

KIBERTERRORIZMUS

„Condor”

Tartalom

I. FEJEZET: Bevezetés	3-4
1.1 Témaválasztás	5
II. FEJEZET: Az Internet születése	7
III. FEJEZET: „Itt gépkalózok élnek!”	8
3.1. A számítógépes környezetben elkövethető bűncselekmények jellemzői	9
3.1.1. A bűncselekmények köre	9-10
3.1.2. A jogsértések tömegessége	10
3.1.3. A tömegességből adódó jelentős kárérték	10
3.1.4. A látencia	11
3.2. A számítógépes környezetben elkövetett bűncselekmények céljairól, okairól	12
IV. FEJEZET: A számítógépes bűnözés	13-15
V. FEJEZET: Kiberterrorizmus	16
5.1. Terrorizmus, mint jelenség	17-19
5.1.1. Kapcsolata a szervezett bűnözéssel	19-20
5.2. A kiberterrorizmus	20-23
5.3. A terrorizmus elleni harc	23-24
5.4. A kiberterrorizmus eszköztára	25-27
5.4.1. Phishing	27-28
5.4.2. Vishing	28-29
5.4.3. Keylogging	29-30
5.4.4. Hacking	31
5.4.4.1. Alapvetés	31-33
5.4.4.2. A „szakma” nagyjai	33-34
5.4.4.3. A hatályos hazai szabályozás	34-45
VI. FEJEZET: Összegzés/következtetés/védekezés	46-48
Irodalomjegyzék	49

I. FEJEZET: Bevezetés

Bűnözés, terrorizmus, számítógépek. A három közti kapcsolat napról-napra szorosabb. Jelenségek, melyek életünk és mindennapjaink velejárói. Az utóbbi időkben a számítógépes bűnelkövetés és terrorizmust ölt ijesztő méreteket, főként utóbbi jelent nagyobb veszedelemet, mivel ha célt ér a támadás, olyan hatást lehet vele kiváltani, melynek következményei beláthatatlanok. Nem is beszélve a pusztulásról, amit életben, lélekben, vagyonban tehet. És bár hazánk nem tartozik a kiemelten veszélyeztetett országok közé, a probléma igenis valós és nem vehetjük fél vállról ezeket a jelenségeket.

Joggal tehetjük fel a kérdést: hol vagyunk biztonságban, ha már otthon a számítógépünk előtt sem.

Megállapítható, hogy úgy általában a bűnözés mértéke az elmúlt években folyamatosan emelkedik. Sajnos ugyanez mondható el az erőszakosságról is. (Témámra nem jellemző ez utóbbi.)

Kiemelendő, hogy a *bűnelkövetések legdinamikusabban fejlődő területe a számítógéppel, és/vagy Internet útján megvalósított deliktumok*. Szinte valamennyi területi szerv jelezte, hogy jelentős mértékben megszaporodtak az ily módon elkövetett cselekmények. Jelentősen megnőtt az elmúlt években az Interneten keresztül megvalósuló zaklatások, becsületsértések száma is. Továbbra is „klasszikusnak” számítanak az ismerősöket, barátokat nyilvántartó közösségi portálokon a személyes adatokkal való visszaélések. Tovább nőtt a száma a készpénz-helyettesítő fizetési eszközökkel történő visszaéléseknek, illetve az „internetes vásárok” (*Teszvesz, Vatera*) során elkövetett csalásoknak.¹

Gyakran vitatott kérdés a számítógépek védelmével kapcsolatban, hogy vajon a kiberbanditizmus valóban újfajta bűncselekményeket vezetett-e be, vagy a csak hagyományos módszerek gigabájtokba és modemekbe csomagolásáról van szó. Mindkét vélemény helytálló. Az identitáslopás például a legősibb csalási módszerek egyike. Az Interneten, számítógéppel elkövetett lopás vagy csalás végül is ugyanaz marad, a cselekmények technikai hátterétől függetlenül.

Azonban életre keltek olyan bűnözési formák is, amelyek hamisítatlanul a XXI. század szülöttei. Itt vannak például a számítógépes vírusok. Sokan a falfirkáláshoz

¹ <http://www.police.hu/megelozes/bunmegelozes/aldozatvedelem/aldvedelem2010.html> [2011. 11. 21.]

használták a vírusírást, vagyis általában egy fiatal, figyelemre vágó ember által elkövetett vandalizmus.

Egy-két évtizeddel ezelőtt a számítógépes bűnözés még közel sem jelentett akkora veszélyt, mint manapság, de mára kimondhatjuk: társadalmi problémává nőtte ki magát. Az információs társadalom felé vezető úton pedig fokozottan igaz ezen állítás. Az információs forradalom negatív eredményeként a társadalmak egyre kiszolgáltatottabbak lettek az adatfeldolgozó rendszereknek. Napjainkban biztonságunk (gondoljunk a személyes adatokat tároló adatbázisokra), és értékeink (például: banki adatbázisok, melyek feltörésével könnyen hozzájuthatnak illetéktelenek vagyonunkhoz) egyre jobban függnék e rendszerek működésének zavartalanságától, s a számítógépes bűncselekmények – többek közt – pont e rendszerek működését támadják.

A jelenség ellen, mind technikai – például: egyre modernebb védelmi szoftverek, technikai berendezések által -, mind jogi eszközökkel fel kell lépni. Hangsúlyozandó, hogy a jogi fellépés nem lehet kizárólag büntetőjogi, mivel a büntetőjog e problémára legfeljebb átmeneti megoldást adhat – persze ez nem azt jelenti, hogy nélkülözni kellene ezen eszközt.²

² <http://www.jogiforum.hu/publikaciok/307#axzz17CoEDxm2> [2011. 06. 10]

1.1. Témaválasztás

Témaválasztásom egyszerűsége aktualitásában rejlik.

A modern világ számtalan egyéb kihívása mellett, az informatika ugrásszerű fejlődésével a bűncselekmények egy egészen új, sajátos fajtája jelent meg: az informatikai bűncselekmények, más szóval: a számítógépes környezetben elkövetett bűncselekmények.

Néhány évtizedes megjelenésük óta ijesztően szaporodnak és minden nap újabb veszélyt jelentenek a XXI. század komputerizált társadalmára, melyben lassan az élet minden aspektusát a számítógépek (és az Internet) határozzák meg.

Minden egyes számítógép aktív Internet-kapcsolattal potenciális áldozat és amilyen könnyű célpont egy otthoni PC egy képzett „szakember” számára, úgy bármely központi adatbázis vagy magasabb szintű „*digitális erőd*” is megtámadható, ahogy arra lentebb többször is hivatkozni fogok.

Ami azonban talán még ijesztőbb jelenség, az a bűncselekmények (nem egyszer a terrorcselekmények) számítógéppel történő megtervezése, összehangolása, szisztematikus véghezvitele. Be kell látnunk, hogy a bűnelkövetők és terroristák legújabb „játszótere” a digitális világ lett.

Mint azt láthattuk, az ilyen jellegű bűncselekmények gomba módra szaporodnak és terjedésüknek nem lehet gátat vetni, mert a fejlett társadalmak saját maguk alkotta ördögi körbe kerültek, a folyamatos fejlődésnek (egyfelől csodálatos dolog), legalább annyi hátránya van (ha nem több), mint előnye. A jelenlegi negatív állapot visszavezethető egyrészt a túl liberális szabályozásra, másrészt az emberi találmányosságra (legyen szó weboldal hamisításról, elektronikus betörésről, adatlopásról és mindezek formáiról).

Egyszóval: a probléma égető és napról napra forróbb.

Kitekintésem fókusza a **kiberterrorizmus**, annak eredete, módszerei, és eszköztára. De szót ejtek a számítógépes bűnelkövetés egyéb módjairól is, valamint a XX. század csodájáról: az *Internetről*.

II. FEJEZET: Az Internet születése

Hogy mikor jött létre az **"Internet"**, pontosan nem lehet tudni, mindenesetre hosszú evolúciós folyamat során jutottunk el oda, amit ma a számítógépes hálózatokat világméretben összekötő rendszernek nevezünk. Bár 2011-ben csaknem mindenki használja már, s szájbarágósnak tűnhetnek a következő sorok, ahhoz, hogy megértsük azt a negatív hozadékat, melyet az informatikai bűncselekményeknek (és kiberterrorizmusnak) nevezünk, tudnunk kell, mi is az Internet, mint a modernkor nélkülözhetetlen eleme.

Az Internet - ha röviden próbálnánk definiálni, - *nem más, mint egy heterogén rendszer, mely a számítógépeket közvetlenül, vagy közvetetten köti össze egymással.* Az Internet azonban nem csak egy világméretű hálózat („a hálózatok hálózata”³), hanem az azt használó emberek közösségének egy merőben új és minden eddiginél népesebb társadalma. Az Internet gyorsabban terjed, mint bármely más médium eddig. Világunkban a rádiónak 38 évre, a televíziónak 13 évre, a kábel TV-nek 10 évre, az Internetnek mindössze 4 év kellett háromszázmillió fogyasztó eléréséhez.⁴

Az Internet eredete az 1960-as évekre vezethető vissza és igazi amerikai sikertörténetnek számít, pedig a globális hálózat megalkotásában európai szakembereknek is komoly szerepe volt.⁵ Az akkori formája még primitív, hétköznapi ember számára használhatatlan módon volt elérhető, éppen ezért nem is lehet összehasonlítani a mai, más szabályok szerint működő rendszerrel. **Csupán az USA-ban volt elérhető, s ott is csak a kormányzati szervek, főként a hadsereg alkalmazta – kicsit sem meglepő módon.** Később az Internet kijutott az akadémiai és vállalati küzdőterre. **Az igazi áttörés a személyi számítógép megjelenésével vette kezdetét, mikor a böngészőfelületek felhasználóbaráttá és anyagilag elérhetővé váltak.**

A hidegháború egyik következménye, hogy az egymással szembenálló és egymástól kölcsönösen rettegő két szuperhatalom (az Amerikai Egyesült Államok és a Szovjetunió), élénk tudományos, technika és technológiai versenybe kezdett.

³ Nagy Zoltán András: *Bűncselekmények számítógépes környezetben*, Budapest, Ad Librum, 2009, 10. o.

⁴ Nagy, 2009, 6. o.

⁵ http://www.sg.hu/cikkek/69740/europa_es_az_internet_szuletese [2011. 07.13]

Az amerikai *Advanced Research Projects Agency Network*⁶ története **1957-ben** kezdődött, az első Szputnyik fellövésével, miután kitört a „szputnyik-sokk”. A Szputnyik komoly veszélyt jelentett, így fel kellett venni a harcot az oroszokkal. A cél az volt, hogy egy lehetséges rakétatámadást megelőzzenek. **Számítógép már 1945 óta létezett, Neumann Jánosnak köszönhetően.** A feladat már csak az volt, hogy hálózatba kössék ezeket az olykor szoba méretű "szörnyeket", hogy aztán együtt dolgozzanak. Abban az időben az Arpanet még nagyon kicsi volt, alig két tucat számítógépet kötött csak össze.⁷

Az első e-mail⁸ program megszületése már 1972-ben bekövetkezett, majd két évvel később az "Internet", mint szó is megszületett. **Ekkor jelent meg az első vírus, az Elk Cloner, 1982-ben, mely nem is volt igazán vírus. Számítógépes berkekben Brian, az 1987-ben megjelent vírus az első kártékony program.** Hiszen a Microsoft operációs rendszerén futott, s emiatt több kárt okozott, mint elődje. Igaz, „Brian” még nem az Internet hullámaait lovagolta meg, hanem a számítógépes adathordozók felületét. Hamarosan már megjelent a vírusokkal szembeni ellenállás is. Számtalan cég jött létre fiatal és feltörekvő számítógép-mágusokkal, akik egymaguk, vagy támogatással nagy üzletet láttak a vírusirtók piacában. S ahogy terjedtek a vírusok, s az ellenük, a számítógépet oltalmazó Antivírus-programok, egyre több háztartás kapcsolódott a világhálóhoz, s egyre több ember került bele a digitális társadalomnak nevezett rendszerbe, s vált egyúttal azzá a közeggé, amelyben az informatikai bűnelkövetők könnyedén megbújhatnak.

A '90-es években robbant ki az Internetes forradalom. 1991-ben jelent meg a WWW, vagyis world wide web, mely leegyszerűsítette az Internetes címeket, s mellyel könnyebbé vált a fogyasztóbarát rendszer kialakítása. 1992-ben az USA kormánya engedélyezte az Internet kereskedelmi célú felhasználását.

Az Internet napjainkra olyan tényező, mely meghatározza az emberek mindennapjait, a kommunikációt és mely olyan információkat tartalmaz rólunk, vagy környezetünkről, melyet bárki megszerezhet, ha a megfelelő eszközök és tudás birtokába jut. Az ilyen adatokkal többféleképpen visszaélhet bárki.

⁶ ARPANET - *Modern Kutatási Projektek Hivatala*; az ARPA-t arra tervezték, hogy akár egy atomtámadást is túléljen

⁷ http://www.sg.hu/cikkek/42842/35_eves_az_e_mail [2011. 08. 11]

⁸ http://www.sg.hu/cikkek/42842/35_eves_az_e_mail [2011. 08. 11]

III. FEJEZET: „Itt gépkalózkodnak!”

Amikor régen a térképészek
lerajzolták az általuk ismert világot,
a szélére mindig odaírták:

Itt sárkányok élnek!

(Ismeretlen szerző)

Napjaink „behálózott” világára is igaz a fenti idézet. Amikor az otthoni gépet vagy a vállalati hálózatot csatlakoztatjuk az Internethez, akkor a saját hálózatunkon kívüli vadon a szó szoros értelmében a világ vége, egyben a világháló kezdete, ahol a gépkalózkodók (cracker⁹) leselkednek, hogy kihasználják az óvatlanokat.¹⁰

3.1. A számítógépes környezetben elkövethető bűncselekmények jellemzői

A számítógépes környezetben elkövetett deliktumok intellektuális cselekmények.

A számítógép, és a hozzá kapcsolódó technikai eszközök kezelése komoly felkészültséget, fantáziát, nem csekély logikai készséget követel. A számítógépes bűncselekmények a fehérgalléros bűnözés (*white-collar crime*) része, bár azt nem fedi le teljesen. Az ilyen bűncselekmények felderítését az a szociológiai körülmény is nehezíti, hogy az elkövetők általában büntetlen előéletűek, a hatóságok „a priori” bizalommal viseltetnek e személyekkel szemben.¹¹ **Balogh Zsolt György** leszögezi: „*mind a számítógépes, mind a fehérgalléros bűnözés olyan önálló kriminológiai kategória, melyek között van ugyan némi átfedés, de arról még sincs szó, hogy bármelyik kategória*

⁹ A komoly szakértelemmel bíró, rosszindulatú támadókat jelölik ezzel a kifejezéssel.

