HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

A KIBERTÉR ÉS SZEREPLŐI

THE CYBERSPACE AND ITS ACTORS

GÉMES Csaba

(ORCID: 0000-0003-3012-2175)

gemes.csaba@uni-nke.hu

Absztrakt

„Az információ hatalom” tartja a közkeletű mondás. A hatalom általánosságban a mások befolyásolására való képességként fogalmazható meg, beleértve a mások befolyásának elkerülését is. A hatalom megőrzése, az egyes országok fennmaradása az elmúlt évezredekben csak a megfelelő fizikai erő alkalmazásával volt garantálható.

Az infokommunikációs technológia elterjedése egy új dimenziót nyitott az emberiség számára: a kiberteret.

Az elmúlt évek eseményei azt bizonyították, hogy a kibertérben olyan mértékű lehetőségek és veszélyek rejlenek, amelyek komoly hatást gyakorolhatnak az állam működésére.

Az állam érdekeinek kibertérben való érvényesítése csak a megfelelő kiberképességek kialakításával, illetve fejlesztésével érhető el. A cikk írója ennek lehetőségeit kutatja. Ebben a cikkben a kibertér értelmezését követően áttekinti a kibertér mindazon szereplőinek körét, akiknek szerepe lehet egy integrált nemzeti kiberképesség létrehozásában.

Kulcsszavak: *kibertér, kiberbiztonság kiberhadviselés, kiberképesség*

Abstract

“The information is power" the common saying keeps it. The Power in generality can be describe as an ability to influence others, including avoiding the influence of others. The Conservation of the power, the survival of individual countries in the last millenniums was only guaranteed by the use of the appropriate physical force.

The spread of info-communication technology has opened up a new dimension for the humanity: the cyberspace.

The events of past years have proved that the extent potential opportunities and threats in cyberspace, which they are serious implications for the functioning of the state.

Asserting the claims of the state in cyberspace only the equivalent cyber capability with his forming and his developing can be rached. The author of the article has been researching the opportunities of this. In this article he reviews those actors who may be involved in the creation of an integrated national cyber capability, after the interpreted the cyberspace.

Keywords: cyberspace, cybersecurity, cyberwarfare, cyber capability

BEVEZETÉS

Az „információ hatalom” tartja a közkeletű mondás. Nehéz lenne ezt cáfolni, látva a napjaink információs társadalma által szolgáltatott számtalan példát. Emellett azt is tényként kezelhetjük, hogy az emberiség által felhalmozott információ mennyisége rohamosan növekszik. De hol is találkozhatunk ezzel az óriási mennyiségű információval? A válaszokat keresve elsőként az információt hatalommá változtatni képes emberi elmét kell említenünk. Mivel az emberi elme befogadóképessége véges, így évezredekkel ezelőtt elkezdtük az információ írásos rögzítését, majd kihasználtuk a tárgyiasult formájú információ továbbításának lehetőségét is. Az elektrotechnika megjelenésével mintegy kétszáz éve képessé váltunk az információ egyre nagyobb távolságra való azonnali eljuttatására is. Az informatika megjelenése lehetővé tette az információk automatizált feldolgozását, majd a távközlés vívmányait kihasználva megérkeztünk az internet korszakába. Mindez azért fontos számunkra, mert a tudati és fizikai tér után a hálózatok világága az információ tárolása és feldolgozására egy új dimenziót nyitott meg számunkra: a kiberteret.

Amennyiben az információ felhasználásával elérhető előnyöket szeretnénk kiaknázni, akkor elsődleges szempontként az információhoz való hozzáférés lehetőségét kell megvizsgálnunk. A tudati, a fizikai és a kibertérben elérhető információk hozzáférhetőségét általánosságban összehasonlítva, akár a hozzáférés technikai lehetőségeit, akár az adott térben elérhető információ mennyiségét tekintve megállapíthatjuk, hogy a kibertérben lévő információ kiemelt és egyre nagyobb jelentőséggel bír.

Nem szabad megfeledkeznünk arról sem, hogy a kibertér rohamosan növekvő adattömegében elérhetőek a saját információink is, így az információhoz való hozzáférés nem csak részünkre nyújt kiaknázható lehetőséget, hanem az esetleges ellenérdekű feleknek is, amelynek megakadályozása érdekében célszerű lépéseket tenni.

Ezeket a szempontokat figyelembe véve egyértelmű, hogy a kibertérben rejlő lehetőségek kihasználására, illetve a szükséges óvintézkedések megtételére egyéni, szervezeti (vállalati, üzleti) és állami szinten is egyre nagyobb az igény. Az igény megfogalmazását követően magától értetődően adódik a kérdés:

Hogyan lehet az igényeknek megfelelő kiberképességet létrehozni, kiépíteni, fejleszteni?

Sajnos erre a kérdésre nincs egyértelmű válasz. A téma vizsgálatát megkezdve egyből szembetűnő, hogy a kiberképességek kialakítása több, egymástól különböző szemléletmód mentén kezdődött meg. Habár a különböző szemléletmód mellett kialakított képességek közt számos hasonlóság is felfedezhető mégis egyértelmű, hogy a kibertér nyújtotta lehetőségek optimális kihasználása önmagában is igen összetett feladat így a megoldás keresése is mélyebb elemzést kíván.

Cikkemben ezt a munkát kezdem meg, amelyben célom a kibertér lényegének és összefüggéseinek, illetve a kibertér kihívásaiban érintett szereplők körének vizsgálata. A vizsgálandó kihívások és szereplők körének meghatározásához - a témában kissé előbbre ugorva – a NATO Kibervédelmi Kiválósági Központja[1] által kiadott békeidejű kibertéri állami tevékenységekkel foglalkozó kiadványban [1] szereplő, az állami és a velük együttműködő szereplőkről szóló cikk [2] gondolatmenetét követtem, amely a kiberképességek kialakításának egy lehetséges megoldási módját vázolja fel.

[1] NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCoE)

A KIBERTÉR

A bevezetésben a kiberteret fontossága alapján, a számunkra egyre jelentősebb értéket képviselő „információ” oldaláról közelítettük meg. Az információ természetes közegét jelentő emberi tudat mellett, a történelem előrehaladtával az információ rajzként, majd írásként tárgyiasulva fizikai formában is elérhetővé vált. Az információ elektronikus tárolásának, feldolgozásának és továbbításának lehetősége új dimenziót nyitott az emberiség számára: a kiberteret.

