10.17625/NKE.2019.006

NEMZETI KÖZSZOLGÁLATI EGYETEM

Doktori (PhD) értekezés

Papp Zoltán István
2018.

NEMZETI KÖZSZOLGÁLATI EGYETEM

Katonai Műszaki Doktori Iskola

PAPP ZOLTÁN ISTVÁN

A KIBERTERRORIZMUS MÓDSZEREI, LEHETSÉGES ESZKÖZEI ÉS AZ EZEK ELLEN TÖRTÉNŐ VÉDEKEZÉS ALTERNATÍVÁI

doktori (PhD) értekezés

Témavezető:

Prof. Dr. Kovács László mk. ezredes Ph.D.

Budapest, 2018.

Tartalomjegyzék

Bevezetés

Az információs jelzővel illetett társadalmunkban élő emberek egyre nagyobb mértékben használják a rohamosan fejlődő technika és a megjelenő új technológiák által megteremtett lehetőségeket, illetve mindennapjaikban – anélkül hogy ez a szélesebb társadalmi rétegekben tudatosulna – támaszkodnak is rájuk napi tevékenységük, ügyintézéseik során, mind magánéletükben, mind munkahelyükön, mind pedig szűkebb-tágabb környezetükben, mivel ezek a megoldások napi életüket kényelmesebbé, munkájukat hatékonyabbá és gyorsabbá is teszik. Ezt a jelenséget tekinthetjük az emberi együttélés új módjának, mivel az információ a társadalom életében, folyamataiban központi szerepet tölt be, és az információnak az előállításához, feldolgozásához, tárolásához és megosztásához külön, de összekapcsolódó infrastruktúrákat rendelnek, melyek a társadalom minden entitása (egyének és különböző szervezeteik, szerveződéseik) számára elérhetőek.

Az információs társadalom fejlődésének fontos állomása volt az, amikor az eltérő rendeltetésű, különböző kiterjedtségű információs rendszerek összekapcsolása oly mértéket öltött, hogy már globális rendszerekké váltak. Ennek következtében a globális rendszerekhez kapcsolódó entitásokhoz az érdeklődésükre számot tartó információk gyakorlatilag azonnal eljutnak, és ez megváltoztatta a társadalom tagjainak a térhez és az időhöz való viszonyát, mivel így egy, de akár több virtuális, saját szociológiai törvényszerűségekkel bíró, párhuzamosan működő társadalom polgárai is lehetnek.

Ugyanakkor ez a fejlődés a valós társadalom szociológiai jellemzőiben negatív változásokat is indukál, mely mögött jelentős részben a gazdaság átalakulása húzódik meg, mivel a társadalmi munkamegosztás is változik. Az ipari szektorban foglalkoztatottak aránya folyamatosan csökken, ugyanakkor a szolgáltatási szektor információkezeléssel foglalkozó munkavállalóinak száma dinamikusan nő, így a társadalom egyre nagyobb hányada lesz jelen, lesz érintett valamilyen módon a globális rendszerek által alkotott kibertérben. Ez a hatás nem csak a szervezeteket, szerveződéseket, hanem az egyéneket is érinti: például a politikai szervezetek stratégiákat dolgoznak ki a választókat foglalkoztató témák és a politikai üzenetek átadásának leghatékonyabb módjának azonosítása, valamint az üzenetek által kiváltott hatások felmérése érdekében. A gazdasági szereplők információs rendszerei pedig a tervezési, termelésirányítási, értékesítési folyamatok hatékonyságát növelik a nyersanyag-, az energiafelhasználás, a marketing költségek optimalizálása vagy az üzletkötés és a pénzügyi tranzakciók gyorsítása által. Ez a fejlődés a kormányzati (közigazgatás, rendészet,

honvédelem, stb.) és a non-profit szektorban (egészségügy, oktatás, kultúra, stb.) működő szervezetek számára is új távlatokat nyit meg, mivel a szervezetek egymás között, illetve az állampolgárok irányába gyors, biztonságos kapcsolat és információcsere lehetőségét is 0biztosítja. A társadalom tagjai pedig önkifejezési módjaikhoz, interperszonális kapcsolataikhoz számos új, téren, időn átívelő kommunikációs lehetőségeket és eszközöket kapnak.

Tehát e fejlődésnek a révén megvalósulhatott az, hogy a politikai, gazdasági és társadalmi folyamatok egyre nagyobb arányú átterelődése a kibertérbe elérte azt a kritikus mértéket, amikor a kibertér már megkerülhetetlen tényező lett. Ennek következtében bizonyos rendszerek olyan fontos szerepet töltenek be a társadalom életében, hogy létük, illetve működésük létfontosságú. E létfontosságú rendszerek alkalmazásával a társadalom környezetéről nyernek folyamatosan információkat, melyeket feldolgoznak (rendszereznek, elemeznek, tárolnak) és szolgáltatnak. Más struktúrák rendeltetése a társadalom entitásainak életét segítő, óvó, összehangoló folyamatok irányítása, szabályozása. Ezek működésének alapja – az őket alkotó technikai eszközök üzembiztonságán és a működtető személyzet felkészültségén túl – maga a pontos információ, melynek megléte, illetve rendelkezésre állása elengedhetetlenül szükséges ahhoz, hogy a rendszerek a rendeltetésüket az elvárásoknak megfelelően töltsék be. Ennek következtében az információhoz kapcsolódó szolgáltatások bárminemű okból történő kiesése jelentős zavarokat idéz elő a társadalom működésében, konkrétan meg is fogalmazható, akár számszerűen is leírható egyéni, társadalmi, gazdasági, katonai és nemzetbiztonsági érdekeket veszélyeztethetnek, melyből kifolyólag ezeknek a rendszereknek védelme kiemelt feladata minden országnak, rendvédelmi, katonai, költségvetési és gazdasági szervezetnek.

