Szabó Imre
(tudományos segédmunkatárs, OKRI)

Informatikai bűncselekmény, informatikai terrorizmus vagy informatikai hadviselés?

1. Mi történhetett a bushehri atomerőműben?

Az informatika és a büntetőjog kapcsolata ismételten előtérbe került 2010. szeptember 21-én, amikor egy német biztonságtechnikai szakértő, a 2010 júliusában először detektált Stuxnet malware[107] (vírus) elemzését követően bejelentette, hogy álláspontja szerint a Stuxnet egy célzott informatikai támadás eszköze, melynek célpontja az iráni atomprogram volt.[108] Okfejtése szerint erre enged következtetni az a tény, hogy a Stuxnet kifejezetten azokkal a Siemens szoftverekkel (pl. nukleáris meghajtású repülőgép-hordozókon is futó Siemens szoftver) kerül aktív kapcsolatba, melyek a cég speciális ipari létesítményekben alkalmazott gépeit – mint amilyenek a bushehri atomerőműben is üzemelnek – irányítják. Feltételezését azzal támasztotta továbbá alá, hogy a vírus a legnagyobb fertőzést Iránban, Indiában, Pakisztánban okozta, ezzel egy időben pedig Irán bejelentette, hogy bushehri atomerőmű beindítását legalább három hónappal elhalasztja.

A Symantec biztonságtechnológia cég a vírus hosszas vizsgálata után sem tudta pontosan meghatározni annak célját, működését, ugyanis a vírus különböző ipari környezetben alkalmazott szoftvereknél különböző eredményeket produkált. A tesztek során megállapítható volt azonban az, hogy a Stuxnet a települést követően módosítja a Siemens program kódjának azokat az elemeit, amelyek ipari létesítményekben alkalmazott vízpumpák, nukleáris centrifugák automatikus számítástechnikai feldolgozási folyamatait irányítják. Például egy vízpumpa, ami a gyári programozás szerint 3 másodpercig üzemelt egy automatizált folyamatban, az a fertőzést követően 150 másodpercig üzemelt.

---

[107] A rosszindulatú számítógépes szoftverek összefoglaló neve.

[108] A témához kapcsolódóan nagyon sok információ napvilágot látott. A tanulmány gondolatmenetéhez elegendő csupán a legfontosabb tényeket kiemelnem. Nem célom a helyzet nemzetközi jog szerinti elemzése, elsődlegesen az informatikai támadások büntetőjogi megítélésének bemutatásához hívom segítségül ezt a közismert eseményt.

A vírus fertőzésének módszere az alábbiak szerint foglalható össze: a vírus legfontosabb tulajdonsága, hogy USB tároló eszközökön[109] keresztül terjed. A vírus az USB eszközön parancsikon fájlban .lnk fájlformátumban található (rootkit vírus), ami a vírusellenőrző szoftverek nélkül vagy nem frissített vírusadatbázissal rendelkező vírusellenőrző szofverekkel üzemelő számítógépen az eszköz tartalmának megnyitásakor aktiválódik. A vírus aktiválását követően meghatározott Siemens szoftvereket keres a megfertőzött számítógépen. Ezek a szoftverek MS SQL adatbázissal dolgoznak, amelynél a vírus egy ismert biztonsági rést kihasználva jut el az adatbázis elemeihez, melyben aztán adatokat változtat meg.
Az USB eszköz segítségével történő terjedés módszerének a célja tipikusan az, hogy olyan számítógépekkel is kapcsolatba kerüljön a vírus, amelyek nincsenek közvetlenül az Internethez csatlakoztatva, vagyis amelyekkel szemben online támadást nem lehet végrehajtani.
Ha feltételezzük, hogy a vírus írójának az volt a célja, hogy elérje a bushehri erőművekben található – egyébként kritikus infrastruktúrát irányító – számítástechnikai rendszereket, akkor viszonylag rövid idő alatt sikerült ezt teljesítenie, csupán annyit kellett tennie, hogy a vírust elszabadította valahol, és megvárta, amíg az eljut a célgépekhez, ahol a vírus kódjában található feltételek teljesülése miatt automatikusan aktiválódik.

A vírusfertőzés módszerének vélhetően sikeres alkalmazása miatt[110], az informatikai támadásokhoz kapcsolódóan újra át kell gondolni azt a számunkra kedvező feltételezést, miszerint a kritikus infrastruktúrákhoz kapcsolódóan nincs okunk informatikai támadásoktól tartanunk, tekintettel arra, hogy ezeket az infrastruktúrákat működtető számítástechnikai rendszerek nincsenek az Internethez csatlakoztatva, így nem érheti őket onnan támadás.

A különböző médiumokban megjelent információk azt is sugallták azonban, hogy itt másról is szó lehet, mint pusztán informatikai támadásról. Egyesek egyenesen az informatikai hadviselés egy új fejezetének kezdeteként aposztrofálták az eseményeket. Milyen következtetések vonhatóak le a megvalósult eseményekből?[111]

---

[109] A pendrive (USB-flash-tároló, USB-kulcs, pendrájv, tollmeghajtó) egy USB-csatlakozóval egybeépített flash memória.