A Kibertér értelmezése

A fogalom eredetét keresve először a görög „*kübernétész*” görög (jelentése: kormányos) szóból eredő kibernetikával találkozunk. A kibernetika egy komplex tudományos irányzat, amely a szabályozás, vezérlés, információfeldolgozás, -továbbítás általános törvényeit kutatja. A kibernetika alapítójának az amerikai matematikus Norbert Wienert tartják, aki a második világháború alatt a légvédelmi rendszerek matematikai problémáival foglalkozva 1940-ben fogalmazta meg a korszerű számítógépekkel szemben támasztott alapkövetelményeket. A kibernetika szóval először az 1946-ban megjelent könyvében [3] találkozhatunk, amelyben az állatokban és a gépekben zajló információáramlás, hírközlés, vezérlés és ellenőrzés kérdéseivel foglalkozik.

A „kibertér” kifejezést William Gibson amerikai-kanadai sci-fi írónak köszönhetjük, aki már az 1970-es években készült első műveiben foglalkozik a kibernetika és a számítógépes hálózatok emberre gyakorolt hatásával. A kibertér fogalmát először az 1982-ben megjelent "Izzó króm” *(Burning Chrome)* című novellájában [4], majd a szélesebb körben ismert 1984-es Neurománc (*Neuromancer)* című regényében [5] használta. Műveiben a „cyberspace” a fizikai világot jelentő „metaspace”-től elkülönült környezetként jelenik meg.

Az idők folyamán számtalan megfogalmazás született a kibertér meghatározására [3]. Ezek alapján általánosságban a kibertér az elektronikus kommunikációs eszközök és rendszerek (számítógép-hálózatok, telefonvonalak, műholdas rendszerek stb.) és a rajtuk található szolgáltatások, információk alkotta virtuális tér, vagy világ összefoglaló neveként értelmezhető [7].

Az internet térhódításával egyre több korábban független kommunikációs hálózat, rendszer, eszköz és szolgáltatás kerül összekapcsolásra, vagy akár kiváltásra az internettel. Ezen folyamat tükrében nem meglepő, hogy a köznapi szóhasználatban a kibertér fogalmát egyre gyakrabban azonosítják az internettel, illetve a világhálón keresztül elérhető virtuális világgal.

Ugyanakkor a fent összegzett általános, illetve a Magyarország Nemzeti Kiberbiztonsági Stratégiájában található hivatalos megfogalmazásból is kitűnik hogy „kibertér” fogalma tágabb területet fed le: „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint e rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.” [8]
Tehát az interneten kívül a kibertér részét képezik az internettől többé-kevésbé független hálózatok, rendszerek és eszközök is amelyek világhálóhoz való csatlakoztatásuk ezután várható, valamint azok is amelyeknél vállalati (ipari, kereskedelmi, stb.) vagy állami érdekből éppen a világhálótól való minél nagyobb függetlenség megőrzése törekednek. A függetlenség igénye többnyire biztonsági okokra vezethető vissza. Legyen az akár a folyamatos és zavartalan működés biztosítása, vagy akár az információkhoz való jogosulatlan hozzáférés, módosítás lehetőségének csökkentése.

A biztonság szempontjából különösen érzékeny pontot jelentenek a mindennapi életünk biztosítása szempontjából kritikusnak tekinthető infrastruktúrák, mint például az energiaszolgáltatás, közlekedés, víz, vagy az agrárgazdaság részeként az élelmiszeripar. Szintén a kritikus infrastruktúrák körében tartoznak az állam működése szempontjából kiemelt

fontosságú elemek, mint például a kormányzás és a védelmi szektor (rendvédelem, honvédelem, nemzetbiztonság) Az egyes kritikus infrastruktúrák működéséhez szükséges információs rendszerek, kiegészülve az önmagukban is kritikus infrastruktúraként értelmezhető hálózatokkal, rendszerekkel és szolgáltatásokkal (mint például telefon- vagy az internetszolgáltatás) külön kiemelt védelmet igénylő csoportot képeznek, kritikus információs infrastruktúraként. Ezen információs infrastruktúrák működési közegét is a kibertér jelenti. A működési közeget említve nem szabad megfeledkeznünk arról sem, hogy az információs rendszereink, eszközeink közötti kapcsolatot biztosító hálózatok, így vezeték nélküli összeköttetéseket biztosító elektromágneses spektrum is kibertér részeként értelmezhető.

A kibertér védelmi oldalról való megközelítésénél találkozhatunk olyan speciális kibertérben megvalósuló jelenségekkel, tevékenységekkel amelyek önálló szakterületként értelmezhetőek, mint például kiberbűnözés (kiberterrorizmus) elleni küzdelem, vagy a kiberhadviselés. Ezen szakterületek speciális feladatrendszere magával vonja a kibertér sajátos, gyakran bővített értelmezését, mint ahogyan az a következő részben látható.

A kibertér katonai és geopolitikai jelentősége

Katonai szempontból a kibertér a korábbi a fizikai térben lévő szárazföldi, tengeri, légi, kozmikus hadszínterek mellett önálló hadszíntérré vált[2]. Ugyan kibertérről csak néhány évtizede, kiberhadszintérről pedig csak néhány éve beszélünk, az elektronikus adattovábbítás. lehallgatás, zavarás már egy évszázada jelen van a hadszíntereken. A híradás, rádiófelderítés és zavarás után megjelent a rádiólokáció, majd az automatizált adatfeldolgozásra épülve az elektronikus irányítású fegyverek, fegyverrendszerek rendszeresítése vált lehetővé. A távközlés és informatikai fejlődése a hadviselésben is drasztikus mértékű változásokat hozott. Napjainkra a szenzorokra épülő felderítő, azonosító és navigációs, illetve vezetés-irányítási és kommunikációs rendszerek komplex – gyakran integrált – rendszerekké fejlődtek. A rendszerek egyes komponenseinek működése illetve az eszközök közötti adatcsere az elektromágneses spektrum különböző tartományaiban valósul meg [9]. Ebből következően nem meglepő, hogy a kibertér katonai értelmezéseiben kiemelt helyet foglal el az elektromágneses spektrum használata. A Magyar Honvédség kibervédelmi koncepciójában [10] a kibertér meghatározásának középpontjában kifejezetten az elektromágneses spektrum használata áll[3], amely a „kiberkörnyezet" fogalmaként[4] egészül ki a felhasználók, a hálózatok, hardver- és szoftverelemek, folyamatok, szolgáltatások, illetve a kibertérben tárolt és továbbított adatok körével. A elektromágneses spektrum és kibertér elválaszthatatlanságát jól példázza az USA hadserege által alkalmazott „kiber-elektromágneses tevékenységek" terminológia[5], amelynek megfelelően a kibertéri műveletek és az elektronikai hadviselést közös direktíva[6] tárgyalja [11] [12].

