpáros a számítógépet a cselekmény közbenső vagy végső céljának fogta fel. Pl.: ha az elkövető az adatlopást az adatok másolásával befejezi, úgy a cselekménye, mint végső cél jelenik meg. Azonban, ha a bűncselekményt manipulált számítógépes programokkal hajtatja végre, úgy a számítógép, mint közbenső cél jelenik meg. Michels definiálása szerint a számítógépes visszaélés felöleli a számítógép használatát, mint a jogtalan hozzáférésben megvalósuló célt és szituációt. Gassin (GASSIN, 1988, p.164) az informatikai bűncselekmények tárgyaként megkülönbözteti az informatikai szabotázst és az informatikai kalózkodást. (IBOLYA, 2012, p.10) Bauknecht a számítógépes manipulációkat, a titkos kémkedést, a gépidő lopást és a szabotázs cselekményeket is ide sorolta. (IBOLYA, 2012, p.10) Yamaguchi szintén hasonló eredményre jutott. (IBOLYA, 2012, p.10) Spreutels a számítógépes hamisítás és a rendszerbe történő jogosulatlan behatolás meghatározásával bővíti a palettát. (IBOLYA, 2012, p.10) Möhrenschlagernél megjelenik a személyes adatokat veszélyeztető támadás is. (IBOLYA, 2012, p.11) Eric Himpton 3 csoportba sorolja a számítógépes bűncselekményeket: *„a szoftver és hardver együttese ellen irányuló bűncselekmények, azon bűncselekmények, ahol a számítógép, mint médium jelenik meg, azon bűncselekmények, ahol a számítógép, mint tárolóeszköz jelenik meg."* (IBOLYA, 2012, p.12) Britz szerint a cybercrime *„olyan számítógépes rendszerekkel vagy internetre csatlakoztatott számítógépekkel való visszaéléseket ölel fel, melyek közvetlenül vagy járulékosan veszteségeket okoznak*." (BRITZ, 2013, p.6)

Magyarországon Polt Péter hívta fel mind a közélet, mind a tudományos világ figyelmét az új jelenségre. Meghatározása szerint a számítógép ugyanis lehet „*a bűncselekmény tárgya és eszköze."* (POLT, 1983, p.60) Pusztai László 4 típusát különböztette meg az interneten megvalósuló bűncselekményeknek: *„a számítógépes visszaélést, az adatkikémlelést, a számítógépes szabotázst, valamint a gépidőlopást."* (PUSZTAI, 1989, p.85) Kunos Imre tanulmányában (KUNOS, 1999, p.28) a számítógépes bűnözést azon bűncselekmények összességeként definiálja, melyek a bűncselekmény elkövetésének eszközéül információtechnológiai eszközöket használnak fel. Az idő előrehaladtával és a technika fejlődésével Nagy Zoltán András is hasonló kategóriákat határozott meg. (NAGY, 2009, p.37) Szabó Imre 2 kategóriába sorolja az internetes bűncselekményeket: *„az internet, mint hálózat ellen elkövetett bűncselekmények, illetve az interneten, mint az elkövetés helyén megvalósuló jogtalan cselekmények."* (NAGY, 2009, p.37) Valamint meghatározta a számítástechnikai bűncselekmények fogalmát, mint *„azok a deliktumok, melyek egy számítógépes rendszerrel vagy számítástechnikai adattal kapcsolatba hozhatók, akár úgy, hogy az elkövetés eszközeként jelennek meg, vagy pedig a bűncselekmény elkövetési tárgyát képezik."* (NAGY, 2009, p.37)

Siegler Eszter különböztette meg a *„számítógépes bűncselekmények"* és a *„számítógéppel kapcsolatos bűncselekmények"* fogalmait. (SIEGLER, 1997, p.736) Számítógéppel kapcsolatos bűncselekmények alatt azokat a cselekményeket értette, *„ahol a számítógép az elkövetés eszköze vagy tárgya."* (SIEGLER, 1997, p.736) A számítógépes bűncselekmény fogalmát azokra a „*deliktumokra használta, melyek kifejezetten számítógépes rendszer és adatok ellen irányult."* (SIEGLER, 1997, p.736)

Sorbán Kinga *„a számítógépes bűncselekmény, számítógéppel kapcsolatos bűncselekmény, informatikai bűncselekmény, kiberbűncselekmény, digitális bűncselekmény, e-bűncselekmény, csúcstechnológiás bűncselekmény kategóriáit különbözteti meg."* (SORBÁN, 2018, p.369)