[110] Irán elismerte ugyan a vírusfertőzések tényét, de cáfolták azt, hogy ténylegesen károkozás történt volna.

[111] Távol álljon tőlem, hogy pusztán a médiumokból hallott információk alapján messzemenő következtetést vonjak le, a helyzet ellentmondásosságára tekintettel azért érdemes elgondolkozni

2. Az informatikai támadások elhatárolása

Az informatikai bűncselekmények[112] határterületén két másik kriminológiai kategória is megjelenik: az egyik az informatikai terrorizmus, a másik pedig az informatikai hadviselés. Mitől lesz egy informatikai bűncselekmény terrorcselekmény, illetve mikortól beszélhetünk informatikai hadviselésről?

A terrorcselekmény és a terrorcselekmény eszközcselekményeiként meghatározott bűncselekmények közötti alapvető különbség a cselekmény motívumában, illetőleg célzatában ragadható meg.[113] A terrorcselekménynél ez a célzat politikai (társadalompolitikai, valláspolitikai stb.) motivációból fakad, míg egyéb esetben a motiváció többnyire az elkövető személyéhez, személyiségéből fakadó igényeihez kötődik. A hazai hatályos szabályozásban abban az esetben, ha a számítástechnikai rendszer elleni cselekményhez mint a Btk. 261.§-ában foglalt terrorcselekmény bűncselekmény eszközcselekményéhez a törvényi tényállásban meghatározott célzat is társul, akkor informatikai terrorcselekményről beszélhetünk. Ilyen például a Btk. 261.§ (1) bekezdésének c) pontjában foglalt célzat is: más állam alkotmányos, társadalmi vagy gazdasági rendjének, nemzetközi szervezet működésének megzavarása.

Az informatikai hadviselésről akkor beszélhetünk, ha a katonai műveleteket virtuális térben viszik végbe[114], vagyis többek között az is ide tartozik, ha a számítástechnikai bűncselekmények körébe tartozó cselekmények elkövetésére katonai művelet keretében kerül sor. Az informatikai hadviselés elsősorban nem igazságszolgáltatási, hanem biztonságpolitikai (védelmi, katonai) kérdés, ezért ennek részletezésébe nem szívesen bocsátkoznék.

A jelen ügyhöz kapcsolódó speciális célzatú informatikai támadásokra vonatkozó ismeretek az informatikai terrorizmushoz kapcsolódó kutatások eredményeihez kapcsolódónak, így az ott megismert kategóriák segítséget nyújtanak a cselekmények megkülönböztetésében.

---

néhány az esetből következő eshetőségen. Kérem, a t. olvasót ebből a szempontból ítélje meg a tanulmányt.

[112] A téma szempontjából jelen esetben a Btk. 300/C.§-ában foglalt számítástechnikai rendszer és adatok elleni bűncselekmény bír jelentőséggel.

[113] Ilyen eszközcselekmény például a Btk. 300/C.§-ában foglalt bűncselekmény is.

[114] Steven A. Hildreth, Cyberwarfare, Congressional Research Service (June 19, 2001). http://www.fas.org/irp/crs/RL30735.pdf

Az informatikai terrorizmus három fő fejlődési iránya különböztethető meg: informatikai terrorizmus, mint a rombolás, pusztítás eszköze (weapon of mass destruction); mint a társadalmi bizalom megdöntésének eszköze (weapon of mass disruption); és mint a tömeges zavarkeltés eszköze (weapon of mass distraction[115]).[116] A buschehri atomerőművet érintő informatikai támadással kapcsolatban az első két kategóriának van jelentősége.

A tömeges pusztítás (weapon of mass destruction) kategóriájához azok a cselekmények tartoznak, melyek olyan számítástechnikai rendszereket érintenek, melyek közveszély előidézésére alkalmas berendezéseket kontrollálnak. Susan W. Brenner szerint, ha egy terrorcselekmény elkövetéséhez számítástechnikai eszközöket használnak, attól még nem beszélhetünk informatikai terrorizmusról. Ennek oka pedig az, hogy amennyiben a közveszélyt kontrolláló számítástechnikai rendszerek elleni támadás után a berendezés ténylegesen közveszélyt idéz elő, akkor azzal nem informatikai katasztrófa valósul meg, hanem például vasúti tömegszerencsétlenség stb. Vagyis az ilyen típusú cselekmények esetén tág értelemben vett informatikai terrorizmusról beszélhetünk.