[2] 2016 júniusában a NATO varsói csúcstalálkozóján az elektronikus formában lévő információ létezési közegét jelentő kiberteret hivatalosan is elismerik ötödik műveleti dimenzióként a korábbi négy fizikai (szárazföldi, légi, tengeri, kozmikus) hadszíntér mellett.

[3] 0 2. 8) pont szerint: „A kibertér: az elektromágneses spektrum használatával meghatározható, dinamikusan változó tartomány, mely az összekapcsolt hálózatok, eszközök és kiegészítő fizikai infrastruktúrák közötti adatok kezelésére szolgál."

[4] 0 2. 8) pont szerint: „Kiberkörnyezet: felhasználók, valamint a kibertérben lévõ hálózatok, eszközök és minden szoftver, folyamat, tárolt vagy továbbított adat, alkalmazás, szolgáltatás, továbbá a hálózatokhoz közvetlenül vagy közvetetten csatlakozó hálózat"

[5] Cyber Electromagnetic Activities (CEMA)

[6] már a [11] direktíva címében is megjelenik, illetve az ezt kiváltó [12] direktíva is követi a terminológiát

A kibertér katonai értelmezését és jelentőségét röviden áttekintve láthattuk, hogy az elektronikus eszközök és az elektromágneses spektrum használata már a „kibertér" és a „kiberhadviselés" kifejezések megjelenése előtti évtizedekben is általános részét képezte a hadviselésnek. Joggal vetődik fel a kérdés, hogy az állami működés egyéb területein mikor és hogyan vált jelentőssé a kibertér használata, illetve vált geopolitikai tényezővé.

A kibertér geopolitikai szerepének sokáig nem tulajdonítottak jelentőséget, sőt az internet úttörői által létrehozott mozgalmak a 90-es években kibontakozó elméleteik szerint az internetet a vadnyugathoz, mint az amerikai demokrácia bölcsőjéhez hasonlítva az internet szuverenitását hirdették, amelyben a világ kormányainak törvényei nem alkalmazhatóak.

Az internet szabadságát hirdető, napjainkban is fennálló elmélet[7] amely szerint az internet nyitott felépítése, erősen decentralizált, központ nélküli működése éppen a szabad információcsere és szólásszabadság jegyében lett létrehozva annak érdekében, hogy az információ szabadon tudjon áramlani, bármilyen akadály ellenére is. Eszerint az internet olyan világ, ahol minden az emberi elmétől származik, ennek megfelelően újratermelhető és terjeszthető anélkül, hogy pénzbe kerülne [13]. Ez a szabadelvű megközelítés képezi a napjainkban is működő hacktivista mozgalmak alapját. Habár az internet használatával összefüggő fenyegetések már ebben e kezdeti időszakban ismertek voltak, az általuk okozott károk nem érte el azt az ingerküszöböt, hogy az internet szabadelvű használata ne uralkodó nézetként maradjon fenn.

A szabad használat korlátozása elsőként a kiberbűnözés elleni védelem területén jelent meg. A számítógépes bűnözéssel összefüggő paragrafusok az egyes országok törvényeiben már a 80-as években megjelentek. Nemzetközi szinten az első lépést az Európai Tanács 1992-ben elfogadott Maastrichti Szerződése alapján létrejött hárompilléres rendszer megalkotása jelentette, amelynek pilléreit a kiberbiztonság mellett a közös kül- és biztonságpolitika, illetve a kiberbűncselekményekkel kapcsolatos szabályozás képezte.

Az első gyakorlati szempontból jelentős nemzetközi szintű megállapodásként az Európa Tanács Számítástechnikai bűnözésről szóló egyezmény (Budapesti Egyezmény) aláírása 2001-ben került sor, amely a kiberbűncselekmények szabályozása kapcsán a nyugati világ számára egyöntetűen elfogadott etalont jelent [14][14].

A kiberbűnözés számos lehetőséget biztosít a terrorizmus támogatására is. A 2001. szeptember 11-ei események hatására a kiberbűnözésből kiválva – mint annak sajátos és szélsőséges formája – a kiberterrorizmus önálló területként jelent meg. A 2000-es évek kiberterét – a kiberbűnözés és kiberterrorizmus veszélyit ugyan szem előtt tartva – az információs társadalom, illetve az ehhez szükséges infrastruktúra kiépítése jellemezte.

A kibertér védelme szempontjából az első kiberháborúnek tekintett 2007-es észtországi kibertámadás-sorozat jelentette a fordulópontot. Az eset rávilágított arra, hogy a kibertérből érkező koncentrált támadás a polgárok létszükségleteit kielégítő ellátórendszert, illetve ezen keresztül az állam egészének működésképtelenségének mértékét is elérheti. Az eset következtében új lendületet kapott a kritikus infrastruktúrák védelme, illetve egyértelművé tette az állami szerepvállalás jelentőségét kibervédelemi feladatok kapcsán [15]

A következő jelentős esemény a Stuxnet névre keresztelt vírushoz köthető, amely 2010-ben jelentősen visszavetette az iráni atomprogramot. A vírus működésének elemzése több, biztonsági szempontból mérföldkőnek tekinthető tényre mutatott rá. Az igen összetett, nagy szakértelemmel megírt vírus több nulladik napi sérülékenységet kihasználva képes volt úgy

[7] Alix Desforges francia geopolitikus elmélete, amely szerint az internet szabadságága az 1960-as évek kulturális forradalmából eredeztethető.

széles körben rejtetten terjedni, hatását – célzott támadásként– csak a kiválasztott típusú radioaktív izotópok dúsítására használt gázcentrifugákban fejtje ki. A vírus a hálózati kapcsolatokon túl képes volt fertőzni az ipari rendszerek frissítésére használt USB eszközökön át, bizonyítva hogy a hálózatoktól gondosan szeparált rendszerek is sikeresen támadhatóak. Az eset az ipari vezérlők sérülékenységén keresztül rávilágított az ilyen típusú informatikai elemeket tartalmazó – korábban szeparáltságuk miatt is biztonságosnak tartott – kritikus infrastruktúrák fokozott kiszolgáltatottságára. Az eset mérföldkövet jelent a abból a szempontból is, hogy a korábbi kibertámadások csak ”soft” (azaz közvetett módon) okoztak károkat, míg a Stuxnet a gázcentifugák túlpörgetésével közvetlen módon, valódi fizikai kárt tudott okozni, bizonyítva hogy a kiberterrorizmus kapcsán korábban csak elméleti feltételezésként megjelenő „hard” típusú támadások is indíthatóak a kibertérből. [16] 223-227. o.]