¹⁰ Thomas, Tom: *Hálózati biztonság*, Ford.: Ketler Iván, Budapest, Panem Könyvkiadó, 2005, 17-18.o.

¹¹ Nagy, 2009, 19-20. o.

egészében tartalmazná a másikat.”¹² Az előbbi megállapítással aligha lehet vitába szállni.

A szakma java része is egyetért ebben.

3.1.1. A bűncselekmények köre

Az ilyen módon elkövetett bűncselekmények körének meghatározásánál máris komoly problémával szembesülünk. **Napjainkra e kör behatárolása rendkívül nehéz,** - ami a bűnügyi tudományokban igen szokatlan – **sőt, mondhatni meghatározhatatlan.**

Az első számítógépes bűncselekmények egyike az egyesült államokbeli Walston & Co. alelnöke által elkövetett sikkasztás volt, aki hamis lyukkártyákat készítve 50.000.- dollárt sikkasztott el még 1959-ben.¹³

Az **ET 9 (89) számú** ajánlása a „Számítógépes-környezetben elkövetett bűncselekményekről” az e körbe vonható bűncselekményekről tartalmazott egy minimális¹⁴ és egy fakultatív¹⁵ listát.¹⁶

A **2001** novemberében Budapesten aláírt „**Számítástechnikai bűnözésről szóló egyezményben**” („**Convention on Cybercrime**”) már egy másfajta felosztást találunk.¹⁷ Az egyezmény következménye, hogy felerősödött a vita a biztonság és az emberi jogok közötti egyensúly kérdésében. Főként a civil szervezetek emeltek hangot

¹² Balogh Zsolt György: *Jogi informatika. Budapest-Pécs, 1998, 266.1.*

¹³ Nagy, 2009, 21. o.

¹⁴ A számítógépes csalás, a számítógépes hamisítás, a számítógépes adatokban és programokban történő károkozás, a számítógépes szabotázs, a jogellenes behatolás: a számítógépes rendszerbe vagy hálózatba történő jogosulatlan bejutás a biztonsági intézkedések megsértése révén, a jogellenes titokszerzés, védett számítógépes programok jogellenes másolása, a félvezető topográfiák jogellenes másolása.

¹⁵ A számítógépes adatok és/vagy programok megváltoztatása, a számítógépes kémkedés, a számítógép jogellenes használata, védett programok jogellenes használata.

¹⁶ August Bequai: *Computer-Related-Crime, ECC, Strasbourg, 1990, 36-69. o.*

¹⁷ **I. cím:** A számítástechnikai rendszer és a számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények

2. cikk: A jogtalan belépés

3. cikk: A jogtalan kifürkészés

4. cikk: Az adatok sérthetetlensége elleni cselekmény

5. cikk: A rendszer sérthetetlensége ellen cselekmény

6. cikk: Visszaélés eszközökkel

II. cím: A számítástechnikai bűncselekmények

7. cikk: A számítástechnikai hamisítás

8. cikk: A számítástechnikai csalás

III. cím: A számítástechnikai adatok tartalmával kapcsolatos bűncselekmények

9. cikk: A gyermekpornográfia

10. Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények

amellett, hogy az egyezmény túl nagy felhatalmazást ad az állami szerveknek (beleértve a jogot a hackerek számítógépének ellenőrzését, a kommunikáció felügyeletét stb.). Az Európa Tanács is csatlakozott az egyezményhez, mint az emberi jogok legaktívabb támogatója.¹⁸

A fentiekből látható, hogy a számítógépes környezetben elkövethető bűncselekmények köre fokozatosan bővül, ahogy a számítástechnika fejlődik, miként a lehetőségek megsokszorozódnak, és ahogy a számítógép nélkül egyre inkább elképzelhetetlen életünk.

3.1.2. A jogsértések tömegessége

Az eszközök elérhetőségével, a különféle hálózatok (leginkább az Internet) folytán a jogsértések is tömegessé váltak. A tömegességet megjelenítik a szerzői jogi jogsértések, a különféle pusztító programok¹⁹ megbecsülhetetlenül nagy száma, mely utóbbiak a hálózatokon lesik áldozataikat.²⁰

3.1.3. A tömegességből adódó jelentős kárérték

A számítógépes környezetben elkövetett különféle jogsértések tömegességéből, valamint az elektronikus adatfeldolgozó- és átviteli hálózatok funkciójából következően a kárérték általában jelentősebb, mint a hagyományos bűncselekményeknél.

A nyolcvanas évek elejéről származó FBI jelentés kiemeli, hogy míg a fegyveres bankrablással az elkövetők átlag 10.000.- US dollárt zsákmányolnak, addig a komputeres elkövetés révén átlag 1.000.000.- dollárt.²¹

¹⁸ Kurbalija, Jovan: *An introduction to Internet governance*, Budapest, Akaprint Nyomdaipari Kft., 2010, 97. o

¹⁹ Egyes források szerint napjainkban az ismert vírusok száma meghaladja a százazretet.

²⁰ Nagy, 2009, 25. o.

²¹ Nagy, 2009, 27. o.

3.1.4. A látencia

A fenti tényező fokozottan igaz ezen bűncselekményekre. Az ismertté vált esetek száma minden bizonnyal csupán töredéke lehet a tényleges számoknak. Nem véletlenül nevezi a kriminológia ezeket a bűncselekményeket az összбүнözés „sötét mezőjének”²².

Tovább növeli a látenciát, hogy pl. a pénzintézetek – mint az egyik leggyakoribb célpontok - többnyire ellenérdekeltek a nyomozó hatóságok törekvéseinek.²³ Ezen kívül a nyomozó hatóság nem mindig rendelkezik megfelelő ismeretekkel, tudással bíró szakemberekkel.²⁴ Ezekre a hiányosságokra a kriminálpolitikának - amelynek a бүнözés elleni küzdelem feltételrendszerét kell kialakítania - reagálnia kell.

A бűncselekmény elkövetője és a бűncselekmény megvalósulásának helyszíne térben, sőt, időben is különválhat, és ez a бűncselekmény bizonyításához szükséges bizonyítékok összegyűjtését nehezíti vagy teszi egyenesen lehetetlenné.

A бűncselekmények felderítése, bizonyítása nem egyszerű feladat. Az áldozat sok esetben nem is - vagy csak későn - szerez tudomást arról, hogy бűncselekményt követtek el a sérelmére.

Az elkövető általában leplezni kívánja magát, és bizonyos szaktudás birtokában az elektronikus adatfeldolgozó és átviteli rendszerekből nyom nélkül távozhat cselekménye elkövetése után.²⁵

²² Nagy, 2009, 30-31. o.

²³ Érthető bizalmatlanságot válthat ki az ügyfelekben, ha kitudódik, hogy valamely pénzintézet számítástechnikai rendszere sebezhető.

²⁴ Kurbalija, Jovan: *An introduction to Internet governance*, Budapest, Akaprint Nyomdaipari Kft., 2010, 98. o.

²⁵ <http://www.matud.iif.hu/01aug/nagy.html> [2011. 10. 11]

3.2. A számítógépes környezetben elkövetett bűncselekmények céljairól, okairól

Röviden megjegyezhető, hogy az e körbe vonható virtuális bűncselekmények elkövetésének motívumai, céljai semmiben sem térnek el a valóságos térben elkövetett bűncselekmények motívumaitól, céljaitól.

A jogtalan vagyoni haszonszerzéstől (pl. csalás jellegű cselekmények), az adatok, titkok jogtalan kifürkészésén át, (kémkedés, titoksértés) a károkozásig terjed (számítógépes hálózatok megbénítása).²⁶ A kör igen változatos.

Sokan nem veszik figyelembe az örökérvényű állítást: *„Mindig van nálunk okosabb, többet tudó, vagy jobban felszerelt támadó”. A katasztrófa bekövetkezésének csaknem biztos módja, ha magunkat hisszük a legokosabbnak.*

²⁶ Nagy, 2009, 34. o.

IV. FEJEZET: A számítógépes bűnözés

„Az eredetinek kinéző hamisítvány a legjobb üzlet.”

Mint ahogy arra már történt utalás, a *számítástechnika néhány évtizedes múltja máris kapcsolatba került a bűnözéssel*. Nincsen ebben semmi meglepő, hiszen bármilyen új területe is jelenik meg a társadalmi viszonyoknak, ott megjelenik a bűnözés is. Gondoljunk csak a XX. század elejére, amikor kezdtek elterjedni az autók. A bűnözők azonnal kocsiba pattantak, hogy egérutat nyerjenek a hatóságokkal szemben.²⁷ Ugyanígy történt ez a számítógépek térhódításával is. Élénken érdeklődni kezdtek a bűnözők az informatika iránt. Mindennapossá váltak a személyes adatokkal való visszaélések, bank-, hitel- és SIM-kártya csalások, adatlopások (PIN kódok, személyes adatok) stb. Ma már nem egy bankrablás vagy terrorakció tervét is számítógéppel készítik.

Ha meg akarjuk határozni a kiberbűnözést, akkor két megközelítésből indulhatunk ki. Ha azokat a cselekményeket vesszük, amelyek a számítástechnikai rendszerek ellen irányulnak, akkor a kiberbűnözést a jogosulatlan hozzáférés; a számítástechnikai adatok és programok törlése, hozzáférhetetlenné tétele, megváltoztatása; a számítástechnikai rendszerek és hálózatok helyes működésének akadályozása; számítástechnikai rendszereken és hálózatokon futó adatok és programok jogosulatlan kifürkészése, valamint a számítógépes kémkedés fedi le.

A másik lehetőség szerint: minden olyan bűncselekmény, amelynek elkövetése az Internet útján történik,²⁸ és ez esetben egy jóval szélesebb kört fog át a kiberbűnözés, azokat is, amelyek kifejezésre jutottak a 2001-es „Számítástechnikai bűnözésről szóló egyezményben”, úgy mint: a számítógépes csalás, szerzői jogi jogsértések, gyermek pornográfia és hálózatbiztonság.²⁹

A gyakorlatilag behatárolhatatlan cselekményi kör annak a negatív következménye, hogy napjainkra **tömegessé váltak a modernkori vívmányok**, ezeket mindenki használja, sőt, sok helyen egyáltalán nem is lehet nélkülük mozdulni. A

²⁷ Moore, Robert: *Cybercrime – Investigating High-Technology Computer Crime*, Anderson Publishing, Oxford, 2011, 1-2. o.

²⁸ Moore, 2011, 83-84. o.

²⁹ Kurbalija, Jovan: *An introduction to Internet governance*, Budapest, Akaprint Nyomdaipari Kft., 2010, 97. o

megszaporodott elkövetések szorosan összefüggnek az emberiség által generált elképesztő adatmennyiséggel, melyet talán jól szemléltet az, hogy innen a Holdig nem lenne elég hely a sorba rakott CD-knek az összes adat tárolására³⁰ – egy ilyen közegben „érezheti magát elemében” egy képzett elkövető (és bizonytalanságban bármelyikünk).

Mindezen cselekmények megvalósításához számítástechnikai eszközök szükségesek,³¹ valamint egy jó szakember, aki járatos ebben. Mindeközben tapasztalatait bővíti, s egyúttal bűncselekményt valósít meg. *És ezek döntő többségére vagy csak későn – amikor már nincs is mit tenni - vagy egyáltalán nem derül fény, más szóval a látencia roppant magas* – ahogy arra már hivatkoztam. És ebben rejlik talán az igazi veszélye az ilyen típusú bűncselekményeknek, sokszor akkor éri támadás a sértetteket, mikor arra nem számít és onnan, ahonnan semmiképp sem várná. ***Kétségkívül az emberek ilyen téren való tapasztalatlanságát – az elhárítást érte - és a látott weboldal iránti bizalmat használják ki.***

Az ilyen bűncselekmények gomba módra szaporodnak. A világ országai az elmúlt negyed évszázadban egyre inkább rádöbbenek arra, hogy ez a kriminális vonal folyamatosan erősödik és valós veszélyt jelent mindenkire nézve. A jogalkotói lemaradásnak komoly ára volt, mégpedig az, hogy napjainkra már kizárt egy hatékony, megfelelő és időtálló szabályozás. Utóbbi azonban főleg annak tudható be, hogy az informatika rémisztően gyorsan fejlődik. Nem túlzás azt kijelenteni, hogy napi szinten jelennek meg újabbnál-újabb fejlesztések. Aligha kérhető számon bárkin, hogy nem tud lépést tartani a rohamosan fejlődő informatikai- vagy kibertársadalommal a nehézkes normatív szabályozás. Pozitívumként említhető, hogy számos államban már egy egészen másfajta szemlélet van kialakulóban. Egy olyan felkészülés, amely már a kibertársadalom tagjait hívja segítségül a probléma megoldására.

2012 év végén jelentette be a brit hadsereg, hogy toborzásba kezd a kiberháborúhoz. Olyan fiatal kémeket akar képezni, akik az Xbox generáció tagjai, akik nem rendelkeznek egyetemi végzettséggel, de otthonosan mozognak a közösségi média és videojátékok világában. A gyakornoki képzésről William Hauge, brit külügyminiszter nyilatkozott, beszédét a dél-angliai Bletchley Park-ban tartotta, ugyanott, ahol a második világháborúban az angolok feltörték a németek kódoló berendezését, az Enigmát. A jelöltek kétéves tanfolyamon sajátíthatnák el a kommunikációs, biztonságtechnikai és mérnöki ismereteket. Hauge szerint a kiberbűnözés és az azzal járó fenyegetés egyre növekvő kockázatot jelent,

³⁰ <http://nonstopuzlet.hu/mennyi-adatot-general-az-emberiseg-20110214.html> [2011.10.10]

³¹ A számítógép egyszerre lehet a bűncselekmény tárgya és eszköze. *Lásd: Nagy, 2009, 37. o.*

így fokozni szeretnék az erőfeszítéseket. Ezekkel a tehetségekkel töltenék fel az Egyesült Királyság kódfejtő állományát. A miniszter úgy véli, ez azért is fontos, mert a fiatal, innovatív generáció megvédheti az országot a fenyegetéstől, amelyek közül néhány van olyan súlyos, mint a németeké a második világháborúban.³²

³² http://index.hu/tech/2012/10/19/kiberhaboruhoz_toboroz_a_brit_hadsereg/ [2012. 11. 23]

V. FEJEZET: Kiberterrorizmus

A fentebb tárgyalt számítógépes bűncselekmények ezen a területen csúcsosodhatnak ki, és léphetnek át egy olyan határt, amely már túlmegy az „egyszerű” bűnelkövetésen, haszonszerzésen. Amikor már bizonyos ideológiai színezetet is kap a számítástechnikai rendszerek elleni támadás (legyen az akár egyéni, akár összehangolt), akkor már egy egészen más minőségbe lép át és sokkal veszélyesebbé válik. Az utóbbi években a terrorista személyek is fogékonyra váltak a technikai újítások iránt. Ennek következtében a számítógépek, hálózatok, programok, okostelefonok stb. bekerültek a terrorizmus eszköztárába. Ahogy az egyes bűncselekmények, úgy a terrorizmus is megjelent a kibertérben és a hagyományos elkövetési módjai kiegészültek a modern technika adta lehetőségekkel. Nemcsak, hogy kiegészültek, hanem fel is erősíthetők, döbbenetes veszélyeket rejtve magában, de ezekről még később lesz szó.