A társadalmi bizalom megdöntésének (weapon of mass disruption) eszköztára nagyon széles. Ebbe a körbe tartoznak azok a cselekmények, melyeket a szakirodalom az „elektronikus dzsihád" kategóriájába[117] sorol. Az ilyen típusú, informatikai terrorcselekmény körébe vonható magatartások elsődleges célpontjai a kritikus infrastruktúrához kapcsolódó eszközök, szoftverek, adatbázisok (energiaellátás, közlekedés, egészségügyi informatika, e-közigazgatás, infokommunikációs szolgáltatások). A támadások célja, hogy az infrastruktúra működésébe vetett bizalom megdöntésével demoralizálja a

---

115 A tömeges zavarkeltés (weapon of mass distraction) lényege a civil lakosság pszichológiai manipulációja. Ide tartozik minden magatartás, melynek célja a civil lakosság demoralizálása azáltal, hogy a lakosságnak a kormányzat hatékonyságába vetett hitét megingatja. A társadalmi bizalom megdöntése és a tömeges zavarkeltés közös eleme a lakosság pszichikai befolyásolása. Míg az utóbbi tisztán pszichikai következményeket eredményez, addig az előbbinél tényleges fizikai beavatkozás is megvalósul azáltal, hogy az érintett számítástechnikai rendszerek működésének akadályozása bekövetkezik.

116 Susan W. Brenner: Cybercrime, Cyberterrorism and Cyberwarfare. In: International Review of Penal Law, Cybercrime. 2006. 77 année nouvelle série ¾ trimesters

117 A tipikus hackertámadások körét foglalja magába. Az interneten számos – terroristák által publikált – forrás található az egyes támadások elkövetésének módszertanáról. Ezeken az oldalakon a módszertani útmutatók mellett számos szoftver is elérhető, mely az elkövetést hivatott elősegíteni. Ilyen gyakorlati útmutató például a „The Encyclopedia of Hacking the Zionist and Crusader Websites" és a „39 Ways to Serve and Participate in Jihad" címet viselő és online elérhető művek is.

lakosságot. A támadás az adott rendszer leállását eredményezheti, azt a látszatot keltve ezáltal, hogy az állam nem képes megvédeni a társadalom működésének alapstruktúráit.

A tömeges pusztítás következménye elsősorban fizikai (tangibilis) eredmény, mely közvetlenül a megtámadott információs rendszer által működtetett eszközöknél jelenik meg, míg a társadalmi bizalom megdöntésénél digitális (intangibilis) eredményről beszélhetünk. A digitális eredmény során az adatokat törlik, megváltoztatják, hozzáférhetetlenné teszik stb., és ennek következményeként tipikus esetben a számítástechnikai rendszer működését akadályozzák.[118]

Irving Lachow és Courtney Richardson elmélete[119] – mely az Amerikai Egyesült Államok és az iszlám terrorista csoportok közötti háborút elemzi – rámutat arra, hogy a terroristák az internetet az USA nemzeti védelmének megsértésére használják. Ezt a tevékenységet azonban nem azáltal valósítják meg elsődlegesen, hogy kritikus infrastruktúrák, illetőleg katonai célpontok ellen intéznek számítástechnikai támadásokat, hanem azzal, hogy aláássák a kormány katonai és diplomáciai erőfeszítéseit, melynek célja az ideológiák harcának megnyerése (to win the war of ideas).[120] Ez alapján azt mondhatjuk, hogy az informatikai terrorizmus legfontosabb célja az, hogy a társadalom fenyegetettség-érzetének szüntelen gerjesztésével az állam cselekvőképességébe vetett bizalmat lerombolja, és ilyen módon valóságosan is aláássa az állam képességét abban, hogy az események felett kontrollt

---

[118] A tudás egyik megjelenési formája a technológia, ami a javak és szolgáltatások előállításához szükséges módszerek és eszközök összességeként definiálható. A technológia lehet tangibilis vagy intangibilis. A tangibilis tudás és technológia gépek, eszközök, tőkejavak formájában ölt testet, míg a technológia intangibilis formája a tárgyi eszközökben meg nem testesült, a termelési folyamattal kapcsolatos azon tudáselemeket foglalja magába, amelyek speciális minőségű javak speciális folyamatok segítségével történő előállításához szükségesek (Artenberg 1999). Artenberg, Peter (1999): Technology Transfer and New Institutional Economics. Dissertation zur Erlangung des akademischen Grades eines Doktors der Sozial- und Wirtschaftswissenschaften an der Wirtschaftsuniversitat Wien. Wien, 1999. Oktober.

[119] Irving Lachow and Courtney Richardson: Terrorist Use of the Internet. The real Story., JFQ/issue 45,2nd quarter 2007. ndupress.ndu.edu (2009.10.15.)

[120] Az USA politikai kommunikációjának jellemzője az alábbi példában jól tetten érhető: A szovjet-afgán háború idején az amerikai sajtóban gyakran előforduló kifejezések voltak a „jihad" és a „mujahideen". Az előbbi jelentése szabad fordításban „igyekvés Istenhez", míg az utóbbi „szent harcost" jelent. Az amerikai – afgán konfliktus idején a médiában már megjelentek a „hirabah" és az „irhabists" kifejezések, melyek jelentése istentelen háború és terrorista.

gyakoroljon (kormányzati politika befolyásolása, kormányzat kényszerítése, civil lakosság fenyegetése).