A 2010-es Wikileaks kiszivárogtatási botrány, majd az az Edward Snowden által 2013-ban kirobbantott lehallgatási ügy rávilágított arra, hogy a kibertér magában hordozza a nagy mennyiségű érzékeny információ megszerzésének és széles körű megosztásának oly mértékű lehetőségét is, amely alkalmas lehet az egyes országok közötti viszonyok megváltoztatására is.]

A katonai vonatkozásban már a 90-es évek óta komoly jelentőséggel bírnak a kibertérben megvalósuló információs műveletek. Habár az emberi tudat kibertéren keresztüli befolyásolása már az elektronikus média (rádió, TV) megjelenésével megkezdődött, az igazi jelentőségét az internet elterjedésével érte el. Eleinte csak a böngészési előzményeken alapuló reklámok, majd a közösségi média, bloggerek, trollok, és egyéb álhír terjesztők befolyásolták a tudatunkat. A kibertéren keresztüli befolyásolási képesség napjainkra már elérte a felső szintű politika közvetlen befolyásolásának szintjét. [17]

A KIBERTÉR SZEREPLŐI

Az egyes országok kormányai, hadseregei, vállalatai és polgárai az elmúlt évek példáin keresztül szembesültek a kibertér egyre növekvő jelentőségével. A kibertér sajátos környezetében látott példák egyszersmind rávilágítottak a saját érdekek megvédésének szükségére és a lehetőségek megragadásában rejlő előnyökre is.

Ez különösen igaz az állam egészének esetében, amelynek érdeke szemben áll a virtuális ér többi szereplőjével, ezen belül a nem állami szférához tartozó szereplőkkel (kiberbűnözőkkel, a hackerekkel, aktivistákkal, másként gondolkodókkal, a nagy magánvállalatokkal) vagy éppen más államokkal. [2]

A felismerést megfontolt elgondoláson alapuló tettek kell hogy kövessék, Az elgondolást célszerű stratégiagént megfogalmazni, amely felvázolja a jelenlegi állapotot, kitűzi az elérni kívánt célokat, valamint ezek alapján kijelöli a célok eléréséhez vezető utat. A célok eléréséhez szükséges kiberképességek kialakításához több út is vezethet.

Az útkeresés egyik fontos szempontját a kezdeti állapotként rendelkezése álló, illetve a kiberképességek kialakítása során igénybe vehető erőforrások jelentik. A kibertér különböző szereplőit tekintve feltételezhető, hogy az erőforrások elosztásában jelentős különbségeket találhatunk, elég akár csak a rendelkezésre álló anyagi háttérre, vagy akár a szaktudásra gondolni. A kibertér szereplőinek az eltérő státuszukból adódóan a jogi értelemben vett lehetőségei is különbözőek. Ugyanakkor egy állam egy adott kiberképességének létrehozásában több szereplő is érintett lehet függetlenül attól, hogy az állami, vagy nem állami szférához tartozik.

Ennek megvalósítási lehetőségeit vizsgálta Alexander Klimburg [18] is, a különböző szereplők tevékenysége közötti hasonlóságokból kiindulva. Klimburg szerint a számítógépes

bűnözés, a számítógépes terrorizmus és a számítógépes hadviselés közös technikai alapokra épül, hasonló eszközöket, logisztikát, és működési módszereket, ugyanazon közösségi hálózatokat és infrastruktúrákat használva, hasonló célokból. Az egyes kibertevékenységek közötti különbség legtöbbször alig felfedezhető. A kiberhadviselés szemszögéből nézve a kiberbűnözés a technikai, (szoftvereszközök és logisztikai támogatás), a számítógépes terrorizmus pedig társadalmi alapot jelenthet (személyes hálózatok és motiváció) az ellenséges csoportok vagy államok számítógépes hálózatainak megtámadására. A nemzet kibertérben történő erőkifejtése három dimenzióra osztható. Elsődlegesen a kormányzat által kordinált működtetési és szabályozási környezet, a nemzetközi szövetségek illetve nemzetközi jog környezete, valamint a nem állami szereplőkkel történő együttműködés. Habár ezekből az állam számára az első két dimenzió tekinthető alapvetően fontosnak, a kibertér természete olyan, hogy a kiberképességek jelentős része a közvetlen kormányzati ellenőrzésen kívül eső üzleti és a civil szektorban rejlik. A kormányzati és a nem állami szektor együttműködésével integrált nemzeti kiberképesség hozható létre.

A nyugati demokráciák képesek motiválni, vonzani a saját állampolgárait, ami alapvető fontosságú az egész nemzeten alapuló kiberképesség létrehozásához. Az „egész nemzet" (whole of nation) biztonságpolitikai megközelítés a kormányzati és a nem állami (üzleti és civil) szektor a közös célok elérése érdekében tett integrált (egész társadalmat érintő) erőfeszítéseit jelenti, amelynek alkalmazása csak mintegy tíz éve kezdődött az Amerikai Egyesült Államokban. A nyugati országok viszonylag lassan ismerték fel az integrált nemzeti képesség fontosságát Ezzel szemben Oroszország és Kína magasan szinten és jól látható módon alkalmazza a nem állami kiberképességeket. [18]

Nem kétséges tehát, hogy a kiberképességek kialakításának tervezéséhez az első lépést a kibertér állami és nem állami szereplőinek megismerése kell, hogy jelentse.