Ebben a fejezetben kitekintünk a terrorizmus, illetve a kiberterrorizmus eredetére, valamint a kiberterrorizmus eszköztárára (az itt bemutatott informatikai bűncselekmények nem szükségszerű velejárói a kiberterrorizmusnak, hiszen bárki által megvalósíthatóak, azonban mégis ebben a pontban kívánom tárgyalni őket, mivel ezzel a fogalommal összhangban okozhatják a legnagyobb kárt és kihívást).

Elöljáróban tehát csak annyit, hogy a kiberterrorizmus és az ebben a szellemiségben elkövetett (hagyományos) és informatikai bűncselekmények, valamint ezek kombinációi (hagyományos és informatikai vagy több informatikai párhuzamosan) egy merőben újfajta, ismeretlen, és csak nagyon nehezen észlelhető és megelőzhető problémát generáltak, melyek a digitális kor „káros mellékhatásai”. A sajtóban olyan változatos elnevezésekkel találkozhatunk ezen negatívumok kapcsán, mint a „számítógépes AIDS” vagy a „delírium digitalis”.

5.1. Terrorizmus, mint jelenség

„analóg terrorizmus vs. digitális terrorizmus”

Tekintsük át röviden a terrorizmust, mint negatív hozadékot, mint „eszközt” és magának a szónak, illetve a jelenségnek a történetét.

A terrorizmus a maga puritán formájában mindig is létezett, de minden korban mást társítottak hozzá. 81 éve annak, hogy Magyarországon utoljára terrorcselekményt hajtottak végre. Matuska Szilveszter 1931 szeptemberében felrobbantotta a biatorbágyi viaduktot, melyen a Bécsbe tartó gyors haladt át, 22 ember halálát okozva.

A terrorizmus olyan ellenség, amely megfoghatatlan, kicsúszik üldözői kezéből, szinte minden irányzatot magába olvaszt, ugyanakkor veszélyt jelent a szabadságjogokra és a biztonságra. Napjaink antiterrorista jogalkotása egészen a 90-es évekig a repülőforgalom ellen elkövetett akciókra irányult. Az antiterrorizmus e korai szakaszában a klasszikus büntetőjog az egyes terrorista akciókat büntette és próbálta megelőzni. (pl. gépeltérítések, túszedések). A terrorizmus³³ kifejezést ekkor még nem alkalmazták. A nemzetközi jogban ez a szó két nem túl régi szövegben jelent meg először: a robbanóanyagokkal elkövetett terrormerényletek megtorlásáról szóló nemzetközi egyezményben (New York, 1997. december 15.) és a terrorizmus pénzügyi támogatását büntető nemzetközi szerződésben (New York, 1999. december 9.). (Nem árt leszögezni azonban, hogy a terrorizmus jelentését egyik alkalommal sem határozták meg pontosan.)³⁴

Habár a legtöbb ember felismeri a terrorizmust, ha szembetalálkozik vele, a szakértők nem nagyon tudják általánosan elfogadott módon definiálni a jelenséget. Az Egyesült Államok külügyminisztériuma például a következő meghatározást adja: *„A terrorizmus előre kitervelt, politikai okokból kivitelezett erőszak, amelyet békés (fegyvertelen) célpontok ellen követnek el csoportok vagy titkos ügynökök azzal a szándékkal, hogy befolyásolják a közvéleményt.”*

³³ A kifejezés a nagy francia forradalom idején született meg, amikor 1793-94-ben a jakobinusok terrorja (a latin szó jelentése: félelem) uralkodott Franciaországban. Úgy tekintettek a terrorra, mint a szabadság megvédelmezésének legjobb eszközére. A terrorizmus tehát egyáltalán nem új jelenség.

³⁴ Ferwagner Péter Ákos-Komár Krisztián-Szélinger Balázs: *Terrorista szervezetek lexikona*. Szeged, Maxim Könyvkiadó, 2003, 9. o.

Paul Pillar, az amerikai Központi Hírszerző Ügynökség (CIA) Terrorrelhárító Központjának egykori igazgatóhelyettese szerint a terrorizmusnak négy kulcseleme van:

- 1. Előre megfontolt, kitervelt, a leggyakrabban valamilyen sérelem vagy düh által gerjesztett cselekedet.**
- 2. Politikai, nem pedig bűnügyi kategória, nem úgy, mint az az erőszak, amelyet valamilyen csoport vagy a maffia pénzszerzés céljából követ el, mert ebben az esetben a pénzszerzés a fennálló politikai rend megváltoztatását szolgálja.**
- 3. A polgári lakosságot, s nem a katonaságot vagy harcra kész csapatokat célozza meg.**
- 4. Egy népből, nemzetből való csoport hajtja végre, nem pedig egy ország hadserege.**³⁵

Ezekben a meghatározásokban a terrorizmus valódi lényege: erőszak alkalmazása ártatlan embereken, akik a legitimnek nyilvánított konfliktusterületen kívül tartózkodnak. Tény, hogy minél távolabb van a támadás célpontja a terroristák által sérelmesnek minősített kapcsolódási pontoktól, annál nagyobb a kiváltott félelem. A valódi üzenet tehát: a társadalom minden tagja „bűnös”, bárkiből lehet áldozat, azaz senki sem érezheti magát biztonságban.³⁶

A terroristák a társadalom széles rétegét akarják megfélemlíteni, mert így akarnak kicsikarni bizonyos politikai irányváltást. A terrorizmus nem pusztán brutális, meggondolatlan erőszak. Szakértők egyetértenek abban, hogy a **terrorakciók mögött mindig meghúzódik valamilyen stratégia**, mindig megfontoltan alkalmazzák civilek ellen, politikai vagy vallási célokból.³⁷

A legrégebbi terroristák azok a szent harcosok voltak, akik a polgári lakosság körében követtek el gyilkosságokat. Az időszámításunk szerinti 1. századi Palesztinában például fanatikus, vakbuzgó zsidók elvágta a rómaiak és a velük együttműködők torkát. A 7. századi Indiában az egyik vallásos szekta tagjai megfojtották azokat, akik a területükre tévedtek, hogy Kali hindu istennek áldozatul kínálják fel őket.

³⁵ Ferwagner-Komár-Szélinger, 2003, 10-11. o.

³⁶ Ferwagner-Komár-Szélinger, 2003, 12. o.

³⁷ Szembe kell nézni azzal, hogy minden esetben terrorizmust szül, ha valamilyen politikai vagy társadalmi törekvést hatalmas túlerővel elnyomnak. Az asszimetria oda vezethet, hogy a gyengébb fél „harcászati metodikaként” választ terrormódszereket. A terrorizmus napjainkra bekerült a hadviselés eszköztárába.

Az általunk jól ismert terrorizmus formái – melyeket gyakran már a tévékamerák is bemutattak – 1968. július 22-én jelentek meg először, amikor a Népi Front Palesztina Felszabadításáért először térített el egy kereskedelmi repülőgépet.³⁸

1. táblázat. A terrorizmus megjelenési formái

	Konvencionális terrorizmus	Tömegpusztító fegyvereket alkalmazó terrorizmus	Számítógépes terrorizmus
Módszerek	Személyek elrablása; közlekedési eszközök hatalomba kerülése; személyek, épületek, infrastruktúrák elleni robbantásos merényletek.	Nukleáris, biológiai és vegyi anyagok harci eszközökké való illetéktelen átalakítása és felhasználása.	Elektronikus vezérlőrendszerekbe való behatolás, ezek manipulálása, ellenük való szabotázs (például: hacking, vírusfejllesztés stb.).
Eszközeik	Hagyományos fegyverek: robbanóanyagok, lőfegyverek, rakéták. Újdonság: eltérített repülőgép, mint mozgó bomba.	Nukleáris bombák; radioaktív, biológiai (vírus, baktérium stb.) vagy vegyi anyagokkal töltött hagyományos (vagy kevert, például „piszkos bombák”*) robbanóeszközök.	Számítógépek, számítógéprendszerek.
Hatásuk	Nagy.	Nagyon nagy.	Nagy.
Fellépésük	Megelőzhető.	Nehezen, de megelőzhető.	Nehezen előzhető meg.
A közvélemény érdeklődése irányukban	Csökken, kivéve a különösen felháborító formában végrehajtott, vagy sok áldozatot követelő eseteket.	Nagyon magas.	Nagyon magas.
A tömegtájékoztató érdeklődése irányukban	Közepes, kivéve a különösen felháborító formában végrehajtott, vagy sok áldozatot követelő eseteket.	Nagyon magas.	Magas.

* A szakzsargonban „piszkos bombának” nevezik a hagyományos kémiai robbanószer és az erősen sugárzó radioaktív anyag (például atomerőművek hulladéka) elegyéből elkészített robbanóeszközt.

39

A terrorizmus megjelenési formái

4.3.1. Kapcsolata a szervezett bűnözéssel

A szervezett bűnözés a világ szinte minden országában megtalálható. Az utóbbi évtizedekben elterjedt terrorizmus a társadalmak ellen irányuló szervezett bűnözés új formája. Ez az új típusú bűnözés az 1960-as évek végén jelent meg és söpört végig a

³⁸ Ferwagner-Komár-Szélinger, 2003, 14. o.

³⁹ Korinek László: *A terrorizmus*, In Gönczöl Katalin-Kerecsi Klára-Korinek László-Lévay Miklós (szerk.): *Kriminológia-Szakkriminológia*, Complex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., Budapest, 2006, 451. o.

nyugati országokon, Dél-Amerikán, Afrikán, a Közel-Keleten, Közép- és Dél-Ázsián.

Ez az erőszak azonban alapjaiban különbözik a szervezett bűnözéstől. Míg a hagyományos szervezett bűnözés célja az anyagi haszonszerzés, addig a terroristák által alkalmazott erőszak mindig politikai célzatú. A gengszterek csak azt ölik meg, akiknek – rendszerint más gengsztereknek – a meggyilkolása révén megszerezhetik vagy megtarthatják a legális vagy illegális kereskedelem területeit. A terroristák ugyanakkor a társadalom sokkal szélesebb rétegét akarják megfélemlíteni.⁴⁰

5.2. Kiberterrorizmus

Az előző pontban említett szélesebb társadalmi réteg pedig a mai technikai viszonyok között már könnyedén elérhető, manipulálható és megfélemlíthető.

Napjainkra a terrorizmus megtalálható a kibertérben is. Az elmúlt tíz évben számos esetet jelentettek, amelyek e körbe vonhatók.⁴¹ A terroristák nagyon intenzíven érdeklődnek a nyilvánosság iránt. A modern terrorizmus egyenesen a médiára van szabva. A terrorizmus gyakran szándékosan szimbolikus célpontok ellen alkalmaz erőszakot. A terrorizmusnak az olyan „tradicionalis” fajtái, mint például a narkoterrorizmus, mellett egy viszonylag fiatal alfaj is kialakult. **A kiberterrorizmus** – a kifejezés a 80-as években született – **a számítógépek, hálózatok és információáramlás területén folytatott terrortevékenység.** Mivel a nyugati társadalom egyre nagyobb mértékben használja a világhálót és kötődik az informatikai technológiához, a kiberterrorizmus mind komolyabb pusztítást okozhat, ami akár a terrorizmus kedvelt formájává is válhat. **A kiberterrorizmus nem azonos a hackerek tevékenységével!**

Ahogy más terrorakció, ez is tipikusan előre kitervelt, politikai célokból végrehajtott, kisebb csoportok, ritkán kormányok által kivitelezett támadás, amit figyelemfelkeltésre, félelemkeltésre vagy a közvélemény és a döntéshozók befolyásolására használnak fel.⁴² A stratégiát a nagy társadalmi visszhangra építik. **Brian Jenkins** már 1974-ben megfogalmazta: „a terrorizmus színház”.

A kiberterrorizmust tekintve nem lehet olyan pontos adatokkal szolgálni, mint a „hagyományosnál” hiszen más közegben, eltérő körülmények között történik.

⁴⁰ Ferwagner-Komár-Szélinger, 2003, 9. o.

⁴¹ Moore, 2011, 255. o.

⁴² Ferwagner-Komár-Szélinger, 2003, 29. o.

Önmagában más a funkciója és az eszközök. Az Internetes támadás nem szed áldozatokat - hacsak nem olyan célpont az áldozat, ahol a polgárok közvetlenül ki vannak téve veszélynek; pl.: kórház, energiaellátó- és szállító rendszerek, közműszolgáltatások, stb.. *A cél ilyen behatolások esetében adat- vagy információszerzés, megfigyelés, működési zavar előidézése, stb..* A legtöbb esetben a cél, hogy nagy médiavisszhangot szerezzenek a támadók, vagy legalábbis figyelmet kapjon a tettük.

A kiberterrorizmus egyik nagy "előnye", hogy nem kell fizikailag jelen lenni a célponthoz való hozzáféréshez, nem kell hozzá sok ember. Az ilyen jellegű akcióknál a támadók messze lehetnek a célponttól, nem kell határokon átkelniük, repülőtéri detektoros kapukon fegyvereket becsempészniük, egyéb fizikai gátakat leküzdeniük. A kiberterroristáknak még a kormányok hallgatóságos beleegyezésére vagy gyengeségére sincs szükségük, és minden gond nélkül titokban tarthatják kilétüket vagy tartózkodási helyüket.⁴³ A terroristák arra is felhasználhatják az ilyen jellegű támadásokat, hogy más jellegű akcióik hatását felerősítsék.

Ha például sikerül megakadályozni a mentőegységek kommunikációját vagy blokkolni a az áram- vagy a vízszolgáltatást hagyományos bomba, biológiai vagy kémiai támadás idején, akkor az növelheti az okozott kár mértékét. Szakértők szerint éppen az ilyen típusú koordinált támadások lehetnek a kiberterrorizmus leghatékonyabb formái.

Nem tudni pontosan, hogy például a legnagyobb ellenségnek kikiáltott al-Kaida rendelkezik-e képességekkel a kiberterrorizmus területén. Egyesek szerint próbálkozott Afganisztánban embereket ilyen feladatokra kiképezni, s olyan számítógépeket is találtak az ázsiai országban, amelyekben az amerikai energiaszolgáltatókról, a vízszolgáltatókról, a kommunikációs rendszerekről és más fontos infrastrukturális területekről találtak információkat, adatokat.