Ha a Stuxnet támadás célja az volt, hogy az iráni végrehajtó hatalom társadalmi megítélésére negatív befolyást gyakoroljon azáltal, hogy az általuk működtetett kritikus infrastruktúrát veszi célba, akkor a cselekmény, fenti csoportosítás szerint a társadalmi bizalom megdöntése (weapon of mass disruption) köréhez tartozik. Ebben az esetben a támadás egyértelmű üzenete az, hogy az atomerőmű berendezése sebezhető, és az maradhat annak beindítását követően is. Az eset azonban ennél messzebb mutat, ugyanis jelen esetben a társadalmi bizalom megdöntésének eszközéül olyan számítástechnikai rendszert állítottak a támadás célpontjába, amely ellen végrehajtott támadás tömeges pusztítás (weapon of mass destruction) kategóriájába sorolható, azzal, hogy a támadás a még üzembe nem helyezett rendszerrel szemben valósították meg. Ez a támadás tehát túlmutat a 2007-ben az „ideológiák harcának" aposztrofált időszakon.

Mindenesetre az informatikai támadások három csoportjának elhatárolása további nehézségekbe is ütközik, melyet egy példával illusztrálnék.

2006 októberében az USA egyik kiemelt beruházásokat kezelő hivatalának számítástechnikai rendszerét támadás érte. A támadás miatt a hivatal megszüntette az internetes kapcsolatot a rendszerrel, aminek következtében a hivatal nem tudta teljesíteni a hatáskörébe utalt feladatainak nagy részét.[121] A támadás nyomai kínai közvetítő szolgáltatók által biztosított kapcsolaton keresztül, Kínában található számítógépekhez vezettek. (Bár arra vonatkozóan volt információ, hogy a támadás egy Kínában található számítógépről érkezett, azonban az már nem derült ki, hogy azt a számítógépet csupán felhasználták a támadáshoz, és az elkövető valójában egy teljesen másik országban indította el az informatikai folyamatokat.) Az elkövetőt nem sikerült felderíteni. Az elkövető az internethez kapcsolódó lehetőségeket kihasználva megőrizte anonimitását. Ebből adódóan azonban nem volt lehetséges eldönteni, hogy az elkövetőt egyéni céljai vezérelték, esetlegesen terrorista célzatú támadást hajtottak végre a hivatal ellen, vagy pedig valamilyen katonai művelet részeként zajlott a támadás.

Alapvetően az informatikai támadásoknál az elkövetés helye meghatározható a támadás során továbbított adat által hagyott nyomok

---

[121] Alan Sipress, Computer System Under Attack, Washington Post (2006. október 6.), http://www.washingtonpost.com/wp-dyn/content/article/2006/10/05/AR2006100501781.html

alapján úgy, hogy az adat haladási útjánál található közvetítő szolgáltatók számítógépein – jobb esetben – megtalálható .log fájlokban[122] tárolt ip címek[123] alapján eljutunk ahhoz a számítógéphez, amelynél az elkövetési magatartás megvalósult. Ebben az esetben sem lesz azonban biztos, hogy az elkövetőt sikerül kézre keríteni, ami ismételten felveti azt a kérdést, hogy miből fogunk következtetéseket levonni az elkövető céljára, ami alapján a bűncselekményt minősíteni tudjuk.

Korábban a biztonságtechnikai szakértők egy jó része képtelenségnek tartotta a kritikus infrastruktúrákat működtető számítástechnikai rendszerek elleni támadás végrehajtását, tekintettel arra, hogy ezek a rendszerek lokális hálózatban működnek és nem kapcsolódnak az Internethez. A sikeres informatikai támadások legtöbbje ezidáig is a számítástechnikai rendszereket üzemeltető emberek sebezhetőségére alapozott[124], és itt is úgy tűnik ez a módszer segítette az elkövetőket. Tekintettel arra, hogy a lokális rendszer nem csatlakozik a világhálóhoz, ezért egyetlen módja maradt a támadás kivitelezésének, nevezetesen, ha a hálózatba más módon juttatják be a vírust, ami jelen esetben egy pendrive segítségével valósulhatott meg. Az, ugyanakkor, hogy egy vírussal fertőzött pendrive-ot miért tudtak ehhez a számítástechnikai rendszerhez csatlakoztatni, az lokális biztonságtechnológiai probléma, mint ahogy az is, hogy miért alkalmaztak MS SQL adatbázist.