A kibertér állami szereplői

A kibertér állami szerepét vizsgálva kiindulópontként tekinthetjük azt a tényt, hogy az egyes országok kialakulását és fennmaradását az erőszakszervezeteken a közigazgatáson alapuló hatalom koncentrált gyakorlása biztosítja[8]. A hatalom általánosságban a mások befolyásolására való képességként fogalmazható meg, beleértve a mások befolyásának elkerülését is. Az állam szempontjából a hatalom a nemzeti célok és törekvések megvalósításának eszköze a kormány kezében. [2]; 1.o.] Az állam monopol helyzetét biztosító hatalom megőrzését évszázadokon át a koncentrált fizikai erő garantálta. A kibertér katonai és geopolitikai jelentőségét meghatározó események bizonyítják, hogy a kibertértérben rejlő befolyásoló erő hatalmi tényezővé vált. Ennek nyomán egyre több ország felismerte, hogy az állami érdekek érvényesítéséra a kibertérben is szükség van.

Az állam kibertérben játszott szerepe három fő tevékenységi területe osztható: a kiberbűnözés elleni védelem, a titkosszolgálatokok tevékenységére és a honvédelemre.

A bűnüldözés és jogérvényesítés

A bűnözés elleni védelem, tágabb értelemben a jogrend érvényesítése a kibertérben is elengedhetetlen az állam és polgárainak védelme érdekében.

[8] Max Weber általánosságban használt meghatározása alapján az állam „a fizikai erő legitim használatának monopóliumával egy adott területen belül", amely tartalmazhatja a fegyveres erőket, társadalmi szolgáltatásokat, állami bürokráciát, bíróságokat és a rendőrséget.

Az információs technológia elterjedésével a kibertér használatának előnyeivel párhuzamosan nőtt a visszaélés lehetősége is. A technológia által nyújtott lehetőségek kártékony hatású kihasználása ellen a jogérvényesítés eszközeivel illetve az ezt támogató műszaki módszerekkel lehet fellépni. A jogi eszközök kibertérben történő érvényesítésének első lépése a jogszabályalkotás. Ennek kezdeti lépésit jelentették a számítógépes bűncselekmények korai szabályozása, majd a kiberbűnözés fentebb tárgyalt részletesebb nemzetközi és állami szinten történő szabályozása. Napjainkban a kiberteret érintő jogi környezet részét képezik a kibertér jelentőségét deklaráló és az elérendő célokat, a fő irányokat meghatározó stratégiák, valamint a célok eléréséhez szükséges szervezet- és feladatrendszert rendelő, illetve a szabályokat rögzítő törvények és egyéb jogszabályok.

A jogszabályalkotás az adott ország állami felépítésétől, illetve az adott jogszabálytól függően parlamenti, kormányzati, ágazati feladat. A jog érvényesítése a végrehajtó hatalom, jellemzően a bíróságok feladata. A jogérvényesítés sarkalatos kérdése a bizonyítékok szolgáltatása, amely igen összetett feladatot jelent az ezért felelős nyomozóhatóságok és a bevont szakértők számára. A megbízhatónak tekinthető bizonyítékok gyűjtése az egyéb védelmi szabályok érvényesítésével együtt egyes információkezelő rendszerek üzemeltetőinek a feladata. A rendszerek védelmi feladatai egyaránt igen komoly műszaki és jogi kihívást jelentenek a jog- és egyéb védelmi szabályok alkalmazásért felelős üzemeltetőkre, a jogszabályalkotásért és az egyéb alacsonyabb szintű szabályozás kialakításért felelős, illetve a szabályok érvényesülésének ellenőrzésért felelős felügyeleti szervekre.

A kiberbűnözés elleni küzdelem feladatai általában a rendvédelmi szervek hatáskörébe tartoznak, Ettől eltérően más szervezetek is érintettek lehetnek. A bűnmegelőzés kapcsán kiemelt fontosságú felhasználói tudatosság kialakítása, vagy a megfelelő szaktudás biztosítása kiegészülve az azt megalapozó kutatási feladatokkal, amelyben az oktatási szféra, különösen az egyetemek és a kutatásokban részt vevő szervezetek érintettek. [18]6 o.]

A kiberbűnözés a kiberbűncselekmények mellet magában foglalja a kiberterrorizmus elleni védelmet is. [18] 4, o.] A kibertetrrorizmus elleni védelem, illetve az egyéb kiberbűnözéshez kapcsolódó feledatokban a nemzetbiztonsági szolgálatok is érintettek lehetnek.

A nemzetbiztonsági szolgálatok

Az államok közötti kémkedés közös és meglehetősen hagyományos tevékenység, amely nemzetközileg elfogadott állami gyakorlat, még akkor is, ha a cselekményt mint olyat általában a nemzeti jogrendekben bűncselekménnyé nyilvánítják. A kémkedéssel szinte egyidős az azzal szembenálló elhárítás is. A hírszerzési és elhárítást tevékenységet végző nemzetbiztonsági szervek természetes módon mindig is kihasználták a technika adta lehetőségeket. Az infokommunikációs technika fejlődésével a lehetőségek kiszélesedésében az információk elérhetősége és mennyisége mellett óriási jelentősége van az anonim lehallgatás és beavatkozás lehetőségének. Ugyan a nemzetbiztonsági szervek konkrét képességei általában rejtettek a külvilág számára, az Edward Snowden által kiszivárogtatott adatok rávilágítottak a kibertér nemzetbiztonsági szempontú kihasználáságának mértékére. [2]; 14. o.]

A fegyveres erők

A kibertér katonai alkalmazása az elektronikai hadviselés területén már egy évszázados, a számítógépes rendszerek védelme területén néhány évtizedre nyúlik vissza.

A kibertérben a védelmi a felderítő és a támadó tevékenységek is egyértelműen értelmezhetőek, ennek ellenére a NATO és az egyes országok csak egy-két éve kezdték a kiberteret önálló hadszíntérként értelmezni. Ez részben visszavezethető a kibertér azon sajátosságaira amely jelentősen eltér a hagyományos fizikai térben lévő (szárazföld, tenger, légi, kozmikus) hadszínterektől.