Azonban, ahogy Dornfeld László is rámutat erre, a joggyakorlat során is merülnek fel kérdések. A büntetőeljárás megindításának és lefolytatásának feltétele, hogy az ügy az adott állam joghatósága alá tartozzon. (DORNFELD, 2017, p.241) A kibertér sajátosságai okán a joghatóság fennállásának meghatározása problémás. Elképzelhető az a helyzet, ahol mind a terhelt, mind a sértett más-más országban tartózkodik, valamint a bűncselekmény során felhasznált információs eszköz harmadik államban található. (DORNFELD, 2017, p.241) Bonyolíthatja a helyzetet, ha az elkövető tranzit harmadik állam területénköveti el a büntetendő cselekményt. (DORNFELD, 2017, p.241)

Az Európai Unió több jogforrása is tartalmaz joghatóságot meghatározó cikkelyeket. A 2005/222/IB kerethatározat 10. cikke az általa szabályozott bűncselekmények körében állapítja meg a joghatóság fennállását. (DORNFELD, 2017, p.244) Ebben az esetben eljárás indítható, *„ha a bűncselekményt egészben vagy részben a tagállam területén követték el, az elkövető az adott állam állampolgára vagy olyan jogi személy sérelmére követték el, amelynek tevékenysége végzésének központja a tagállam területén található."*(DORNFELD, 2017, p.244) A cikk 4. bekezdése sorrendiséget állapít meg a joghatósággal rendelkező államok között. (DORNFELD, 2017, p.244)

A kerethatározatot a 2013/40/EU irányelv váltotta fel. (DORNFELD, 2017, p.244) A 12. cikke meghatározza az elkövetés helyét, illetve az állampolgárságot, de lehetőséget ad a tagállamoknak, hogy megállapítsák joghatóságukat, *„ha területükön található jogi személy sérelmére történt elkövetés vagy pedig az elkövető szokásos tartózkodási helye a területükön van."* (DORNFELD, 2017, p.244) Fontos megjegyezni, hogy ezen uniós jogforrások csak az általuk szabályozott bűncselekmények esetében tartalmaznak szabályokat. Az ide tartozó esetekben további gondot jelent a szövetségi államokon belül annak megállapítása, hogy a büntetőeljárás tagállami vagy szövetségi szinten induljon. További probléma, ha uniós államon kívül más állam is érintett az ügyben. (DORNFELD, 2017, p.244)

Miskolczi Barna és Szathmáry Zoltán szerint „*a joggyakorlat ellentmondásainak okai a releváns elkövetési mozzanatok kiválasztására, ezen mozzanatok eltérő felfogására és az elkövetési magatartás kiterjesztő értelmezésének gyakorlati igényeire vezethető vissza."*(MISKOLCZI-SZATHMÁRY, 2018, p.111) A tartalombűncselekmények esetében az interneten hozzáférhető elektronikus adatok tartalma alapozza meg, hogy egyáltalán szükséges-e a büntetőjogi fellépés, és az elkövetési magatartás a tartalmakhoz való hozzáférésben, azok birtoklásában, valamint az adatokkal végzett műveletekben nyilvánul meg. Ezen bűncselekmények esetekor az egyes adatok helye, ezen kívül az adatokkal való rendelkezés helye alapozza meg az elkövetés helyét. Tehát, a külföldi szerveren jogsértően kezelt szerzői művekkel belföldön végzett, vagy belföldről kezdeményezett műveletek belföldi elkövetésként értékelhetőek. (MISKOLCZI-SZATHMÁRY, 2018, p.113)

Összefoglalva a fentebb írtakat véleményem szerint célszerűbb lenne az egységes terminológia kialakítása egy esetleges nemzetközi egyezmény megalkotása érdekében.

Összegzés

Összegzésként megállapítható, hogy még igencsak messze állunk egy egységes kiberbiztonsági kódex megalkotásától. Főleg az eltérő állami gyakorlat, érdekek, amik jelenleg nem engedik meg az egységes szabályozást. Továbbá a folyamatos változás, ami a cybercrime fogalmát illeti, ki tudja, mit tekinthetünk 10 év múlva annak. Ugyanakkor biztosnak látszik, hogy a jövő a kiberdiplomácia felé hajlik, emiatt szintén szükséges lenne a nemzetközi összefogás egy egységesen kodifikált dokumentum megalkotására.