A felderítés tehát eddig sem volt egyszerű, azonban a Stuxnet támadás további elemeket adott az informatikai támadások kriminalisztikáját érintő problémakörhöz azzal, hogy a bushehri atomerőmű ellen végrehajtott támadást a fent vázoltnál is kifinomultabb módszerrel hajtották végre. A vírussal történő informatikai támadások elkövetőinek felderítése nehezebb mint a közvetlenül megvalósított, fent részletezett informatikai támadások elkövetőié, tekintettel arra, hogy a vírusok terjedésének nyomon követése

---

[122] A forgalomra vonatkozó adatokat tartalmazó fájlokat log fájloknak nevezik. A forgalomra vonatkozó adat minden olyan, a számítástechnikai rendszeren átmenő és a számítástechnikai rendszer által, mint a kommunikációs lánc egyik eleme által létrehozott kommunikációra vonatkozó adat, mely jelzi a kommunikáció származási helyét, rendeltetési helyét, útvonalát, óráját, napját, terjedelmét és időtartamát vagy a szolgáltatás típusát (2001. évi CXXI. számú törvény miniszteri indokolása

[123] Az IP cím olyan azonosító adat, amellyel az Internetbe kötött számítógépek, úgynevezett gazdagépek (host) bármelyikét egyértelműen azonosítani lehet. Ez az azonosító négy számból áll, amelyeket egymástól pont választ el (például 000.000.000.000).

[124] Erről több információ a social engineering módszerének leírásához kapcsolódó szakirodalomban található.

nehezebb a meghatározhatatlan terjedési folyamatok miatt. Az, hogy a vírus terjedésének világhálón történő terjedése mellett[125], a világhálóhoz nem kapcsolódó elemek is kerültek, melyek az esetlegesen rögzített terjedési láncolatot megszakították, további kihívások elé állítja a nyomozó hatóságokat.

Mindegyik informatikai támadási típus esetén a felderítés sikerének legfontosabb eleme a hatékony nemzetközi bűnügyi együttműködés. A globális támadások elleni fellépés sikere a gyors és pontos információszolgáltatáson múlik, hiszen amíg lokálisan rendelkezésre állnak az adatok az egyes támadási állomásokon, addig, ha nemzetközi együttműködés (pl. jogsegély) keretében kell adatokat megszerezni, akkor a felderítés sikere nagyban azon múlik, hogy az adott együttműködés mennyire hatékonyan, pontosan és gyorsan képes kiszolgálni a nyomozó hatóság információigényét.

A Stuxnet vírushoz hasonló támadásoknak Magyarország is ki van téve, tehát óhatatlanul felmerül a kérdés, hogy mit tehet a jogalkalmazó, ha egy ilyen, vagy hasonló történeti tényállással találkozik. Anélkül, hogy a célzatra vonatkozóan messzemenő következtetéseket vonnánk le, jelen tanulmány keretében elegendőnek mutatkozik csupán az alapcselekmény értékelésének elemzése, hiszen már abban is ellentmondás fedezhető fel.

3. A számítástechnikai vírusokkal végrehajtott támadás megítélése a hazai jogban

A cselekmény hazai jogszabályi környezetben történő értékelésénél a Btk. 300/C. §-ának (2) bekezdésének b) pontjában foglalt bűncselekmény megállapíthatóságát célszerű megvizsgálni.[126]

Az Európa Tanács Számítástechnikai Bűnözésről Szóló Egyezményének (a továbbiakban: CCC) értelmezéséhez kiadott jelentése[127] (a továbbiakban: CCC jelentés) részletesen foglalkozik a rendszer sértetlensége elleni cselekményekkel. A CCC ötödik artikulusa szerint a szerződő felek kötelezettsége arra terjed ki, hogy megtegyék azokat a jogalkotási lépéseket,

---

[125] Lásd a korábban vázolt lineárisnak mondható támadást, amelynél informatikai nyomokat hagyhat a .log fájlokban a támadás.

[126] Btk. 300/C.§ (2) bekezdés b) pontja: aki adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését jogosulatlanul akadályozza, vétséget követ el, és két évig terjedő szabadságvesztéssel büntetendő.

[127] Convention on Cybercrime, Explanatory Report (2001. nov. 8.)

melyek alapján bűncselekménynek minősül a számítástechnikai rendszer működésének számítástechnikai adatok bevitelével, továbbításával, megkárosításával, törlésével, megrongálásával, megváltoztatásával vagy megsemmisítésével való, jogosulatlan és szándékos, jelentős akadályozása (serious hindering). Látható, hogy a hazai szabályozás azzal, hogy csupán a rendszer akadályozását emelte be a Btk.-ba, elhagyva a jelentős akadályozás kitételét, szélesebb körben állapította meg a büntetőjogi felelősséget.

A CCC jelentés 66. pontja szerint az akadályozás azokat a cselekményeket foglalja magába, ami zavarja a számítástechnikai rendszer funkcióit. Ennek a bűncselekménynek a megállapítására kerülhet sor adatok (bármilyen formában, méretben, vagy frekvencián) számítástechnikai rendszerekbe történő küldésével, ha azok a megtámadott rendszer használatára, vagy más rendszerrel történő kommunikációjára hátrányos hatást fejtenek ki. Ebben a bűncselekményi körben kell vizsgálni azoknak a programoknak az alkalmazását, melyek DOS (denial of service) támadás generálására alkalmasak. Ide tartozik továbbá a rosszindulatú kódok (pl. vírusok) bevitele a számítástechnikai rendszerbe, amelyek akadályozzák, illetőleg lényegesen lelassítják a rendszer működését, vagy olyan programok alkalmazása, amelyek nagy mennyiségű e-mail-t küldenek egy meghatározott címzettnek azért, hogy a rendszer kommunikációs funkcióit blokkolják. A CCC jelentés 70. pontja szerint ugyanakkor a támadást szándékosan kell elkövetni, ez pedig akkor valósul meg, ha az elkövető szándéka kiterjed a jelentős akadályoztatásra is.