Az elmúlt években az Egyesült Államokban is fokozódik a kiberterrorizmus iránt táplált félelem. Az „elkerülhetetlen” kibertámadások elleni védelmi képesség erősítésére szólította fel az amerikai informatikai biztonságért felelős vezetőket **Keith Alexander** tábornok, a külföldön végzett elektronikus hírszerzésre 1952-ben alapított Nemzetbiztonsági Ügynökség (*National Security Agency, NSA*) vezetője.

⁴³ Változás a „klasszikus” terrorizmushoz képest, hogy ebben a körben az „öngyilkos merénylő” viszonylag nehezen értelmezhető, de persze nem kizárt. Azonban a kiberterrorizmusra inkább az a jellemző, hogy ezek az elkövetők is nagyban elkötelezettek az ügyük mellett, ám az életüket nem igazán akaródzik feláldozni a siker érdekében. Az életáldozat tehát nem tipikus. *Lásd: Moore, 2011, 253. o.*

Ugyanez az ügynökség már 1997-ben nagyszabású titkos kísérletbe kezdett. Harmincöt hackert béreltek fel, hogy szimulált kibertámadást indítsanak. Az NSA azt kívánta vizsgálni, hogy a megtámadott szervek milyen intézkedéseket tesznek, hogy elhárítsák a támadást, és, hogy ezek elegendőek-e. A teszt eredményeként a hackerek az alábbi tetteket vitték véghez:

1. Az áramhálózat Los Angelesben, Chicagóban, Washingtonban és New Yorkban összeomlott, komoly áramkimaradást okozva ezen városok környékén,
2. Egy utasszállító gép ikonját eltüntették a légi irányítás képernyőjéről, aminek következtében a gép később lezuhant,
3. A washingtoni áramhálózat bedöntésével, a hackerek képesek voltak a 911-es segélykérő hálózatot is tönkretenni,
4. A Védelmi Minisztériumban egyszerre kapcsolták le a számítógép-, telefon- és e-mail hálózatot.
5. A haditengerészet egyik cirkálójának számítógépes rendszerét szintén lekapcsolták.

Az „Operation Eligible Receiver” névre keresztelt gúnytámadás során a hackerek a Védelmi Minisztérium 36 gépe felett vették át az irányítást, mely irányítás olyan elemi szinten történt, hogy a támadók bármit megcsinálhattak volna a gépekkel, amihez csak kedvük lett volna. Ez az akció felnyitotta a rendszerek működéséért felelősök szemét. Természetesen a repülőgép katasztrófa nem volt valós, de a felismerés az volt: itt akár emberek is meghalhattak volna!⁴⁴

A tábornok az informatikai biztonsági szakemberek konferenciáján komolynak minősítette a kibertámadásokkal kapcsolatos helyzetet, hangsúlyozva, hogy a pusztító eszközöket javarészt még nem vetették be, ezért ezt az időt ki kell használni a védelem erősítésére. **William S. Lynn**, a volt amerikai védelmi miniszterhelyettes ugyancsak ilyen támadások veszélyére hívta fel a figyelmet, melyeket érzékeny pontokra, például áramellátó központokra mérhetnek. Megítélése szerint a katonai hálózatok vagy a polgári infrastruktúra olyan csomópontjai, mint a közlekedési rendszerek vagy az energiaszektor elleni támadások képzelhetők el, melynek súlyos gazdasági következményei, anyagi kára és emberáldozat lehet az ára. Lynn szerint a katonai elhárításnak kellene védenie a civil infrastruktúrának ezen szegmenseit. Szerinte ez ugyanolyan együttműködés lenne a hadsereg és a szolgáltatók között, mint amikor mondjuk hurrikán esetén a katonai járművek is részt vesznek a mentésben.⁴⁵

Egyébként nem tudni, hogy hány szervezet rendelkezik a kiberterrorizmushoz

⁴⁴ Moore, 2011, 255-256. o.

⁴⁵ <http://htka.hu/2011/02/25/kiberterroristak-tamadasatol-tart-az-usa/> [2011. 11 14]

szükséges szakértelemmel. A Tamil Tigrisek⁴⁶ már követték el ilyen akciókat Srí Lanka kormánya ellen. A japán Aum Sinrikjo szekta készen állt a japán rendőrség kommunikációjának megakadályozására. A kiberterrorizmus, mivel nélkülözi a hagyományos terroreszközök drámaiságát, sok csoport számára nem vonzó.⁴⁷

A terroristák azonban nem csak terrorcselekményeket hajtanak végre a neten, hanem saját magukat is propagálják. Míg évekkel ezelőtt a terroristák csak akkor kaptak felületet, ha a híradóban, netán a sajtóban szerepeltek, mára azonban minden "magára valamit is adó" terrorszervezet rendelkezik honlappal. 2001. szeptember 11-e előtt a terrorcselekmények informatikai háttere nem sok figyelmet kaptak. A propagandát szolgálja az önálló honlap készítése, melyet aztán fel lehet tölteni olyan elemekkel, mint a házi videó (mely egyre jobb minőségű), a manipulált fényképek, vagy a különféle animációk. A saját logo, vagy zászló profilt kölcsönöz a terrorszervezetnek, és utána sokkal könnyebb azonosítani.

A <http://www.siteinstitute.org/> oldalon a terroristák által készített felvételek vannak. Olyan felvételek, melyeket 2001 előtt csak elvétve, vagy egyáltalán nem láthattunk a világhálón. **Az elmúlt 10 évben a terrorista oldalak száma 12-ről 4500-ra emelkedett.**

5.3. A terrorizmus elleni harc

A terrorizmus elleni fellépés mindig magában hordozza annak a veszélyét, hogy az állam a terroristák céljával egybevágoan hagyja magát provokálni, és a válaszlépésekkel belép egy felettébb bizonytalan, öngerjesztő folyamatba. További általános gond, hogy a terrorizmus elleni harc nemcsak hogy drága, de elkerülhetetlenül együtt jár számtalan, a demokratikus jogállam lényegét adó alkotmányos- és szabadságjog korlátozással.

*A cél olyan stratégia megválasztása, amely **megfelelő, alkalmas, megbízható és arányos.*** A **megfelelő** jelző azt jelenti, hogy a terrorista cselekményekre adott választ a társadalom meghatározó része kellően határozottnak, de ugyanakkor visszafogottnak találja, vagyis a *reakció a közvélemény többsége számára elfogadható legyen.* Az **alkalmasság** a terrorizmust kiváltó *társadalmi okok alapos vizsgálatára utal.* A

⁴⁶ A Tamil Tigrisek a Srí Lanka-i kormány ellen harcoló szeparatista szervezet. Az utóbbi években messze a legtöbb öngyilkos támadást ők hajtották végre.

⁴⁷ Ferwagner-Komár-Szélinger, 2003, 30. o.

megbízhatóság az antiterrorista politika egészének módját jelenti. A *politikai cél megszabása után a végrehajtóknak minden esetben eltökéltségre, következetességre és a részrehajlás nélküli konzisztens alkalmazásra van szükségük.* Az **arányosság** pedig azt jelenti, hogy az állam reakciójának arányban kell állnia a sérelemmel. Csak az a visszavágás igazolható az elszenvedett sérelemmel, amely nem teremt hivatkozási alapot az erőszak fokozására.⁴⁸ Ezek alapján többé-kevésbé meghatározhatóak az antiterrorista stratégia legfontosabb elemei:

- ***Törekvés a terrorizmust kiváltó társadalmi, politikai, etnikai, vallási feszültségek demokratikus módon való megszüntetésére.***
- ***A biztonsági erők létszámának, kiképzettségének, technikai felszereltségének erősítése.***
- ***A társadalmi mozgástér kockázatainak csökkentése.*** (például mikrochipes útleveél, a repülőtereken a bőröndök fóliázása, mágneskapuk stb.)
- ***A társadalom tagjai feletti fokozott ellenőrzés.***
- ***A médiával az ésszerű önkorlátozás elfogadtatása,*** annak érdekében, hogy a terroristák nehezebben jussanak az óhajtott nyilvánossághoz.
- ***Különleges antiterrorista törvények elfogadása.*** (Bizonyos törvények a magukat meggondoló, bűnbánó terroristáknak kiutat, visszatérést jelent, amennyiben világszemléletük meggyőzően megváltozik. Például az olasz penitenciatörvény (1982) vagy a disszociális törvény (1987).
- ***A nemzetközi összefogás erősítése.***
- ***A szóba jöhető terrorista célpontok védelmének fokozása.***
- ***A terroristák anyagi bázisának szétrombolása.***
- ***A nemzeti adatbázisok egyesítése.***⁴⁹

Az antiterrorista stratégia elemei

⁴⁸ Korinek, 2006, 457. o.

⁴⁹ Korinek, 2006, 458-459. o.

5.4. A kiberterrorizmus eszköztára:

Vegyük sorra, hogy milyen arzenál áll a számítógépes bűnözők és kiberterroristák rendelkezésére. A felsorolás nem tekinthető örökérvényűnek, hiszen naponta jelenhetnek meg újabb fenyegetések

Előtte azonban szólnunk kell néhány szót a **malware** támadásokról általában. A kifejezés a malicious software angol szóösszetételre utal, amely valamilyen rosszindulatú programot jelent. Egy összefoglaló elnevezés, amely a számítógépes munkafolyamatot, elektronikus adatot, a számítástechnikai eszközöket károsító programokat felöleli. Ilyenek például a **számítógépvírusok és programférgek**, melyek különböző hatásúak lehetnek, melyek adatállományok, programok, hardverek ellen irányulnak. A **trójai-programok** egy másik programhoz kapcsolódik. Az eredeti program indításakor a felhasználó tudta és akarata nélkül aktiválódik, és távolról vezérelhető zombi-géppé a számítógépeinket. Ez pedig sajnos **nem a felhasználónak szerencse, hanem csakis a botnetek irányítóinak.**⁵⁰

A **botnet** (*robot network*) zombi számítógépek hálózata.

A **zombi számítógép** olyan számítógép, amelyet különböző vírusokkal és trójai szoftverekkel irányítása alá vesz egy cracker. A számítógép erőforrásait ezután a saját céljára, sokszor DoS-támadások erősítésére használja. Az ilyen botokkal irányított gépeket használják spamek küldésére is.

A **botnet** célja, hogy nagy teljesítményű, gyors, mégis anonim infrastruktúrát nyújtson a spammernek, mellyel az könnyen és gyorsan tud nagy mennyiségű spamet küldeni, illetve más törvénytelen cselekedeteket folytatni. A botneteket hétköznapi, otthoni, iskolai, vállalati számítógépek alkotják. Egy számítógép anélkül tagja lehet egy botnetnek, hogy a gazdája ezt kérte, megengedte volna, vagy akár egyáltalán tudna róla. Egy speciális program települ a gépre, mely a háttérben fut anélkül, hogy a számítógép gazdája azt észrevenné.

Egy botnet gyakran több tízezer számítógépből áll. Méretük folyamatosan változik.

A spyware-ek (kémprogram) a felhasználó aktivitását rögzíti, jelszavainkat vagy más ránk vonatkozó adatot fűrkész ki és továbbítja egy másik számítógépre a hálózaton, Részben hírszerzési célokat szolgál. A **keylogger-programok** olyan speciális kémprogramok, amelyek naplózzák a billentyűleütéseket. Ezek voltak a program alapú malware-ek.

⁵⁰ http://antivirus.blog.hu/2010/03/16/668_szazalek_novekedes [2011. 08. 10]

Léteznek még a szöveg alapú malware-ek. Ilyenek például a **spam-ek**, mely kéretlen kereskedelmi küldeményeket jelent. Sajnos milliószámra terjednek a számítógépes hálózatokon, foglalva a memóriát, használva a rendszergazdák drága munkaidejét, idegesítve a felhasználókat ezek törlésével. A **hoax-levelek** általános, gyerekes szövege, a felhasználó babonás félelmére épít. A **phishing-re** a későbbiekben bővebben kitérek még.

Az ilyen programok kétféleképp kerülhetnek gépeinkre. Az egyik az *offline* feltöltés, melyhez fizikai jelenlét is szükséges. Külső adathordozó útján terjeszthető. A számítógépes hálózatok elterjedésével ez a módszer háttérbe szorult, és napjainkban elegendő az *online* feltöltés. Előnye, hogy gyors és egyszerű, nem kell jelen lenni. Egy merőben új kihívás nehezíti napjainkban a felhasználók életét. A fent említett malware-ek hatásmechanizmusa az ún. nulladik napi támadást követően ismert lesz, így az ellenük kifejlesztett vírusirtó programok is hamarosan megjelennek. Ezzel szemben elmondható, hogy a kiberháború új minőségű szakba lépett. A **Stuxnet** és a **DuQu** egyedi, célzott hatása miatt nem valószínű, hogy lesz általános ellenszere. Míg a kommersz malware-ek minden számítógépen ugyanazon hatásokat váltják ki, addig ez a két újfajta program csak egy-egy célba vett technikai-technológiai vagy más művelet megbénítására alkalmas. A precíziós bombázáshoz hasonlóan, ez is célzott támadás.

Az USA ilyen malware-rel kívánta lassítani az iráni atomprogramot. Bár a források nem cáfolták és nem erősítették meg. Az amerikai kormányzat legfelső szintje rendelte meg a támadást. Az akció fedőneve: „Olympic Games” volt. A feladatot bonyolította, hogy a natanzi erőmű belső informatikai hálózata offline üzemmódban működött, tehát csakis helyszíni feltöltés volt lehetséges. A Stuxnet beépült az operációs rendszerbe és azon keresztül fejtette ki hatását. Úgy írták meg a programot, hogy más rendszerekben ne tehessen kárt, csakis a centrifugák működésének megzavarására alkották meg. Mire felfedezték a vírust, addigra már három mutálódott verzió futott az atomerőmű számítógépein, és tönkretett kétezzer centrifugát a nyolcezerből. Ez történt 2009-2010 között. A Stuxnet egy félelmetesen hatásos program, viszonylag békés eszköze a harcnak. Azonban az iráni kiruccanása után a program ismertté vált, elemei kikerültek a „szabadpiacra”. Valószínűsíthető, hogy mára már jóval fejlettebb eszközök is léteznek.

Lássunk néhány veszélyesebb támadást kicsit részletesebben:

5.4.1. Phishing⁵¹

A modern információs és informatikai rendszerek transznacionális és határok nélküli jellegéből adódóan mára az egyik legelterjedtebb bűnözési formává a számítógéppel elkövetett visszaélések váltak. Ennek leginkább terjedő formája az adathalászat, azaz phishing. Az utóbbi időben Magyarországon is egyre nagyobb problémát jelent. Az adathalászok (identitás tolvajok) célja, hogy minél rövidebb idő alatt a lehető legtöbb adatot megszerezzék. Mivel a csalók általában megbízható személynek vagy cégnek adják ki magukat, és az Interneten keresztül (személytelenségbe burkolózva) lépnek kapcsolatba az áldozatokkal, nagy esélyük van arra, hogy tetteiket sikeresen vigyék véghez. **A csalások érintettjei csak utólag, és sokszor nagy veszteségek árán értesülnek a történetekről.**

Az adathalászat, mint bűnözési forma, amelynek célja ma már egyértelműen az anyagi haszonszerzés, a "bizalomra építő támadások" kategóriájába tartozik. *A módszerről az 1990-es évek közepén, az egyik legnagyobb amerikai internetszolgáltató, az AOL ellen elkövetett adatlopás révén értesült a világ.*⁵²

A veszély ma globális szinten folyamatosan nő, a technika pedig a személyi számítógépek és szoftverek fejlődésével egyidejűleg tökéletesedik.