A kibertérben komoly problémát jelent a bizonyíthatóság hiánya. Ez egyaránt igaz a támadást indító eszközök és azok fizikai helyének egyértelmű azonosítására. Ennél is nagyobb

problémát jelent a szemben álló fél személyének, szervezeti hovatartozásának, országának azonosítása. Nincs közös nemzetközi jogalap arra sem, hogy milyen típusú célpontok ellen, milyen jellegű illetve mértékű támadás tekinthető katonai értelemben vett kibertámadásnak.[15]; 35-38].

A kibertér nem állami szereplői

Hackerek

Az internet fejlődése a hackerek felemelkedésével járt. A hackerek az informatikai iránt érdeklődő, többnyire a fiatalabb generációkba tartozó személyek, akik informatikai rendszerek, szolgáltatások feltörésével kezdtek foglalkozni, elsősorban a kíváncsiság és a felfedezés öröme által hajtva. A hackerek figyelemre méltó célpontok kiválasztásával, látványos módon történő feltörésével, vagy az onnan megszerzett adatok által hírnévre tettek szert. Fontos megemlíteni hogy maga a hackelés sokáig nem számított bűncselekménynek. A büntető törvénykönyvek többnyire nem a hackelés cselekményét rögzítették annak hatása alapján. Ha az esetek kivizsgálására került sor akkor legfeljebb más jogi normák, például a szerzői jogok megsértése, vagyontárgyakban okozott károk képezték a jogalapot.

A jogi megítélés alapján szokássá vált a hackerek megkülönböztetése. A jogszabályok keretein belül tevékenykedő ártalmatlan hackereket fehér, az azokat átlépő rosszindulatú tevékenységet folytatókat fekete, illetve a mindkét oldalon tevékenykedőket szürke kalapos hackerként emlegetve. A valóságban igen nehéz különbséget tenni, sok esetben a jogi megítélés egyértelműen nem tisztázható. Gyakran előfordul, hogy a politikai, vagy a média általi megítélés dönti el az egyes esetek, vagy a hackerek megítélését. Az infokommunikációs technológiák és a szolgáltatások globális piaccá válásának köszönhetően a rendszerekkel és szolgáltatásokkal szembeni rosszindulatú tevékenység, az adatok megszerzéséhez jövedelmező szakmává vált, sokakat arra ösztönözve, hogy erre a területre szakosodjanak.

Napjainkra kialakult az a jogi szempontból is elfogadott etikus hackelésnek nevezett tevékenység amely a biztonsági üzletág keretein belül segít megvédeni az ügyfeleket a rosszindulatú szereplők ellen. Az etikus hackelés során úgynevezett (sérülékenységi) teszt keretében az ügyfelek beleegyezésével tesztelik a rendszer biztonsági mechanizmusait, amelyek célja a biztonsági szint emelését segítő javaslatok megfogalmazása. Másrészt az informatikai biztonsági szakértőknek is szüksége van hackerek támadási technikáinak ismeretére, ezzel szilárd alapot nyújtva a támadások gyakoriságának és általuk az okozott károk csökkentésére vagy megakadályozása, vagyis a megfelelő védelem kialakításához. Az informatikai biztonsággal foglalkozó oktatásra is specializálódott cégek napjainkban már széles körben elérhetővé tették a tanúsított etikus hacker[9] és hálózabiztonsági[10] képzéseiket.

A szürke kalaposként említett hackerek céljukként a kibertér biztonságosabbá tételét tekintve, a szélesebb közösség érdekében használják képességeiket. Ugyan tevékenységüket a rosszindalatú felekkel szemben fejtik ki, cselekedeteiket ugyanúgy jóváhagyás nélkül végzik, így az egyes rendszerekben szolgáltatásban felhatalmazás nélkül elkövetett beavatkozásuk, jogi értelemben ugyanúgy bűnnek számít. Tetteik igazolását – mint a jó szándéktól vezérelten a magasabb eszmék megvalósításaként – az egyes szolgáltatások, az internet és kibertér biztonságosabbá tételére való törekvésükre való hivatkozásban látják. A szürke kalaposok néha azzal is kárt okoznak, hogy a rendszerek, szolgáltatások sérülékenységeit nyilvánosságra hozzák vagy kiszivárogtatják, viszont ők ezt megelőzően általában kapcsolatba lépnek az

[9] CEH: Certified Ethical Hacking
[10] CNDA: Certified Network Defense Architect

érintett tulajdonosokkal, üzemeltetőkkel, akár a biztonsági hibák elhárításához szükséges információkat is megosztva velük.

A fekete kalapos hackerekkel is előfordul hogy felkeresik az érintetteket, viszont azt többnyire zsarolási szándékkal teszik. A fekete kalapos hackereket elsősorban személyes haszonszerzésre használják készségeiket és tudásukat. Hírnevük többnyire arra vezethető vissza, hogy valamilyen ellenszolgáltatás fejében tesznek, vagy éppen nem tesznek meg valamit. [2]

Kiberbűnözők

A 20. század végét jellemző jelentős infokommunikációs beruházásoknak, informatikai biztonsági fejlesztéseknek köszönhetően, illetve a nagyobb rendszerekben megvalósítható jogosulatlan hozzáféréshez szükséges készségszint jelentősen megnőtt. Ugyanakkor a rohamosan növekvő számú – jellemzően alacsony biztonságtudatossági szinttel rendelkező – internetfelhasználók gyakran a megfelelő védelem nélkül alakították ki a számítógépes rendszereiket. Ez a jelenség gyökeresen megváltoztatta a számítógépes bűnözés jellegét.

Ezen túlmenően a számítógépes bűnözés nemzetközi szabályozásának, és a már elfogadott egyezmények országonkénti alkalmazásának hiánya, illetve a korlátozott együttműködés, nagymértékben segítették az óriási bevételeket produkáló globális számítógépes bűnözés kialakulását.

Az elmúlt két évtizedben olyan rejtett gazdaság alakult ki, amelyben viszonylag alacsony összegért bárki hozzájuthat bűncselekmények elkövetéséhez használható szoftverkomponensekhez, adatbázisokhoz, és akár támogató szolgáltatásokhoz is. Ráadásul ezek viszonylag alacsony számítógépes ismeretekkel is komoly eredményeket produkáló kiberbűncselekmények elkövetésére alkalmas eszközzé állíthatóak össze. [2]

Hacktivisták

A hacktivizmus (hacktivism) a hackelés (hacking) és az aktivizmus (activism) kifejezéséből összeállított mesterséges szó, amelyet 1996-ban alkotott meg a Cult of the Dead Cow[11] hackercsoport egyik tagja.