A számítástechnikai rendszer elleni bűncselekmény elkövetési magatartásai az adat bevitele, az adat továbbítása, megváltoztatása, törlése, illetőleg egyéb művelet végzése. Melyik elkövetési magatartással valósul meg a vírusok segítségével elkövetett informatikai támadás?

A hatályos jog szerint a számítástechnikai vírussal végrehajtott informatikai támadás „adat bevitelének" minősül, azonban korábban ez az elkövetési magatartás nem szerepelt a tényállásban. A Legfelsőbb Bíróság BH1999. 145 számon közzétett döntésében még a tényállás korábban hatályban volt változatában szereplő „egyéb meg nem engedett műveletek" elkövetési magatartásával kapcsolatban vizsgálta és tartotta megállapíthatónak a számítástechnikai vírusok terjesztését. Az ügy történeti tényállása szerint a vádlott olyan vírust telepített, amely aktiválását egy későbbi időponthoz kötötte, így a leleplezésekor a rendszer akadályozása nem következett be. Az eredeti adatbevitel tehát önmagában nem akadályozta a

rendszer működését, s az adatokon a vádlott utóbb nem változtatott, nem is törölte azokat, és a hozzáférhetetlenné tétel magatartást sem valósította meg.[128]

A számítástechnikai vírussal megvalósított támadáshoz kapcsolódóan probléma a cselekmény megítélésénél az, hogy nem egyértelmű, hogy a rendszer akadályozása az adott bűncselekmény tényállás szerint megkövetelt eredménye-e vagy pedig célzata. Egyik megoldásnál sem ütközünk ellentmondásba a büntetőjogi dogmatika rendszerében. Ha immateriális bűncselekményként kezeljük a cselekményt, akkor az adat rendszert akadályozó szándékkal történő bevitelével a bűncselekmény befejezett, függetlenül attól, hogy az a rendszer működését ténylegesen akadályozta-e vagy sem, vagy csak később akadályozta volna. Ha pedig materiális bűncselekményként kezeljük a tényállást, akkor azokban az esetekben, amikor a vírus nyomán a rendszer akadályozása nem következik be az adat bevitelével történő rendszer akadályozásának befejezett kísérletéről beszélünk, melynél a bűncselekmény befejezettséghez a rendszer akadályozásának ténylegessége szükséges.

A Legfelsőbb Bíróság BH2009. 264. számon közzétett eseti döntésének indokolása szerint a Btk. 300/C (2) bekezdésének b) pontja immateriális bűncselekményt határoz meg:

„ A (2) bekezdés a) és b) pontja között a tételesen felsorolt elkövetési magatartások kisebb eltérése mellett az az alapvető különbség, hogy a b) pontban meghatározott cselekményt az elkövető a számítástechnikai rendszer működésének akadályozására irányuló szándékkal valósítja meg. Ennek megfelelően a bűncselekmény megvalósulásához az elkövető egyenes, vagy eshetőleges szándékának ki kell terjednie arra, hogy cselekményével jogosulatlanul akadályozza a számítástechnikai rendszer működését. Az akadályozás megvalósításához eredmény létrejötte nem szükséges, a bűncselekmény az elkövetési magatartás tanúsításával befejezetté válik."

Ezzel ellentétes álláspontot képvisel Berkes György[129], aki szerint a kérdéses bűncselekménynél a jogszabály meghatározza az elkövetési magatartás tényállásszerű eredményét. Ebből is adódik az a következtetése, hogy a tényállásszerű eredmény, nevezetesen az akadályozás bekövetkezésével válik a bűncselekmény befejezetté.

---

[128] Tóth Mihály: Gazdasági bűnözés és bűncselekmények. KJK–KERSZÖV, 2002, 326. oldal.

[129] Berkes György: Magyar Büntetőjog. Kommentár a gyakorlat számára. 300/C, 716/3, 33. pótlap.

Berkes álláspontjával értek egyet, különös tekintettel arra, hogy a kérdés túlmutat a vizsgált bűncselekményen, mivel a büntetőjog általános részéhez kapcsolódó kérdéseket is érint.[130]

Jelen esetben például amikor immateriális bűncselekményként értékeljük a Btk. 300/C §. (2) bekezdésének b) pontjában foglaltakat, akkor azzal kettős büntetendőség hiányában megfosztjuk Magyarországot a büntető joghatóságától azokban az esetekben, amikor egy külföldi elkövető külföldről számítástechnikai vírussal támadást intéz egy Magyarországon található rendszer ellen. Ha viszont a cselekményt materiális bűncselekményként kezeljük, akkor a Magyarországon megtámadott számítástechnikai rendszer, mint az eredmény bekövetkezésének a helye megalapozza Magyarország büntető joghatóságát a területi elv alkalmazásának segítségével.