A legfontosabb tanulság, hogy az elektronikus levelezés, valamint az Internetezés során nagyon körültekintően és megfontoltan kell cselekedni, ugyanis az egyre kifinomultabb és trükkösebb csalások egyik legfontosabb mozgatórugója az emberi hiszékenységre és a kíváncsiságra.

Az utóbbi években, az ún. okostelefonok színrelépésével egy újabb szinten is kamatoztathatják tudásukat a számítógépes bűnelkövetők. Ezek hamisítatlanul XXI. századi eszközök, amelyek PC-szerű funkciókkal is rendelkezhetnek. Ez azonban csak egy, a számos meghatározás közül. Nincs elfogadott definíció arra a kérdésre, hogy mi is az az okostelefon. Éppen a fent említett számítógép jellege vonzza az informatikai bűncselekmények elkövetésére szakosodott egyéneket. Mivel mára már szinte valamennyi számítógép adta lehetőség elérhető és használható a telefonokon, így logikusan következik, hogy a számítógépes bűncselekmények elkövetésének feltételei is

⁵¹ Password harvesting fishing = jelszóhalászat

⁵² Magyarországon az első, ismertté vált phishing támadás az Inter-Európa Bankot érte, 2003-ban.

hiánytalanul megvannak. Felgyorsult életünk megköveteli, hogy alkalmazkodjunk a felgyorsult világhoz, és egyre kevésbé kerülhető ki, hogy a modern technika rabjaivá váljunk. Az okostelefonokkal gond nélkül csatlakozhatunk az Internetre – amennyiben elérhető egy WI-FI hálózat, vagy egyéb, előfizetéses módon lehetőség van rá -, és máris teret engedünk, hogy adatainkhoz hozzáférjenek. E-mail, közösségi oldalak, Skype, web böngészés, adatforgalom, még a fájlcsereléshez is adott minden. Ezek során pedig könnyen áldozatul eshet a gyanútlan felhasználó.

Az egyik legnagyobb problémát az aktív mobilbankolás jelenti. Ennek során már nem csak személyes adatainkat „vadászhatják” le, hanem pénzünket is. Hozzáférhetnek jelszavainkhoz (amennyiben ki sem jelentkezünk ezen rendszerekből, arra sincs szükség), manipulálhatják pénzügyi tranzakcióinkat, kárt okozva ezzel.

A felhasználók 89 százaléka nem hiszi, hogy készülékén keresztül ellophatják pénzügyi adatait. Az AVG⁵³ megbízásából készült kutatás szerint a tengerentúli felhasználóknak nincs félelemérzetük, amikor okostelefonjukon egy banki alkalmazást használnak. Ezekkel az alkalmazásokkal akár banki átutalásokat is indíthatnak, és más megbízásokat is kiadhatnak a bankjuk felé, mintha csak az otthoni számítógépeik előtt ülnének.

A különbség főleg abban áll, hogy míg az otthoni környezetben kialakult egy egészséges félelemérzet a vírusokkal, adathalászokkal és egyéb fenyegetettségekkel szemben, addig az okostelefonoknál ez hiányzik. A felmérés szerint 89 százaléka egyáltalán nem tart attól, hogy mobilbankolás során illetéktelenek juthatnak az adataikhoz. A válaszolók 91 százaléka emellett nem tart egy olyan vírusfertőzéstől, amely a banki szoftvert is érintheti. Ráadásul ezzel párhuzamosan 29 százaléuk tárol bizalmas pénzügyi adatokat, 35 százaléuk pedig bizalmas dokumentumokat az okostelefonján.⁵⁴

5.4.2. Vishing

A phishing egyik egyre inkább terjedő változata a vishing, azaz az Internet alapú telefonálásra (VoIP) épülő csalás. Mivel a bankok jelentős része azt javasolja, hogy phishing e-mail érkezésének gyanúja esetén az ügyfél hívja fel a bankot, mert a telefonos megerősítés segíthet elkerülni azt, hogy adathalászat áldozatává váljon, ez a

⁵³ Az AVG Technologies, korábbi nevén Grisoft, 2001-ben alakult Csehországban, de kiterjedt hálózattal rendelkezik Európa többi részén és az Egyesült Államok területén is. A cég fő profilja a számítógépes biztonság.

⁵⁴ <http://techcorner.hu/computerworld/fejlett-mobilbankolas-nem-gondolunk-a-veszelyekre.html> [2012. 11. 23]

módszer jelentős sikereket hoz a csalóknak, ráadásul - olcsósága miatt - hamar megtérül. A bűnözők egy adott körzetszámot alapul véve automatizált programot indítanak, amely egymás után tárcsázza a lehetséges hívószámokat. Amennyiben a telefont felveszik vagy bekapcsol az üzenetrögzítő, azt kéri egy gépi hang, hogy a tulajdonos hívjon fel egy megadott telefonszámot, mivel a rendszer letiltotta a bank- vagy hitelkártyáját. A csalók rendszerint ügyelnek arra, hogy a telefonszám a lehető legjobban hasonlítson a bankok tényleges ügyfélszolgálati számaihoz. Ha az illető felhívja, akkor a nyomógomb-választós, automatikus rendszer (több más lehetőség mellett) elmondja, hogy ha letiltott kártyáját kívánja újraaktiválni, adja meg a nevét, a kártya számát, a régi és az új PIN kódot. Így a csalók minden adat birtokába jutnak.

Az eddigiekben tárgyalt módszerek minden esetben a felhasználó - nem tudatos - együttműködését feltételezték. Az **ún. "eltérítéssel adathalászat" (pharming)** azonban a jövőbeni fenyegetések közül az egyik legveszélyesebb. *Itt ugyanis nem szükséges a felhasználó kooperációja, sőt, az érintett általában nem is tud arról, hogy - számítógépe révén - milyen jellegű cselekmény részesévé vált.*⁵⁵

5.4.3. Keylogging

A pharming kategóriájába sorolható az az eset, amikor a trójai program, a vírus, a becsapós e-mail vagy az álweboldal "kiegészítésképpen" ún. billentyűleütést naplózó (keylogger) funkcióval is rendelkezik.

Világszerte 2000-től kezdve (300 feltárt eset) folyamatosan nőtt az ilyen módszerrel elkövetett, ismertté vált támadások száma, 2005-től pedig már aggasztó méreteket öltött (6191 feltárt eset)! Ezek a számok évről évre sokszorozódnak.

Az Internetről százával tölthetők le erre képes programok.⁵⁶

Érdekes – és egyben ezernyi kérdést duzzasztó – hír látott nemrég napvilágot. A NetworkWorld szakembere két laptopon is talált gyárilag telepített billentyűzet-naplózó

⁵⁵ <http://www.nbh.hu/oldpage/bmenu6pp.htm> [2011. 11. 02]

⁵⁶ Thomas, 2005, 45. o.

szoftvert. A gyártó részéről a terméktámogatási-szolgálat vezető munkatársa nem tagadta annak meglétét.

Nevezett program működése a felhasználó számára nem látható, viszont rögzít minden egyes billentyűleütést. Ráadásul azokat is, amiket a felhasználó a jelszó szövegmezőn üt le, így kiválóan alkalmas jelszólopásra.

Rájött, hogy a StarLogger gyárilag került a gépre, a maga részéről egyszerűen eltávolította azt és folytatta munkáját. Azonban amikor a géppel gond adódott és helyette egy másik, R540-es modellre váltott, akkor azon ugyanúgy ott ült a StarLogger.

A Samsung terméktámogatási szolgálat vezetője megerősítette, hogy, a Samsung helyezte el a StarLogger-t a laptopjain, hogy „*monitorozza a gép teljesítményét és használatát*”. Magyarán: a cég a vásárló megkérdezése nélkül kívánt adatokat gyűjteni a felhasználás módjáról.

Ez azonban a kisebbik gond. Ha nem is kérdőjelezi meg senki a szoftver telepítése mögötti jószándékot (merthogy a StarLogger-rel igen könnyű lenne visszaélni, jóformán mást sem lehet vele), az FTC⁵⁷ szerint egyértelmű, hogy illegális lépés. ***„Biztonsági lyukakat létrehozó titkos szoftverek telepítése tolawodó és törvénytelen.”***

Nyilvánvalóan törvénytelen és etikátlan az efféle tevékenység. Mindemellett nagy felelősség is kezelni azt a rengeteg adatot, ami a Samsung laptopokra telepített naplózó alkalmazásokból összegyűlik. A rengeteg, a lehető legérzékenyebb személyes és üzleti adatokból álló információhegy rossz kezekbe kerülve igen nagy károkat okozhat.⁵⁸

Nem sokkal később azonban megcáfolták a rémhíreket és a lavina elindítója elnézést kért. A GFI Security menedzsere a Sunbelt blogján kért elnézést minden érintettől, vállalva, hogy a Vipre agresszív kártevő-kutató eljárása adta a hamis riasztást, melyre támaszkodva a Samsung keylogger rémhír rövid idő alatt bejárta a világ híroldalait.

A szakember tévedését, (mint ahogy egy a vírusirtóét is, mely hamis riasztást adott, azt gondolva a Windows/SL mappáról, hogy a StarLogger fészke) a Microsoft !Live szlovén nyelvi mappája okozta.⁵⁹

A magyarázat megállja a helyét, mivel könnyedén előfordulhat egy ilyen „ütközés” a programok között. Mindenesetre erősen elgondolkodtató, hogy ha nincs ilyen gyárilag telepítve, akkor ugyan miért ismerte el a terméktámogatási szolgálat munkatársa a létét?

⁵⁷ Federal Trade Commission – Amerikai Szövetségi Kereskedelmi Felügyelet

⁵⁸ <http://nonstopmobil.hu/keylogger-lenne-samsung-laptopokon-20110331.html> [2011. 09. 08]

⁵⁹ <http://nonstopmobil.hu/nincs-samsung-keylogger-es-a-vipre-hibaja-a-remhir-20110401.html> [2011. 09. 09]

5.4.4. Hacking („elektronikus betörés”)

„Az információ szabad akar lenni, de mindenhol láncra verik.”⁶⁰

5.4.4.1. Alapvetés

Amikor korunkra jellemző gyorsasággal létrejött a világháló és berendeződött a kiberuniverzum, ahogy az már lenni szokott az új jelenségekkel az ember világában, születésével egy időben azonnal megjelent az árnya is.⁶¹ **A hacking talán a legtöbbször megvalósított számítógépes bűncselekmény.** A hacking-et és a hacker-t talán legkifejezőbben, „elektronikus vagy virtuális betörőnek, cselekményét pedig „elektronikus vagy virtuális betörésnek” magyarázhatnánk. Igazi magyar megfelelője nincs a fogalomnak, ahogy sajnos több számítástechnikai fogalomnak sem.⁶² Bár a XXI. századi média – tévesen – szinte kizárólag a számítógépkalóz, sőt a számítógépes bűnöző szinonimájaként használja, a hacker fogalma hatalmas átalakuláson ment át az elmúlt évtizedek folyamán.⁶³ Eredeti jelentése kezdetben teljesen mást jelenthetett. Valószínűleg a fafaragók nevezték így magukat a világ leghíresebb műegyetemén. Szintén ezzel a kifejezéssel illették a massachusettsi Technológiai Intézetben (MIT) a hagyományosnak számító trükkös diáktrefák kiagyalóit. Még az irodalmi művekben is inkább a pejoratív értelmében említik, ritkábban szerepel **„etikus támadóként”, holott ez is egyik jelentése.** Pedig igen sok köszönhető nekik. Hackerek építették az első személyi számítógépeket és ők fejlesztették ki az egyetemi-hálózatként induló Internetet is – aminek első, nyers alapjait persze a hadsereg alkotta meg. A diáktrefák pedig folytatódtak a kibertérben is: az összekapcsolt számítógépeket védő biztonsági rendszerek megkerülése, a neten keresztül elérhető rendszerek hozzáférési jogosultságainak megszerzése a digitális elit sportja és hobbija volt.⁶⁴ A hackerek ismerték és számon tartották egymást. Az Internet a múlt század kilencvenes éveinek elején rohamosan terjedt és a magánszektorba is egyre inkább beáramlott, így ezek

⁶⁰ Wark, McKenzie: *Hackerkiáltvány*. Ford.: Nagy Mónika Zsuzsanna, Budapest, Noran Libro Kiadó, 2010, 67. o.

⁶¹ Warren, Peter – Streeter, Michael: *Az internet sötét oldala*. Budapest, HVG Kiadó Rt., 2005, 7. o.

⁶² Nagy, 2009, 67. o.

⁶³ Mitnick, Kevin D. – Simon, William L.: *A legendás hacker – A megtévesztés művészete*. Ford.: Lénárt Szabolcs, Budapest, 2003, Perfect-Pro Kft., V.

⁶⁴ Ez kezdetben teljesen ártalmatlan, sőt biztonsági megoldásokat fejlesztő volt.

számítógépei is csatlakoztak a világhálóra. Ezek után a hacker szubkultúra léte egyre kényelmetlenebbé vált, hiszen a sorozatos betörések aláásták a rendszerek biztonságába vetett hitet. Megjelentek a károkozás tilalmát kimondó „hacker etikára” fittyet hányó számítógépkalózok is, akik rombolásra és nyerészkedésre használták a biztonsági hiányosságokat.⁶⁵

A rosszindulatú bitbuherátorok cracker néven kerültek be a szubkultúra szlengszótárába, amely ma is nagy hangsúlyt helyez a hacker és a cracker⁶⁶ megkülönböztetésére.

Az elektronikus adatfeldolgozási- és adatátviteli rendszerek védeltsége, biztonsága e tevékenységek zavartalan ellátásának első és legalapvetőbb követelménye.⁶⁷

Érdekes és sok szempontból tanulságos **McKenzie Wark** *Hackerkiáltvány* című munkája, melyben a szerző, burkoltan vagy épp nyilvánvalóan a marxista elméletet frissítette fel a modern korra optimalizálva azt.