A hacktivizmus a szólásszabadság, az emberi jogok és az információ szabadsága jegyében. számítógépes hálózatokon (általában az interneten) a hackerek által használt eszközöket alkalmazó aktivista mozgalom, Lényegét tekintve a hagyományos demonstrációk és polgári engedetlenség digitális megfelelői.

A hacktivisták a szürke kalapos hackerekhez hasonlóan, az írott jog szempontjait az etikai, illetve morális szempontoknak rendelik alá. Célpontjaik azok a mozgalom ellenfélként azonosított szervezetek, vállalatok és egyének, amelyek a hacktivista csoport rendelkezésre álló eszközökkel sikeresen támadhatók, és annak eredménye a figyelem felkeltésére alkalmas. A sikeresen támadott célpontok között számos nagyváros honlapja mellett már szerepelt a Sony, az USA szenátusa és hadserege, a CIA, az FBI, és számtalan más szervezet, amelyek támadása nagy hírveréssel járt.

Az alapvető hacktivista módszerek három csoportra oszthatók. Ezek közül legalapvetőbb az adott ügy melletti tömegtámogatás demonstrálására használt túlterheléses támadás[12], amelyet lényegében az ülősztrájk virtuális megfelelőjének tartanak .

A második – talán legjellemzőbb – hacktivista eszköz a weboldalak feltörése és átalakítása (defacement), ami a túlterheléses támadással szemben konkrét üzenetek megfogalmazására

[11] Cult of the Dead Cow: (A Döglött Tehén Kultusza) Az egyik első nevezetessé vált, 1984-ben a Texasban alakult hackercsoport

[12] DDoS: Distributed Denial of Service

alkalmas, ráadásul ezzel a módszerrel az üzenet közvetlen megjelenítése, közzététele, magán a megtámadott felületen történik. A weboldalak feltörésének és átalakításának eredeti – fizikai térben megvalósuló – a falfirka, vagy plakátok felülragasztása, átalakítása.

A hacktivista eszköztár harmadik csoportját a betörés, Információszerzés és kiszivárogtatás jelenti, ami tulajdonképpen a klasszikus hacker módszerek hacktivista csoportok általi használatát jelenti. Ebben az esetben a cél a weboldalak, adatbázisok, e-mail fiókok feltörése és az így szerzett információ kiszivárogtatása, nyilvánosságra hozatala.

A 2010-es évek elején elindult változás során a korábbi kisebb hacktivista csoportok hálózatba szerveződve olyan globális hacktivista mozgalmakká álltak össze mint az Anonymous, a LulzSec, az Indignados, vagy az Occupy

Közös vonásuk, hogy alapvető céljuknak tekintik a szabad terek megteremtését, legyen szó a kibertérről, vagy a közterekről, a politika, vagy a közbeszéd tereiről, ezért összefoglaló néven a „Terek Mozgalmaiként" nevezik őket.

Létrejöttükkel – kihasználva a kor technikai lehetőségeit – az alulról építkező civil hálózatok korábban nem látott globális kiterjedtségét és egyidejű szervezettségét valósították meg. A Terek Mozgalmai a 2011-ben, illetve az azóta kibontakozó világméretű tüntetéshullámok során példátlan összehangoltságról tettek tanúbizonyságot. [2] [20]

A felhasználók

A kiberszereplők ismertetésének végén – de nem utolsó sorban – szót kell ejtenünk az átlagos felhasználóról, aki egyrészt saját eszközeivel, információival, profiljával, tudati befolyásával és befolyásolhatóságával megjelenik a kibertérben. Másrészt a felhasználó mindennapi élete függ azoktól a kritikus infrastruktúráktól, amelyek mögött sérülékeny infokomunikációs rendszerek működnek. A felhasználó részese lehet a kibertérben folyó támadásoknak akár elkövetőként (ha nincs is tudatában) vagy áldozataként. A felhasználónak saját érdeke, hogy ezek ellen lépéseket tegyen. Ugyanakkor az államnak is felelőssége van abban, hogy az állam – beleértve a polgárai – kibervédelméről gondoskodjon.

ÖSZZEFOGLALÁS

Az egyes országok tekintetében az állam képezi a hatalom megtestesülését. A hatalom megtartását, az álam fennmaradást évszázadokon keresztül fizikai erővel kellett garantálni. A cikkben kiemelt események rávilágítottak arra, hogy az információtechnológi fejlődésével a kibertérben olyan mértékű lehetőségek és veszélyek rejlenek amelyek – akár az infrastuktúrákon, akár az állampolgárokon keresztül – komoly hatást gyakorolhatnak az állam működésére. A kibertér megnövekedett jelentőségét az egyes országok és szervezetek, szövetségek felismerték és lépéseket tesznek az érdekeik kibertérben is megvalósuló érvényesítése érdekében. Az ennek érdekében megfogalmazott stratégiai célok csak a megfelelő kiberképességek kialakításával illetve fejlesztésével érhetők el. A kiberképességek kialakítása már elgondolás szintjén is igen komoly feladatot jelent, mivel a megvalósítás a legtöbbször csak igen összetett és sajátos, sokszor még ismeretlen megoldásokon keresztül történhet. Célom ezen kiberképességek kialakításának kutatása, amelynek keretében ebben a cikkben a kibertér értelmezésén kívül áttekintésre kerültek a kibertér azon szereplői, amelyek jelentős szerepet játszhatnak az egyes kiberképességek kialakításában.

A kibertér szereplőinek áttekintése alapján megállapítható, hogy azok tevékenysége közös technikai alapokra épül. Hasonló eszközöket és működési módszereket, valamint többnyire ugyanazon infrastruktúrákat, hálózatokat és szolgáltatásokat használják. A különbségek jellemzően a motivációban a tevékenység társadalmi elfogadottságában és jogszerűségében, illetve az adott keretek közt elérhető eredményekben fedezhető fel. Az állami oldalon világosan körvonalazódik a kibertér feletti érdekérvényesítő képesség megszerzésének és fenntartásának szükségessége. Ehhez rendelkezésre áll az állam saját szervezeteinek képességei, amelyek

alkalmazásához biztosítottak a jogi keretek, kiegészülve a nemzetközi együttműködés lehetőségeivel. Ezzel szemben a nem állami szereplők között felfedezhetők társadalmi vagy etikai szempontból elfogadhatónak tartott, mégis egyes esetekben a jogszerűség határát súroló tevékenységek is. Ugyanakkor ezek a képességek igen hatásosak, viszont az állam – a jelenlegi jogi keretekből adódó korlátok miatt – azokat közvetlenül nem használhatja. Mivel az államnak szüksége lehet a nem állami képességek – akár közvetett módon történő – kiaknázására is, célszerű lehet amerikai, orosz és kínai példákkal alátámasztott integrált nemzeti képességek alkalmazási lehetőségeit vizsgálni.