Ugyanakkor célszerű megjegyezni, hogy a korábban említett elkövetési magatartáshoz az „egyéb meg nem engedett műveletek végzéséhez" hasonlóan a hatályos szabályozás is tartalmazza az „egyéb művelet végzése" elkövetési magatartását. A törvény miniszteri indokolása szerint egyéb műveletnek nevezhető minden olyan nem nevesített magatartás, mely a számítástechnikai rendszer működésének akadályozását eredményezi. Ez is inkább a bűncselekmény eredmény-bűncselekményként történő alkalmazása felé billenti nálam a mérleg nyelvét, tekintettel arra, hogy a „rendszer akadályozásának szándékával megvalósított egyéb művelet végzése" meglehetősen határozatlan tényállási elemnek minősíthető ahhoz, hogy anyagi legalitáshoz kapcsolódó kérdéseket vessen fel.

Röviden visszatérve a jelentős rendszerakadályozás problémájához fontosnak tartom megemlíteni az információs rendszerek elleni támadásokról szóló, 2005. február 24-i 2005/222/IB tanácsi kerethatározatot.[131] A kerethatározat 3. cikke értelmében minden tagállam meghozza a szükséges intézkedéseket annak érdekében, hogy valamely információs rendszer működésének számítógépes adatok bevitele, továbbítása, megrongálása, törlése, minőségi

---

[130] Szintén az előbb említett döntés szerint „a számítástechnikai rendszer működésének akadályozása magában foglalja például azt az esetet is, ha a rendszerbe valótlan adatok kerülnek be, és további működése ezeken a valótlan adatokon alapul, ekként a rendszerben lévő adatok megbízhatóságához, hitelességéhez és titokban maradásához fűződő érdek sérül."
Álláspontom szerint ha önmagában csupán az adatok megbízhatóságához fűződő érdek sérül, akkor az a) pont szerinti eset valósul meg, míg a b) pont szerinti eset megvalósulásához szükséges, hogy a számítástechnikai rendszer – ami elkülönül a számítástechnikai adattól – működéséhez fűződő érdek is sérelmet szenvedjen.

[131] 2005/222/IB, HL 2005 L 69, 2005. február 24., 67.

rontása, megváltoztatása, elrejtése vagy hozzáférhetetlenné tétele révén történő szándékos és súlyos akadályozása vagy megszakítása, amennyiben azt jogosulatlanul követték el, legalább a jelentősebb esetekben bűncselekménynek minősüljön. Tekintettel arra, hogy az Európai Közösség Bírósága a Pupino ügyben[132] kimondta, hogy a tagállamok igazságügyi hatóságai kötelesek a nemzeti jogot az uniós normák szellemében, azaz a kerethatározatoknak (is) megfelelően értelmezni, ezért a súlyos rendszerakadályozás kérdését akkor sem lehet figyelmen kívül hagyni, ha azt a hatályos Btk. nem tartalmazza.

Mi lehet a Btk. helyes értelmezése, mikor állapítható meg a számítástechnikai rendszer jelentős/súlyos akadályozása? A külföldi jogirodalomban uralkodó álláspont szerint a rendszer akadályoztatása csak abban az esetben állapítható meg, amennyiben a rendszerakadályozás jelentős az adott rendszer működésének következményeihez viszonyítva.

„A cselekmény elkövetési tárgya a számítástechnikai rendszer, mely működésének akadályozása azt jelenti, hogy a rendszer nem működik hibátlanul, használhatatlanná válik. Az adatfeldolgozó berendezés és az adathordozó akkor válik használhatatlanná, ha használhatósága jelentősen korlátozódik, azaz a számítástechnikai rendszer funkcióját úgy befolyásolja, hogy az a célját nem tudja a továbbiakban teljesíteni.[133]"

Más álláspont szerint a számítástechnikai rendszer működése az adatfeldolgozást is jelenti, ami magába foglalja adatok számítástechnikai rendszer segítségével történő mentését, feldolgozását, de ugyanúgy jelenti az adatok dokumentálását és előkészítését is. Ezért a számítástechnikai rendszer fogalma nemcsak az adatfeldolgozási folyamatot tartalmazza, hanem a hozzá kapcsolódó további adatokkal való eljárást és azok felhasználását is.[134]Ezt az értelmezést azonban sokan kritizálják, mivel túlságosan tágan vonja meg a tényállás alkalmazási körét.[135] A német büntető dogmatikában ezért korlátozták a számítástechnikai rendszerekre vonatkozóan a törvény

---

[132] C-105/03

[133] Hilgendorf, Eric: Grundfälle zum Computerstrafrecht. In: JuS 1996, 1082–1084. oldal, 1084. oldal.

[134] Lencker, Theodor – Winkelbauer, Wolfgang: Computerkriminalität – Möglichkeiten und Grenzen des 2. WiKG (I),(II), (III). In: CR 1986, 824–831. oldal, 830. oldal.