Ebben a hackereket olyasvalakiknek írja le, akik mindig megteremtik annak a lehetőségét, hogy új dolgok jussanak a világba, melyek nem feltétlenül csak a jó dolgok, de mindenképpen újak. *A művészetben, a tudományban, a filozófiában és a kultúrában, illetve bármely tudástermékben, ahonnan adat gyűjthető, ahonnan információ nyerhető, és ahol az információból a világ számára új lehetőségek adódnak, ott vannak a hackerek, hogy kinyerjék az újat a régiből.* Jóllehet, mi teremtjük meg ezeket az új világokat, de nem mi birtokoljuk őket.

A hackerek arra használják tudásukat és éles elméjüket, hogy fenntartsák autonómiájukat. Egyesek csak a pénzért csinálják. Mások nem alkusznak meg. A hackerek általában nem csatlakoznak másokhoz. Nemigen akarózik feladniuk az egyedülállást.⁶⁸

Miként arra már történt utalás, az információs kor kiteljesedése soha nem látott mennyiségű adatot generál. A szükséglet fölötti, egyre bővülő mértékű többlet eredményeként a hackelés kapacitása is egyre kiterjedtebb.⁶⁹

⁶⁵ Mitnick – Simon, 2003, *Perfact-Pro Kft.*, V.

⁶⁶ A crackerek a szerzői jog megsértői. Az Interneten számtalan oldalon található ilyenre alkalmas programok. Lásd: Nagy Zoltán András: *A jogosulatlan belépés a számítógépes rendszerekbe (hacking) megítéléséről.* In Korinek László-Kóhalmi László-Herke Csongor (szerk.) *Emlékkönyv Irk Albert egyetemi tanár születésének 120. évfordulójára, 2004, Pécs, Kódex Nyomda Kft., 2004, 159. o..*

⁶⁷ Nagy, 2009, 67. o.

⁶⁸ Wark, 2010, 12-13. o.

⁶⁹ Wark, 2010, 14. o.

A hack megéri a virtuálist – és átalakítja az aktuálist.⁷⁰

A könyv szerzője – Wark – is megállapítja, hogy sokan a hackeri tevékenységet, kizárólag a kriminalitásra kívánják korlátozni. *Az az általánosabb vélekedés, hogy a hacking a fiatalkori bűnözés új formája, vagy a nihilista vandalizmus, netán a szervezett bűnözés kiszolgálója.*

De van, hogy a hackert ártalmatlan szubkulturaként jelenítik meg, mint valamely elragadtatott otthoni hobbitevékenységet.

A hacker valódi birodalma a virtuális. A hacker a virtuálisból teremti meg az aktuális mindig-új kifejezéseit. **Hackelni annyit tesz, mint a virtuálist az aktuálisba szabadítani.** A természet bármely tartománya lehet a virtuális forrása. A hackereknek az az érdekük, hogy szabadon hackelhessenek a hackelés kedvéért.⁷¹

5.4.4.2. A „szakma” képviselői

A lengyel **Andrzej Adamski** teljes joggal veti fel a „jó hacker” fogalmát. Tevékenykednek *nemes szándékú hackerek is, akik letörlik a pedofil és más pornó oldalakat, a gyűlöletkeltésre alkalmas uszításokat, a kábítószer-fogyasztást népszerűsítő, bombakészítést bemutató stb. oldalakat.*

Őket nevezi a szakma „**White-Hat Hackernek**”. Ezek ellentétei a „**Black-Hat Hackerek**”, akik a biztonságtechnikai intézkedések kijátszására írják a programokat. Hálózatokat is támadnak. A két kategória között helyezkednek el a „**Grey-Hat Hackerek**”. Őket akár opportunistáknak is nevezhetjük, mivel a világhálón keresgélve áldozatra lesnek, betörnek, majd erről értesítik a sértettet, és felajánlják segítségüket egy bizonyos térítés ellenében. A hacker létra legalsó fokán az ún. „**Script Kiddie**” áll. Akik jóval veszélyesebbek, mint azt pozíciójuk sugallná. Ők olyan programokat keresnek, amelyek alkalmasak az informatikai abúzusok elkövetésére, majd ezeket (tényleges hatásmechanizmusukat nem ismerve) rászabadítják a célpont gépére, nem is sejtve a lehetséges következményeket. Létezik még a „**Hactivist**” kategória, akik saját álláspontjuk terjesztésére veszik át a hatalmat pl. népszerű weboldalak fölött. Bizonyos szerzők a „**Kiberterroristákat**” is a hackerek egyik csoportjának tekintik, és annyiban megállja a helyét, hogy az ilyen terroristák valóban rendelkeznek számítástechnikai ismeretekkel.⁷² Azonban újra hangsúlyozandó, hogy a hacker nem

⁷⁰ „Ahhoz, hogy valami hack legyen, az eseményt át kell járnia az újításnak, a stílusnak és a technikai virtuozitásnak.”

⁷¹ Wark, 2010, 42-45. o.

⁷² Bryant, Robin: *Investigating digital crime*, John Wiley & Sons Ltd., Chichester, 2008, 24-26. o.

egyenlő a kiberterroristával. A kiberterroristáról feltételezhető, hogy hacker, de a hacker nem kiberterrorista!⁷³

Világszerte hackerek is tesztelik a szoftverek béta verzióit, így még a program kísérleti szakában mód áll a biztonság növelésére.

Realitás az is, hogy a bűnüldözés, a modern hadviselés sem nélkülözheti a hackinget.

Látható tehát, hogy a hacker szó nem a bűnöző vagy a kiberterrorista szinonimája, nem azonos a bűnelkövetés egyik új formájával. Óvakodni kell téves azonosítástól!

5.4.4.3. A hatályos hazai szabályozás

A hatályos szabályozás bemutatása előtt foglaljuk össze a szabályozás történetét dióhéjban.

Magyarországon egészen az 1990-es évekig szabályozatlan volt ez a terület. A számítógépes deliktumok fiatalága tetten érhető, mivel az Európa Tanács is csak az 1980-as évek második felében⁷⁴ hozott létre egy szakértői bizottságot, hogy összegezze a számítógépes bűncselekményekre vonatkozó ismereteket. A szakértői jelentés 1989-ben készült el és annak alapján az Európa Tanács 1989. szeptember 13-án ajánlást bocsátott ki a tagállamok számára arra nézve, hogy mely cselekményeket nyilvánítsanak büntetendővé. A nemzeti törvényhozásokhoz intézett útmutatás egy minimum és egy fakultatív listát tartalmazott.⁷⁵

Az ENSZ 1994-ben jelentette meg az informatikai bűnözéssel kapcsolatos tanulmányát, amely meghatározta a számítógéppel kapcsolatos bűncselekmények lehetséges megjelenési formáit és hangsúlyozta az együttműködés fontosságát.

Az Európai Gazdasági Közösség Tanácsa 1991. május 14-én fogadta el a „Számítógépi programok jogi védelméről” szóló, 91/250/EGK irányelvet, (amelyet

⁷³ Napjainkban az „Anonymus” nevű egyén (szervezet) tevékenysége jelenti az egyik legnagyobb kihívást.

⁷⁴ Az OECD külön bizottsága 1983 és 1985 között végzett felmérése az európai államok joggyakorlata és tapasztalatai alapján készítette el a büntetőjogi reformokat is sürgető, „Computer-Related Crime: Analysis of Legal Policy” című jelentését. (Lásd: Molnár Gábor: *Gazdasági bűncselekmények*, Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2009, 276. o.

⁷⁵ Lásd még: III. fejezet 3.1.1. pont

hatályos kívül helyezett az Európai Parlament és a Tanács 2009/14/EK irányelvének 10. cikké (2009. május 25. napjától).⁷⁶

Kezdetben Magyarországon (is) a csalás keretében értékelték ezt a bűncselekményt. Később az a felfogás vált uralkodóvá, hogy természetes személy, mint passzív alany hiányában a csalás megállapítására nem kerülhet sor. Ezért döntött a jogalkotó az ilyen jellegű cselekmények új tényállásban való szabályozására.⁷⁷ Ennek eredményeként hazánkban 1994. évi IX. törvény révén került pönalizálásra, számítógépes csalás néven.

Az 1996. évi LII. törvény további módosításként a hagyományos telefonok, valamint mobil rádiótelefonok útján igénybe vehető szolgáltatásokkal kapcsolatos visszaéléseket is büntetendővé nyilvánította, s ezzel kiegészítette a bűncselekmény törvényi tényállását.⁷⁸

Már ebben az időszakban is igényként merült fel a számítógépes adatok kikémlelésének szankcionálása, illetve az „elektronikus betörés” (hacking) önálló bűncselekménnyé nyilvánítása. Hiányoztak a Btk.-ból a számítógépes elkövetéssel kapcsolatos speciális definíciók is, mint például a számítógép, a számítógépes adat és adatfeldolgozás fogalma.

Újabb, jelentős változást hozott az 1999. évi CXX. törvény., amely a nagy nyilvánosság általános részi fogalmát kiterjesztette az elektronikusan rögzített információ távközlő hálózaton való közzétételére, valamint beiktatott számos kapcsolódó részletszabályt.^{79 80}

Az Európa Tanács informatikai bűnözésről szóló egyezményében foglalt büntetőjogi rendelkezésekkel összhangban léptette életbe a számítástechnikai rendszer és adatok elleni bűncselekmény tényállását a 2001. évi CXXI. törvény 57.§-a, mely ezzel a szabályozást koncepcionálisan változtatta meg.

A számítógépes csalás tényállása helyett a 300/C. §-ba iktatta a „Számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása”

⁷⁶ Molnár, 2009, 277. o.

⁷⁷ Molnár, 2009, 278. o.

⁷⁸ Horváth Tibor-Kereszty Béla-Maráz Vilmosné-Nagy Ferenc-Vida Mihály: *A magyar büntetőjog különös része*, Korona Kiadó, Budapest, 1999

⁷⁹ Molnár, 2009, 278. o.

⁸⁰ A Különös Részbe új – a számítógépes bűnözéssel összefüggő – bűncselekményeket iktatott be: a szerzői és szomszédos jog védelmét biztosító műszaki intézkedés kijátszását (329/A. §), a jogkezelési adat meghamisítását (329/C. §), valamint az iparjogvédelmi jogok megsértése tényállását (329/D. §), ezen felül a 300/C. § (2) bekezdése további minősített esetként jelölte meg, ha a bűncselekmény különösen jelentős kárt okoz. (Lásd: Molnár, 2009, 279. o.)

elnevezésű bűncselekményt és egyúttal a 300/F. §-ban található értelmező rendelkezésekben meghatározta a számítástechnikai rendszer fogalmát is.⁸¹ Ezzel a jogalkotó régi adósságot törlesztett, mely szabályozás végre időtállóan bizonyult.

A számítógépes bűncselekmények jogi tárgya általában

„A számítástechnikai rendszerek információ rögzítésére, feldolgozására, tárolására, továbbítására szolgálnak. Az elektronikus adatfeldolgozás- és adatátvitel egymásra épülő műveletek, feladatok sorozatát jelentik.

Mind az elektronikai adatfeldolgozás résztevékenységeit, mind annak egészét jogszabályok övezik, biztosítják. Ezen **normák meghatározzák az elektronikus adatfeldolgozás módját, terjedelmét, időbeli határait, a feldolgozást végzők jogait, kötelességeit, az adattovábbítás irányát, az adathordozók védelmét** stb. Ebből következik, hogy az elektronikus adatfeldolgozás rendjének kialakulnak konstans elemei, amelyek beépülnek az e körben születő jogi szabályokba. Kiemelkedően fontos társadalmi-gazdasági érdek az egyre bővülő és jelentősebbé váló elektronikus adatfeldolgozás és adatátvitel folyamatának, technikai feltételeinek, az ott kezelt információknak a biztonsága, védelme, zavartalansága, azaz az elektronikus adatfeldolgozó rendszer integritásának biztosítása.”⁸²

Mivel azonban ezek a rendszerek általában több funkciót is ellátnak, az ellenük irányuló támadás gyakran sért más társadalmi értéket is. Tehát ezek a bűncselekmények kettős jogtárggyal jellemezhetők. (pl. egy számítógépes csalás egyszerre sérti az adatfeldolgozás integritását és a vagyoni viszonyokat)⁸³

A számítógépes bűncselekmények elkövetési tárgya általában

A jogi tárgyak általában közvetett jellegűek, mivel zömében csak valamely, a jogi tárgyat megtestesítő tevékenységi tárgyon keresztül sérthetők vagy veszélyeztethetők. Ha a jogi tárgy kívülvilágban érzékelhető dologon szimbolizálódik, akkor tevékenységi tárgya van a bűncselekménynek. Ezzel szemben az immateriális bűncselekményeknél tevékenységi tárgy nem jöhet szóba.

A tevékenységi tárgy egyrészt a jogi tárgyat képező társadalmi viszony előfeltétele, másrészt pedig a védeni kívánt társadalmi viszony fizikai kifejeződése.

A büntető-jogtudomány napjainkig testi tárgyakat, illetve személyeket ért tevékenységi tárgy alatt.

A fizikai léttel bíró dolog sajátosságai az alábbiak:

- *A dolog a kívülvilágban testet öltött és látható objektum.*
- *Általában meghatározható vagyoni értékkel bír.*
- *A jogi védelem egyediségüket fogja át.*
- *Az ellene irányuló támadás a kívülvilágban változást idéz elő.*⁸⁴

⁸¹ Molnár, 2009, 280. o.

⁸² Nagy, 2009, 60. o.

⁸³ Nagy, 2009, 60. o.

⁸⁴ Nagy, 2009, 62-63. o.

Látható, hogy *az elektronikus adat nem teljesen felel meg a klasszikus tárgy „sémának”*.

Mégpedig:

- *Az elektronikus adat immateriális és láthatatlan, megjelenítésükhöz technikai eszközök és számítógépes szoftverek szükségesek.*

- *Az adat vagyoni értéke nem minden esetben határozható meg pontosan, az adat milyensége adhatja annak igazi értékét, egy adott környezetben, adott időben rendelkezik vagyoni értékkel.*

- *Jogi védelmük is, ebből következően csak akkor merül fel, ha saját környezetükből akarják törölni, kifürkészni, továbbítani. Egyediségük irreleváns, korlátlanul másolhatók.*

- *Az elektronikus adat immateriális jellegéből adódóan az ellene irányuló támadás sem idéz elő a külvilágban érzékelhető változást.*

A számítógépen vagy adathordozón tárolt adat ellopása nem jelenti az adat „elvitelét”.

Általában az adatok megrongálása sem eredményez külvilági elváltozást, kivéve, ha a számítógépet vagy adathordozót erőszakos hatás éri. Az adatok megrongálásáról beszélhetünk, ha azokat megváltoztatják.⁸⁵

A hatályos szöveg a következő:

Számítástechnikai rendszer és adatok elleni bűncselekmény

300/C. § (1) Aki számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad, vétséget követ el, és egy évig terjedő szabadságvesztéssel büntetendő.