Irodalomjegyzék

Berki Gábor (2016) Kiberháborúk, kiberkonfliktusok. In: Pintér István, Műhelymunkák: A virtuális tér geopolitikája. Budapest, Geopolitikai Tanács Közhasznú Alapítvány, pp. 266.-325. ISSN 1788-7895

BRITZ Marije (2013) Computer Forensics and Cyber Crime. London, Pearson. p. 23. ISBN: 978-0132677714

Clapper James (2016) Statement for the Record: Worldwide Threat Assess- ment of the US Intelligence Community. Senate Armed Services Committee. Letöltve: www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_ SFR_FINAL.pdf (Utolsó letöltés: 29/05/2021)

Deres Petronella (2016) Internetes bűnözés. In: Tóth András. Technológia jog-Új globális technológiák jogi kihívásai. Budapest, Patrocinium Kiadó. pp. 243-250 ISBN 9789639808720

Dornfeld László (2017) Az elektronikus bizonyítékszerzés aktuális kérdései. Kriminológiai Közlemények, 2018.évi évf, 2. sz. pp. 241-255.

Gassin Raymond (1988) Az informatika büntetőjoga, Magyar Jog 1988.évi évf, 2. sz. pp. 164-172.

Gyaraki Réka (2020) A nemzetközi intézmények szerepe a kiberbiztonságban In: Török Bernát. Információ és kiberbiztonság. Budapest, Ludovika Egyetemi Kiadó. pp. 199-267.

Holecz József (2017) A Geraszimov-doktrína- Egy másik megvilágításban. Felderítő Szemle, 2017.évi évf. 3-4.sz.pp. 5-28. ISSN: 1588-242X

Ministry of Foreign Affairs of Georgia(2008) Cyber Attacks Disable Georgian Websites, Letöltve: http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html (Utolsó letöltés: 29/05/2021)

Ibolya Tibor (2012) A számítástechnikai jellegű bűncselekmények nyomozása. Budapest, Patrocinium kiadó, p. 9-15. ISBN 9786155107764

Kovács László (2009) Információs hadviselés kínai módra. Budapest. Nemzet és Biztonság, 2009.évi évf 7. sz. pp. 25-45.

Kovács László (2018) Kiberbiztonság és –stratégia. Budapest, Dialóg Campus Kiadó, 104. p., 104.

Kunos Imre (1999) A számítógépes bűnözés. A modern információtechnológia felhasználása a bűnözésben. Belügyi Szemle, 1999.évi évf.11. sz. pp. 28-42. ISSN: 2677-1632

Mártonffy Balázs (2020) Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták In: Török Bernát. Információ és kiberbiztonság. Budapest, Ludovika Egyetemi Kiadó, pp. 308-321.

Miskolczi Barna- Szathmáry Zoltán (2018) Büntetőjogi kérdések az információk korában. Budapest, HVG-Orac Lap-és Könyvkiadó Kft., 11. p., ISBN 978 963 258 428 7

Nagy Zoltán András (2009) Bűncselekmények számítógépes környezetben, Ad Librum, Budapest, 2009, pp. 37. ISBN 9789639888920

Nyáry Gábor (2020) Kiberdiplomácia: hatalom, politika és technológia a geopolitika ötödik dimenziójában In: Török Bernát. Információ és kiberbiztonság. Budapest, Ludovika Egyetemi Kiadó, pp. 321-343.

Polt Péter (1983) A számítógépes bűnözés. Belügyi Szemle, 1983.évi évf. 6. sz. pp. 60- 64.

Pusztai László (1989) Számítógép és bűnözés. In: Gödöny József: Kriminológiai és Kriminalisztikai Tanulmányok. Budapest, Közgazdasági és Jogi Könyvkiadó, pp. 85- 146. ISSN: 1586-4596

Siegler Eszter (1997) A számítógéppel kapcsolatos és a számítógépes bűncselekmények. Magyar Jog, 1997.évi évf. 12. sz, pp. 736- 742. ISSN: 0025-0147

Sorbán Kinga (2015) Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói. Themis Folyóirat. 12. évf. 1. sz. p.348. ISSN 2064-0900

Sorbán Kinga (2018) Vírusok és zombik a büntetőjogban. In Medias Res, 2018.évi évf. 2. sz. pp. 369-386. ISSN: 2786-152X

W. Jaburek- G. Schmölzer (1985) Computer- Kriminalitat, Wien, 20-23.