[135] Leipzinger Kommentar, Strafgesetzbuch, Großkommentar. Hrsg. von Burkhard Jähnke, Heinrich-Wilhelm Laufhütte und Walter Odersky, 11. kiadás, Berlin, 1992 ff. TOLKSDORF: 303b. § Rn. 3. f.

alkalmazását. A rendszer működésének akadályozása csak olyan berendezések adatfeldolgozásának akadályozása esetén merül fel, mely egy vállalkozás vagy hivatal vonatkozásában jelentős, ami akkor fordulhat elő, ha az érintett intézmény az adatfeldolgozás kiesése esetén a feladatait a továbbiakban nem, vagy csak jelentős többletráfordítással tudja ellátni. Az, hogy egy adatfeldolgozás jelentős-e, csak az elkövetési magatartás által közvetlenül érintett vállalkozás vagy hivatal működése alapján határozható meg. A támadás közvetett kihatását nem lehet figyelembe venni az akadályoztatáshoz kapcsolódóan, mert az polgári kárigények kielégítését vonná a büntetőjogi tényállás alá. Fontos továbbá, hogy az elkövetési magatartásnak okozati összefüggésben kell állnia az adatfeldolgozás zavarásával. Az adatfeldolgozás veszélyeztetése nem elegendő a tényállás megállapításához. Az adatfeldolgozás, azaz a számítástechnikai rendszer működésének akadályozása, akkor áll tehát fenn, ha az akadályozás jelentős, az csak nagy idő- és költségráfordítással hárítható el.[136]

4. Zárszó

Az iráni atomerőmű ellen végrehajtott cselekmény minősítéséhez a fentiek alapján tehát célszerű lenne ismernünk azt, hogy a vírusfertőzés a rendszer jelentős/súlyos akadályozását valósította-e meg. Ha ez a körülmény nem állapítható meg, akkor nem beszélhetünk informatikai bűncselekményről. Ellenkező esetben pedig ahhoz, hogy az informatikai bűncselekményt, mint a terrorcselekmény eszközcselekménye értékelhessük, szükséges annak tisztázása is, hogy az informatikai bűncselekmény elkövetője a szándékos bűncselekményt milyen célból valósította meg. Ezt követően pedig szükséges még azt is tisztázni, hogy adott esetben az informatikai támadás katonai akció keretében került végrehajtásra vagy sem. Ezeknek az információknak a hiányában pontos válaszokat nem lehet adni arra a kérdésre, hogy mi történt valójában Iránban.

Az informatika szerepe a bűnözők körében egyre nagyobb szerepre tesz szert, ezért a jogalkalmazóknak is figyelembe kell venniük ezt a tendenciát. Az informatika mint természettudomány a legtöbb esetben megfelelő válaszokat ad az egyes, informatikai környezetben megvalósított bűncselekmények tényállási elemeihez kapcsolódó tények jellemzőire,

---

[136] Hilgendorf, Eric: Grundfälle zum Computerstrafrecht. In: JuS 1996, 1082–1084. oldal, 1084. oldal.

biztosítva ezáltal a kétséget kizáró bizonyítást. Ehhez kapcsolódóan azonban szükséges az, hogy az informatikai folyamatok működési modelljeit legalább alapszinten ismerje a jogalkalmazó, hogy az egyes speciális kérdésekhez kapcsolódó szakértői válaszokban foglalt leírásokból a megfelelő következtetéseket tudjon levonni. Ennek a leghatásosabb módja az informatika és a büntetőjog kapcsolatának tanulmányozása, illetőleg a jogász- és rendőrképzésben az ilyen irányú ismeretek oktatása.

Az informatika és a terrorizmus sajátos kapcsolatán túl gyakran hangoztatott problémaként jelenik meg az, hogy a közbiztonságra hivatkozással az alapvető szabadságjogainkat korlátozó szabályozás zajlik. Az esetleges jogkorlátozás indokoltságát a terrorcselekményhez kapcsolódóan nehéz kétségbe vonni, még akkor is, ha ténylegesen nem valósult meg ilyen jellegű cselekmény közvetlenül Magyarországot érintően. Nagyban megkönnyítené azonban a terrorcselekményekhez kapcsolódó jogkorlátozások társadalmi elfogadottságát az, ha a jogkorlátozásokhoz kapcsolódó vita nem csupán valamely cselekmény büntetendővé nyilvánítása körében zajlana le, hanem a konkrét büntetőeljárás megindulása előtt, a felderítés, és bűnmegelőzés szakaszához kapcsolódó jogalkotásban és jogalkalmazásban is érvényesülnének a jogállami kritériumok, és a jogállami jogalkalmazás a nyomozó hatóságok általánosan elfogadott, köztudomású jellemzője és minőségük mércéje is lenne. Ennek érdekében fontos lenne a jogalkalmazás informatikával érintett területein compliance eljárások alkalmazása, amely eredménye elősegítené a jogalkotók munkáját, felhívhatná a figyelmet a jogalkalmazásban lévő belső ellentmondásokra is, egységesítve ezáltal a jogalkalmazást.