(2) Aki

- a) *számítástechnikai rendszerben tárolt, feldolgozott, kezelt vagy továbbított adatot jogosulatlanul megváltoztat, töröl vagy hozzáférhetetlenné tesz,*

- b) *adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését jogosulatlanul akadályozza, vétséget követ el, és két évig terjedő szabadságvesztéssel büntetendő.*

(3) Aki jogtalan haszonszerzés végett

- a) *a számítástechnikai rendszerbe adatot bevisz, az abban tárolt, feldolgozott, kezelt vagy továbbított adatot megváltoztat, töröl vagy hozzáférhetetlenné tesz, vagy*

⁸⁵ Nagy, 2009, 63-64. o.

b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését akadályozza, és ezzel kárt okoz, büntetett követ el, és három évig terjedő szabadságvesztéssel büntetendő.

(4) A (3) bekezdésben meghatározott bűncselekmény büntetése

a) egy évtől öt évig terjedő szabadságvesztés, ha a bűncselekmény jelentős kárt okoz,

b) két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekmény különösen nagy kárt okoz,

c) öt évtől tíz évig terjedő szabadságvesztés, ha a bűncselekmény különösen jelentős kárt okoz.

A 300/F. § értelmező rendelkezést is fűz hozzá, miszerint:

A 300/C. és a 300/E. § alkalmazásában számítástechnikai rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy az egymással kapcsolatban lévő ilyen berendezések összessége.

A bűncselekmény tárgyi oldala

A jogi tárgy az elektronikus adatfeldolgozó- és adatátviteli rendszer integritása, biztonságos működése,⁸⁶ ezek rendeltetésszerű működéséhez, és a rendszerben tárolt, feldolgozott, illetve továbbított adatok megbízhatóságához, hitelességéhez fűződő érdek, valamint az, hogy ezeket az adatokat csak az arra feljogosítottak ismerhessék meg.⁸⁷ A (2) bekezdés a) pontjában az adatok tartalmától függően az azok által megtestesített érték, érdek. A (3) bekezdésben az elektronikus adatfeldolgozó és átviteli tevékenység mellett jogi tárgynak tekinthető a felhasználók vagyoni viszonya is.⁸⁸

Az elkövetési tárgy az elektronikus adatfeldolgozó- és adatátviteli rendszer, vagy annak valamely eleme (például egyetlen számítógép), valamint a (2)-(4) bekezdésben a számítógépes adat, amely elektronikus impulzus.⁸⁹

A Fővárosi Bíróság egyik ítéletében kiemelte, hogy a cselekmény megállapítása szempontjából maga a számítógép nem is bír jelentőséggel, hanem annak funkciója az

⁸⁶ Nagy, 2004, 165. o.

⁸⁷ Erdősy Emil – Földvári József – Tóth Mihály: *Magyar büntetőjog-Különös rész*, Budapest, Osiris Kiadó, 2004, 441. o.

⁸⁸ Gál István László: *Gazdasági büntetőjog közgazdászoknak*, Akadémiai Kiadó, Budapest, 2007, 212. o.

⁸⁹ Nagy, 2004, 165. o.

igazán meghatározó. Ennek iskolapéldája a taxióra, melyet az abba beszerelt saját kódolású szoftver működtet.⁹⁰

A tényállásban meghatározott elkövetési magatartások 2 formája kerül megemlíetésre:

1. *A jogosulatlan belépés*

2. *A rendszerben történő jogosulatlan bent maradás.*⁹¹

Az „**elektronikus betörés**” az adatállomány kezelésére szolgáló számítógépen keresztül, tehát közvetlenül, avagy a technika fejlődése folytán a számítógépes, és a telekommunikációs hálózatok integrációja révén a számítógépeket összekötő telefon vagy elektronikus adatátviteli vonalakon (*dataline*) keresztül, tehát közvetetten történhet.

A jogosulatlan belépés abban az esetben minősül büntetendőnek, ha az elektronikus adatfeldolgozó- és átviteli hálózat védett, azaz biztonsági eljárások, megoldások védik a jogosulatlan használatától. **Tipikusan ilyen a felhasználói név és a jelszó.**

A (3) bekezdésben szerepel a számítógépes csalás meghatározása.

Az elektronikus adatfeldolgozási folyamatot vagy annak eredményét befolyásoló megtévesztő magatartások számítógépes csalás elnevezéssel váltak ismertté. A számítógépes csalás struktúrája hasonló a tradicionális csalás tényállási szerkezetéhez:

- az elkövető oldalán jogtalan haszon elérése, mint cél,
- ennek érdekében megtévesztő magatartás és
- a sértett oldalán vagyoni kár előidézése.⁹²

A bűncselekmény alanyi oldala

A bűncselekmény alanya az első fordulat esetében a belépésre nem jogosult személy, míg a második fordulatban a belépésre jogosult személy lehet. ***A cselekménynek nincs speciális alanya, kívülállók és a rendszert használók általában egyaránt elkövethetik, egyes fordulatokat azonban mégis csak a körülhatárolható személyek követhetik el.*** Az (1) bekezdés első fordulatának a rendszerbe történő

⁹⁰ Erdősy – Földvári – Tóth, 2004, 442. o.

⁹¹ Ha a támadó a rendszer eredeti feltörése után is meg akarja tartani hozzáférését, akkor a későbbi belépésekhez **rejtekaajtót** (backdoor) helyez el. Ennek módszere, eszközei és technikája erősen rendszerfüggő, de az elérendő cél mindig az, hogy témaszámokat, időzített lefutó programokat, fertőzött indítóállományokat helyezzen el, bekapcsoljon különböző távoli elérést biztosító szolgáltatásokat, és a legitim alkalmazások és szolgáltatások egy részét trójaiakra cserélje. A lehetséges eszközök sokszínűek Lásd: Thomas, 2005, 45-46. o.

⁹² Gál, 2007, 214. o.

belépésre egyébként jogosult személy nem lehet a tettese. Az (1) bekezdés második fordulatát csak a rendszerbe belépésre jogosult követheti el. A (2)-(4) bekezdés eseteiben a bűncselekmény bárki által elkövethető.⁹³ Büntetéskiszabási szempont lehet, és súlyosító körülményként jöhet szóba, ha az elkövető hivatali, hivatásbeli kötelezettségét kihasználva követi el a bűncselekményt (pl. rendszergazda), vagy ha számítástechnikai képesítéssel bír, vagy számítástechnikai cég, szerviz dolgozója stb.

A hatályos magyar törvény szerint közömbös a szakismeret, a tudás szintje.

A bűncselekmény csak szándékosan valósítható meg. Az elkövetőnek tisztában kell lennie azzal, hogy a védett rendszerbe lép be jogosulatlanul vagy marad ott bent, és ezt a magatartást kívánatosnak tartja (*dolus directus*), vagy ebbe belenyugszik (*dolus eventualis*). A (3) bekezdésben meghatározott számítógépes csalás célzatos cselekmény, így csak egyenes szándékkal valósítható meg.⁹⁴

Kriminológiai tapasztalat, hogy a potenciális elkövetői kör zöme azokból kerül ki, akik a pénzmozgásokat rögzítő elektronikus adatfeldolgozás folyamatában – közvetlenül – részt vesznek (pl. operátorok, programozók), vagy ott könnyedén hozzáférhetnek a számítógépekhez.⁹⁵

A halmazati kérdések ma is vitákra adhatnak okot. Legfőbb kérdés, miként határoljuk el a vagyon elleni csalást a számítógépes csalástól. Korábban a számítógépes adatok manipulálásával elkövetett csalásokat konzekvensen a Btk. 318. §-a alapján minősítette. A 90-es évektől erősödtek fel azok a nézetek, amelyek szerint van egy elkövetéskor ki nem fejtett, jelen nem lévő magatartás és itt a sértett utólagos megtévesztéséről van szó, valamint a sértett nem fejt ki aktív magatartást a megtévesztés hatására, amely a károsodáshoz vezet.

A számítógépes csalásnál az elkövetéskor a károsult nem kerül kapcsolatba a tettel, a megtévesztés, mint elkövetési magatartás nem is közvetlenül személyt, hanem gépet érint és a számítógépes csalásnál a kárt szenvedett rendszerint csak a kár tényéből, utólag értesül a történetekről.

Manapság azonban, hasonlóan az okirat-hamisításokkal leplezett csalások esetén is töretlen a halmazatot megállapító gyakorlat, így annak sincs akadálya, hogy a vagyon elleni bűncselekmény mellett megállapítsuk a jogosulatlan belépést, adatbevitelt,

⁹³ Erdősy – Földvári – Tóth, 2004, 444. o.

⁹⁴ Gál, 2007, 215. o.

⁹⁵ Gál, 2007, 215. o.

adatváltoztatást vagy törlést, mivel ezek a magatartások önmagukban is büntetést érdemelhetnek.⁹⁶

A bűncselekmény stádiumai

Az első fordulat esetében a hálózatba, számítógépbe történő belépéssel a bűncselekmény befejezetté válik. Kísérletig abban az esetben jut el az elkövető, ha a védelmi megoldások kijátszását próbálgatja vagy a nyitott portokhoz kíván kapcsolódni.

A második fordulat esetében a belépés jogszerű volt, ám a jogosult nem lépett ki onnan. Ez tiszta mulasztásos alak, aminek nincs kísérlete.⁹⁷

Rendbeliség

A bűncselekmény rendbelisége a számítástechnikai rendszerek számához igazodik. A törvény valamennyi számítástechnikai rendszer önálló büntetőjogi védelmét biztosítja, függetlenül attól, hogy azok tulajdonosa, illetőleg üzemeltetője azonos vagy különböző természetes vagy jogi személy, illetőleg jogi személyiség nélküli szervezet.

Az egyes számítástechnikai rendszerek sérelmére megvalósított akár azonos, akár különböző elkövetési magatartások száma a rendbeliséget rendszerint nem érinti. A következetes ítélkezési gyakorlatnak megfelelően a természetes egység keretében nyerhet értékelést.⁹⁸

A cselekmény a gazdasági titok megsértésének bűncselekményével (300. §) valóságos alaki halmazatot alkot.⁹⁹

A másik ebbe a körbe vont tényállás a Btk.-ban a **számítástechnika rendszer védelmét biztosító technikai intézkedés kijátszása**. A 300/E. §-al a jogalkotó voltaképpen az elektronikus adatfeldolgozás- és átvitel veszélyeztetésének legkorábbi stádiumát rendeli büntetni, azzal, hogy pönalizálja a 300/C. §-ban szabályozott hacking előkészületét, illetve az ehhez nyújtott bűnszegélyt.

A bűncselekmény **célzatos**, mivel a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából követik el.

Néhány szóban ki kell térnünk a 2013. július 1.-jén hatályba lépő új Btk. (2012. évi C. törvény) szabályozására is. Először is új fejezetbe került. A hatályos Btk. XVII.

⁹⁶ Erdősy – Földvári – Tóth, 2004, 446. o.

⁹⁷ Nagy, 2004, 161-167. o.

⁹⁸ 33. pótlás-716/5 In: Magyar büntetőjog, Kommentár a gyakorlat számára, második kötet, Szerk.: Rabóczki Ede, HVG-ORAC Lap- és Könyvkiadó Kft.

⁹⁹ Gál, 2007, 215-218. o.

fejezetében szerepel a gazdasági bűncselekmények között, mely elhelyezéssel a szakma nem minden tekintetben értett egyet. Mivel a jogi tárgya nem a gazdálkodás rendje, hanem az információs rendszerek megfelelő működtetése és az abban foglalt adatok megőrzéséhez fűződő társadalmi érdek, ezért az önálló fejezetben való elhelyezés indokolt volt. Az új törvényben már önálló fejezetben kapott helyett, a XLII. fejezetben, mely a Tiltott adatszerzés és az információs rendszer elleni bűncselekmények címet viseli, és a hatályos szöveghez hasonlóan, két bűncselekmény törvényi tényállása vonatkozik az információs rendszerekre. Témánk szempontjából az első a jelentős.

Információs rendszer vagy adat megsértése

423. § (1) Aki

a) információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad,

b) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy

c) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,

vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés büntett miatt egy évtől öt évig terjedő szabadságvesztés, ha az (1) bekezdés b)-c) pontjában meghatározott bűncselekmény jelentős számú információs rendszert érint.

(3) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el.

(4) E § alkalmazásában adat: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.^{100 101}

A bűncselekmény jogi tárgyai az (1) bekezdésben a számítástechnikai rendszerek integritása, biztonsága. Az (1) bekezdés b) és c) pontjában e rendszerek biztonságos működése, c) pontjában az előzőek kiegészülnek az elektronikus adatok megbízhatóságához, hitelességéhez fűződő érdekekkel, valamint tartalmától függően az azok által megtestesített értékkel.

¹⁰⁰ http://www.complex.hu/kzldat/t1200100.htm/t1200100_34.htm [2012. 11.27]

¹⁰¹ A hatályos Btk. 300/C. §-át a törvény szétválasztja, és a jogtárgy védelem alapján annak (3)-(4) bekezdését külön tényállásként szabályozza a vagyoni elleni bűncselekmények körében. A hatályos Btk. 300/C. § (1) bekezdésében szereplő bűncselekmény tényállását érintően a törvény változtatást nem tartalmaz, de a szigorítás jegyében a büntetési tétel maximumát egy évről két évre emeli fel. A hatályos Btk. 300/C. § (2) bekezdése szerinti elkövetési magatartásokon a törvény érdemben nem változtat. Módosul a jogosulatlan akadályozás annyiban, hogy a törvény a technikai fejlődés gyors ütemére és eszközeinek változatosságára tekintettel nem határoz meg elkövetési módokat.

A bűncselekmény elkövetési tárgyai:

- akár egyetlen számítógép vagy számítástechnikai rendszer, ideértve a számítógépes hálózatot,
- elektronikus adat, amely elektronikus impulzus.¹⁰²

A tényállásban meghatározott **elkövetési magatartások**:

Az (1) bekezdés a) pontjában szabályozott esetben, a jogosulatlan belépés történhet egyetlen, más által jogszerűen birtokolt vagy használt számítógépbe, illetve egy számítógépen keresztül egy védett hálózatba. Közömbös, hogy a számítástechnikai hálózat belső hálózat (ún. extranet, pl. egy egyetemi hálózat) vagy az Internet részét képező védett hálózat (pl. egy biztosító hálózata), amely a weboldalon át érhető el. Mindkét esetben szükséges, hogy a hálózat biztonsági megoldásokkal védett legyen és ez a védelem aktív legyen, azaz szükséges legyen a belépéshez, jelszavak, kódok, egyéb azonosítók használata. *Mindkét elem szükséges feltétel.* Nem jogosulatlan a belépés, ha a számítógép, rendszer vagy hálózat nem védett, illetve a védelem nem aktivált (pl. nyilván elérhető WI-FI esetében).

aa) Az első fordulatban, az elkövető az aktív védelemmel ellátott számítógépbe vagy védett hálózatba jogosulatlanul lép be, akkor ha

- *a számítógép, vagy hálózat biztonsági rendszer hiányosságait kihasználva lép be jogosulatlanul, vagy*

- *a jogosult felhasználó nevével (belépési kódjával), jelszavával, vagy a belépést biztosító adat birtokában lép be.*

Közömbös a kódok, jelszók megszerzésének módja: megtévesztéssel, más csalárd módon, kifürkészéssel, a felhasználó hanyagsága folytán, kódtörő program segítségével, erőszakkal, fenyegetéssel vagy más módon.

ab) *A belépési jogosultsága kereteinek túllépésével, illetőleg annak megsértésével történő bennmaradás.*

Az elkövető saját felhasználó nevével, jelszavával, az engedélyezett belépési ponton lép be az információs rendszerbe, ám *a felhasználói jogosultságát meghaladó műveleteket kíván folytatni.*

¹⁰² A számítástechnikai rendszerek olyan számítógépekből, hozzájuk tartozó perifériákból állnak, amelyek valamilyen kommunikációs kapcsolaton keresztül közös erőforrásokat érhetnek el, azaz hálózatokat alkotnak. A kommunikációs kapcsolat megvalósulhat elektronikus, vagy optikai kábelben, rádióhullámok, műholdas sugárzás stb. útján.