FELHASZNÁLT IRODALOM

[1] ZIOLKOWSKI, K (Ed.): *Peacetime Regime for State Activities* In: *Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013. https://ccdcoe.org/sites/default/files/multimedia/pdf/PeacetimeRegime.pdf (letöltve: 2017.10.09.)

[2] CZOSSECK, C. *State Actors and their Proxies in Cyberspace* In: ZIOLKOWSKI, K (Ed.): *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013. pp. 1-29.

[3] WIENER N.: Cybernetics or Control and Communication in the Animal and the Machine The Massachusetts Institude of Technology, Cambridge, 1961, p. 212, ISBN: 0-62-230007 https://uberty.org/wp-content/uploads/2015/07/Norbert_Wiener_Cybernetics.pdf

[4] GIBSON, W.: *Izzó króm*, In: GIBSON, W.: *Izzó króm*, ford.: Bárday Tamás, Gáspár András, Hoppán Eszter, Szántai Andrea, Szántai Zsolt, Valhalla Páholy, 1997, pp. 133-163., ISBN 9639039284)

[5] William GIBSON: *Neurománc*, ford.: Ajkay Örkény, Valhalla Páholy Kft., Budapest, 1992, p.344 ISBN: 963-7632-05-0

[6] HAIG Zs.: *Információ, társadalom, biztonság*. NKE Szolgáltató Kft., Budapest, 2015. 978-615-5527-08-1

[7] HAIG Zs.: VÁRHEGYI I.: *A cybertér és a cyberhadviselés értelmezése*. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 18: (Elektronikus szám) 2008. pp. 1-12. http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf (letöltve: 2017.10.16.)

[8] A Kormány 1139/2013. (III. 21.) Korm. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról http://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf (letöltve: 2017.11.08.)

[9] HAIG Zs, Kovács L, Ványa L, Vass S, Németh András (szerk.).: *Elektronikai hadviselés* Budapest: Nemzeti Közszolgálati Egyetem, 2014. 271 p. (ISBN:978-615-5305-87-0) https://opac.uni-nke.hu/webview?infile=&sobj=9276&source=webvd&cgimime=application%2Fpdf%0D%0A (letöltve: 2017.11.08.)

[10] 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról. Hivatalos Értesítő, a Magyar Közlöny melléklete, 2013. 48. sz., Magyar Közlöny Lap- és Könyvkiadó, 2013. pp. 13873-13882. http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2013/10.pdf (letöltve: 2017.11.22.)

[11] FM 3-38 *Cyber Electromagnetic Activities*, Headquarters, Department of the Army Washington, DC, 12 February 2014. https://fas.org/irp/doddir/army/fm3-38.pdf (letöltve: 2017.11.22.)

[12] FM 3-12 *Cyberpace and Electronic Warfare Operations*, Headquarters, Department of the Army Washington, DC, 11 April, 2017. https://fas.org/irp/doddir/army/fm3-12.pdf (letöltve: 2017.11.22)

[13] DOUZET, F.: *Geopolitika a kibertér megértéséhez*, In: Pintér István (szerk.) Műhelymunkák: A virtuális tér geopolitikája. 367 p. Budapest: Geopolitikai Tanács Közhasznú Alapítvány, 2016. pp. 19-41. (ISBN:978-963-9816-34-3) http://mek.oszk.hu/16100/16182/16182.pdf (letöltve: 2017.12.27.)

[14] DORNFELD L.: *A kibertér főbb nemzetközi és nemzeti szabályozásai*, In: Pintér István (szerk.) Műhelymunkák: A virtuális tér geopolitikája. 367 p. Budapest: Geopolitikai Tanács Közhasznú Alapítvány, 2016. pp. 43-88. (ISBN:978-963-9816-34-3) http://mek.oszk.hu/16100/16182/16182.pdf (letöltve: 2017.12.27.)

[15] KOVÁCS L, ILLÉSI Zs.: Cyberhadviselés HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA XXI.:(1-2.) pp. 29-41. (2011) http://www.mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_5.pdf (letöltve: 2017.12.14.)

[16] KOVÁCS L, SIPOS M.: A Stuxnet és ami mögötte van II.: Célok és teendők HADMÉRNÖK VI:(1) pp. 222-231. (2011) http://www.hadmernok.hu/2011_1_kovacs_sipos.pdf

[17] KOVÁCS L, KRASZNAY Cs: *Mert övék a hatalom: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során*, STRATÉGIAI VÉDELMI KUTATÓ KÖZPONT (ELEMZÉSEK) / CENTER FOR STRATEGIC AND DEFENSE STUDIES ANALYSES Budapest, 2017:(9) (2017) pp. 1-11. http://archiv.netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-9-az-internet-politikat-is-befolyasolo-hatasa-a-2016-os-amerikai-elnokvalasztas-soran-kovacs-l-krasznay-cs.original.pdf (letöltve: 2018.01.15.)

[18] KLIMBURG A.: *Mobilising Cyber Power*, Survival - Global Politics and Strategy, London, 2011. pp.41-60. (letöltve: 2017.12.27.) http://users.clas.ufl.edu/zselden/coursereading2011/klimcyber.pdf (letöltve: 2018.01.15.)

[19] KRASZNAY Cs.: *A rendvédelmi szervek helye a kibervédelemben* MAGYAR RENDÉSZET XIII:(különszám) (2013) pp. 109-118. http://krasznay.hu/presentation/rendvedelem_krasznay.pdf (letöltve: 2018.01.15.)

[20] A Terek Mozgalmai – Kezdőoldal http://hu.occupy.wikia.com/wiki/Occupy-wiki (letöltve: 2018.01.22.)