Az (1) bekezdés b) pontjában szabályozott esetben az elkövető a számítástechnikai rendszerhez történő hozzáférést követően a rendszer működését akadályozza.

Az (1) bekezdés c) pontjában szabályozott esetben: az információs rendszerben lévő adat (elektromos impulzus) jogosulatlanul vagy jogosultsága kereteit túllépő változtatása, törlése, hozzáférhetetlenné tétele. Az elektronikus adat megváltoztatása egy gyűjtőfogalom, amely az adat tartalmának bármilyen módon történő módosítását jelenti. Ez felöleli az elektronikus adat felülírását, kiegészítésén túl annak részleges törlését is, hiszen ez utóbbi is az adat tartalmának módosítását jelenti.

Az elektronikus adatok hozzáférhetetlenné tétele: az adat elrejtése olyan fájlban, amelyet jelszóval véd az elkövető, ott tárolja, az adatállományt kódolja, vagy a hálózaton csak az általa ismert helyre másolja.

De idetartozhat az adathordozó elrejtése, fellelhetőségének eltitkolása, az adat kódolása, a fájl tartalmazó könyvtár jelszóval történő védetté tétele stb.

Lévén a számítógépes program is elektromos impulzusok meghatározott, logikai sorrendje, úgy azok megváltoztatása, törlése, stb. büntetni rendelt.

A tényállás megállapításakor a törvény figyelemmel volt az *információs rendszerek elleni támadásokról* és a 2005/222/IB tanácsi kerethatározat felváltásáról szóló irányelv-tervezet rendelkezéseire, ennek megfelelően kerültek meghatározásra a bűncselekmény minősített esetei. Minősített esetként szabályozza a törvény a cselekményt, ha az jelentős számú információs rendszert érint, illetve társadalomra kiemelt veszélyessége okán még súlyosabban minősülő esetként határozza meg, ha a cselekményt közérdekű üzem sérelmére követik el.

A bűncselekmény alanyi oldala: a bűncselekmény bárki által és szándékosan valósítható meg. Büntetékiszabási szempontok között súlyosítóként jöhet szóba az információs rendszer működéséért felelős személyek büntetni rendelt ténykedései.

Látható tehát, hogy a régi és az új szabályozás között számottevő különbség nincsen. Az új törvény némileg pontosít a szövegen, összhangba hozza azt nemzetközi standard-dal; az önálló fejezetben történő elhelyezéssel régóta adós volt a jogalkotás, ezzel a lépéssel talán megkezdhető a felzárkózás az informatikai bűncselekmények elleni harcban.

Informatikai bűnözés szomszédainknál

Az egyik eset „hőse” *Makszim Kovalcsuk* ukrán állampolgár, aki lopott szoftverekkel kereskedett az interneten. Ezt az önmagában még nem túl kiemelkedő ügyet „megfejlte” pénzmosással és hamis bankkártyákkal való visszaéléssel. A jól jövedelmező kereskedelemmel összesen 3 millió dollár kárt okozott egy nagy szoftvergyártónak. Bár ennek csak egy részét kapta kézhez, még így is nagyot szakított a 26 esztendőes fiatalember, akit Bangkokban egy kaliforniai bíróság kérésére tartóztattak le, és helyeztek kiadatási őrizetbe (azóta valószínűleg ítélet is született). A hírek szerint 20 évet és 500.000. dollár pénzbüntetést helyeztek kilátásba, amennyiben a pénzmosást is rá tudják bizonyítani.

A másik eset Romániában történt, ahol **Dan Dumitru Ciobanu** állt az iasi bíróság előtt a Blaster-F féreg megírásának és terjesztésének vádjával. Lebukása teljesen mezei nyomozati munkának köszönhető: a féreg törzsében egy román nyelvű üzenetet helyezett el, miszerint *"Ne menj a hidrotechnikai szakra!!! Csak az idődet pazarlod... Birsan, már vár a nyugdíj!!! Sz*rok a diplomára!!!!!!"*. Innentől kezdve a román hatóságnak nem volt nehéz dolga megtalálni. Az egyetemista 3-tól 15 évig terjedő szabadságvesztésre számíthatott.

Látható, hogy szomszédjaink nem tétlenkedtek. Valamiben tehát jobb lemaradni szomszédjainktól. Akár egy heccből megírt és a kibertérbe eresztett vírus miatt is megüthetjük a bokánkat. Bár ez idáig vírusírás miatt senkit nem ítélték el Magyarországon, de az Elender jelszóadatbázisát közzétevő hackereket nem jogerősen 2 év felfüggesztett börtönre ítélték.¹⁰³

¹⁰³ http://itcafe.hu/hir/informatikai_bunozes_a_szomszedainknal.html [2011. 11. 07.]

VI. FEJEZET: Összegzés-következtetés

„Mindig egy lépéssel a fejlesztők előtt.”

Mindenképpen be kell látnunk, hogy az ezredforduló óta kényelmetlen velejárója életünknek minden fent megemlített cselekmény, és ezek biztosra vehetően csak szaporodni fognak. Véleményem szerint terjedésüknek gátat vetni már nem lehet, csupán lassítani. Napjainkra már túlságosan is rabjaivá váltunk a modern eszközöknek, a képzeletbeli ló gyeplőjénél azonban a bűnözők ülnek.

A kiberbűnözés veszélyével alaposan megváltozott a szoftverek iránti igény is, korábban az a volt az elsőrendű cél, hogy mennyi funkcióra alkalmas.

Ellene a hatékony védekezés mindenképpen biztonságtechnikai szakemberek feladata és bár totális védelem nem létezik, minden létező eszközzel arra kell törekedni, hogy a jogosulatlan belépések se anyagilag, se pedig időben ne ériék meg.

Szomorú tényként kell megállapítani azt is, hogy - bár az Internet és az e-mail forgalom biztonságát garantáló programok fejlesztői sem ülnek babérjaikon, hiszen egyre gyorsabban ismerik fel az új vírusokat, kémprogramokat, így a felhasználók egy-egy káros alkalmazás felbukkanása után akár egy órán belül is védelmet kaphatnak – az előny sajnos mégis a bűnözőknél van, hiszen tevékenységük nem ismert határokat, nincsenek játékszabályaik, minden eszközzel támadnak, amire csak gondolni lehet vagy oly módon, melyre álmunkban sem gondolnánk.

Éppen erre a felkészült védekezésre való válaszként a támadók nem nyílt támadással gyűjtenek adatot, hanem valódinak tűnő e-mailek, honlapok mögé rejtőzve, kémprogramok segítségével nyitnak hátsó kikaput legféltettebb adatainkhoz, titkainkhoz.¹⁰⁴

S ami a leginkább szembetűnő: szinte minden nagyobb támadás pontosan időzített, tökéletesen alkalmazkodva az üzleti és a fogyasztói élet szokásaihoz.¹⁰⁵

¹⁰⁴ Így például a YouTube-on is számtalan olyan videó tekinthető meg, amely lejátszása alatt egyúttal jelszólopó, billentyűzetfigyelő szoftver települ gépünkre.

¹⁰⁵ A 2007-es amerikai Superbowl döntője előtt az eseménynek otthont adó Dolphin Stadion honlapját fertőzték meg, s az idelátogató szörfözők gépére titokban kémprogramok települtek. A Cyber hétfőn, vagyis a hálaadást követő hétfője után – amely hagyományosan a legnagyobb kiskereskedelmi forgalmat generáló nap az évben – a Sunbelt Software képviselői 40.000 olyan hamis oldalt találtak, amelyek álkulcsszavak segítségével a Google keresési eredményei közt az élre kerültek.

Az elmúlt évek legnagyobb újdonsága a változatos csatlományformátumok mellett kétség kívül az volt. hogy a legjobban szervezett spamtámadások során a felhasználók teljes neve és pontos e-mail címe jelent meg. A spammerek a *MySpace*, a *Facebook* és egyéb közösségi portálokra gyűjtötték össze az elérhetőségeket, nem kell külön hangsúlyozni, hogy ezekkel miként lehet visszaélni.

Kétségtelen, hogy az emberek többsége általában véve megbízik az adott oldalakban és talán pont ez a bizalom szolgáltatja azt a masszív alapot, amelyre a visszaélések, elektronikus betörések épülnek.

Ahogy arra az elején is utaltam, a számítógépes bűnözés elleni fellépés nem lehet pusztán jogi fellépés. Ami a védelem technikai oldalát illeti, egy pillanatra sem szabad levonnunk a szemünket a számítógépes bűnözőkről, mert ha csak kicsit is nagyobb teret kapnak, akkor teljesen felforgatják mindennapjainkat. Azonban egyből szembesülünk azzal a problémával, hogy meddig terjedjen a védelem? Hiszen ha túlságosan törekszünk a teljes körű védelemre (ahogy erre a botrányos Samsung laptop ügyben hivatkoztam), lehet, hogy fel kell adnunk személyes szabadságunkat, és a ló túlsó oldalára átesve, könnyen egy „orwelli rémálomban” találhatjuk magunkat.

Mivel nem lehet pusztán jogi a fellépés és mikor éppen az örök macska-egér párharcban a rabló mégis megelőzi a pandúrt, akkor a nagy szoftverüzemeltetők feladata az, hogy a nyílt veszélyeztetettség időszakát a lehető legrövidebbre csökkentsék, a javítókódokat mielőbb a felhasználók kezébe juttassák.

Az Európai Unió az utóbbi időben ismét elővette a témát. Elsősorban a megnövekedett támadások miatt vált ismét kellemetlenné a terrorizmus jelenléte, s azon belül a kibertámadásoké. Az Európai Bizottság fokozni kívánja az Európai Unió terrorizmusellenes fellépését. Egyre fontosabb a kritikusnak minősített infrastruktúrák megvédése. Eközben az EU a Kutatás-fejlesztési Keretprogramból 40 millió eurót szán kutatásra.

Talán hazánkban is felfigyel végre a jogalkotás és jogalkalmazás a veszély valódiságára, hiszen elegendő csak a szomszédos országokra tekinteni. Bár nem lehet elkiabálni, hazánk kiberterrorizmus fenyegetettsége talán ugyanolyan alacsony, mint hagyományos terrorfenyegetettsége. Azonban akkor sem ülhet tovább a babérjain a jogalkotás, hiszen látványosan hanyagolja a témát, és hiába ússzuk meg ezerszer, ha csak egyszer is valaki sikerrel jár annak beláthatatlan következményei lehetnek. Idézzük csak fel a fent említett támadásokat... már a számítástechnika hajnalán is micsoda

felfordulást okoztak. Mostanra pedig, amikor szó szerint **mindent** számítógépek vezérelnek, egy-egy sikeres támadás akár észrevétlen is maradhat.

Már egy ideje erősödnek azok a hangok, melyek a reflektorfényt a számítógépes bűnözésre irányítanak. Nyilvánvaló, hogy a jelenlegi szabályozás nem fedi le maradéktalanul e bűncselekmények változatos, és egyre bővülő körét.

És addig se felejtsük a másik örökérvényű megállapítást sem, miszerint:

A biztonság leggyengébb láncszeme mindig az ember!

Adatainkkal mindig bánjunk elővigyázatosan, jelszavainkat amilyen gyakran csak lehet, változtassuk meg és ne hagyjunk önszántunkból olyan információkat magunk után, melyek segítségével még könnyebben kifürkészhetővé válunk (gondolok itt a cetlikre, monitorokra felfirkantott jelszavakra, belépési útmutatókra, kódokra). Sok laikus nem érzékeli, hogy mennyire könnyen ellophatják adatait és nincs rá garancia, hogy egyáltalán valaha rájön.

IRODALOMJEGYZÉK:

- Bequai, August: Computer-Related-Crime, ECC, Strasbourg, 1990
- Bryant, Robin: Investigating digital crime, John Wiley & Sons Ltd., Chichester, 2008
- Erdősy Emil – Földvári József – Tóth Mihály: Magyar büntetőjog: Különös rész, Budapest, Osiris Kiadó, 2004
- Ferwagner Péter Ákos – Komár Krisztián – Szélinger Balázs: Terrorista szervezetek lexikona. Szeged, Maxim Könyvkiadó, 2003
- Gál István László: Gazdasági büntetőjog közgazdászoknak, Budapest, Akadémiai Kiadó, 2007
- Horváth Tibor-Kereszty Béla-Maráz Vilmosné-Nagy Ferenc-Vida Mihály: A magyar büntetőjog különös része, Budapest, Korona Kiadó, 1999
- Kurbalija, Jovan: An Introduction to Internet governance, Budapest, Akaprint Nyomdaipari Kft., 2010
- Mitnick, Kevin D. – Simon, William L.: A legendás hacker. Ford.: Lénárt Szabolcs, Budapest, Perfact-Pro Kft., 2003
- Molnár Gábor: Gazdasági bűncselekmények, Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2009
- Moore, Robert: Cybercrime – Investigating High-Technology Computer Crime, Anderson Publishing, Oxford, 2011
- Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Budapest, Ad Librum, 2009
- Nagy Zoltán András: A jogosulatlan belépés a számítógépes rendszerekbe (hacking) megítéléséről. In Korinek László - Kőhalmi László – Herke Csongor (szerk.) Emlékkönyv Irk Albert egyetemi tanár születésének 120. évfordulójára, Pécs, 2004
- Thomas, Tom: Hálózati biztonság. Ford.: Ketler Iván, Budapest, Panem Könyvkiadó, 2005
- Wark, McKenzie: Hackerkiáltvány. Ford.: Nagy Mónika Zsuzsanna, Budapest, Noran Libro Kiadó, 2010
- Warren, Peter – Streeter, Michael: Az internet sötét oldala. Budapest, HVG Kiadó Rt., 2005