Az információs infrastruktúrákra és rendszerekre, illetve az ezekben kezelt információkra épülő, egyre dinamikusabban virtualizálódó társadalom entitásaira számos veszély leselkedik, mivel a kibertér felértékelődésével összhangban itt is megjelentek a társadalomra veszélyes jelenségek, úgymint a bűnözés, a terrorizmus, a rémhírterjesztés, a politikai és gazdasági kémkedés, a személyes adatok elleni visszaélések.

Az információs rendszerek által kezelt adatok megszerzése, manipulálása, illetve a rendszerek üzemzavarainak előidézése mögött számos jogszerű, illetve jogszerűtlen motiváció húzódhat meg. Előbbi esetében például a saját reguláris fegyveres, rendészeti erők, vagy hírszerző szolgálatok tevékenysége értendő, addig utóbbi esetében minden más tevékenység e körbe sorolható, melyek közül megítélésem szerint a kiberterrorizmus emelhető ki legveszélyesebb

jelenségként, mivel – a „hagyományos" terrorizmussal összhangban – ennek repertoárjában jelenik meg a legtöbb eszköz és módszer, továbbá a kibertér által nyújtott lehetőségek a kiberterroristákat a jogellenes cselekményeikben a földrajzi tértől függetleníti és nagyfokú anonimitást is képes számukra biztosítani. Mindezek mellett a kibertér – sajátosságaiból adódóan – segíti azt, hogy bárki – megfelelő elköteleződés és bizonyos feltételek mellett – kiberterroristává válhasson.
A kiberterroristák anyagi haszonszerzés végett támadhatják a gazdasági folyamatokat irányító (banki, ipari) rendszereket, zavar- és félelemkeltés érdekében rombolhatják a kommunikációs, közlekedési, kommunális hálózatokat, rendészeti műveletek idején a felvonultatott rendvédelmi erők kommunikációját akadályozhatják, tevékenységük hatékonyságát ronthatják, vagy csak épp információszerzésre, propaganda-terjesztő és támogató jellegű tevékenységre használják fel az információs infrastruktúrákat. A kiberterrorizmus felismerését nehezíti, hogy a kibertérben jogellenes célból alkalmazott eszközök és módszerek szinte azonosak, motivációtól függetlenek, tehát egy terrorcselekmény bekövetkeztéig a jogi tényállás nehezen állítható fel.

A kibertérben megszerezhető információkon túl számos logikai és fizikai hatáson alapuló eszköz áll rendelkezésükre, melyekkel cselekményeiket megvalósíthatják, mivel ezek megvásárlása, megalkotása, összeszerelése a hétköznapi emberek számára is elérhető, és ez a körülmény fokozott kockázatként jelenik meg az információs infrastruktúrák üzemeltetőinek, illetve a rendvédelmi erők oldalán.

Az információs társadalom entitásainak életében az információs infrastruktúrák hangsúlyos szerepet töltenek be, így védelmük is kiemelt szerepet kell, hogy kapjon. E tevékenységben mind az üzemeltetőkre, esetleg mind a felhasználókra, illetve magára az államra is jelentős szerep hárul. A különböző szerepkörökben végzendő tevékenységek meghatározásához azonban a saját képességek megismerése, a működési környezet mélyreható ismerete, a fenyegetések azonosítása, illetve mindezek folyamatos monitorozása elengedhetetlen, és amennyiben a különböző szerepkörök felismerik az együttműködés lehetséges kereteit, úgy a védelmi, megelőző tevékenység hatásfoka növelhető. Így a kiberterrorizmus esetében azonosítani kell, hogy milyen módszerek vannak, kik lehet az elkövetők, milyen infrastruktúrák ellen, milyen jellemzők ellen, milyen eszközök jelenthetnek veszélyt, a védekezést, a hatékony beavatkozás lehetőségét milyen módszerek akadályozhatják.

Tudományos probléma megfogalmazása

Az információs társadalom magas szintű működésében az információs infrastruktúrákra kiemelt szerep hárul, és e fontosságból adódóan változatos módszerekkel végrehajtott rosszindulatú és ártó tevékenység fókuszába is kerülnek, melyek mögött különböző támadók sokszínű motivációi húzódnak meg.

A különböző célok elérése érdekében, különböző indokokra hivatkozva támadhatják őket kifejezetten e célra létrehozott – adott ország szövetségi rendszerén kívüli – állami szervek, szervezetek (katonai alakulatok, hírszerző szolgálatok), melyek tevékenységüket professzionális céleszközökkel valósítják meg. E körbe tartozó támadó jellegű tevékenységek hatásfokát nagyban növeli az a körülmény, hogy az állami szerveknek a céleszközök beszerzésére, tervezésére, fejlesztésére gyakorlatilag korlátlan humán- és anyagi erőforrások állnak rendelkezésükre, sok esetben műszaki, technológiai és személyi háttéradatbázisokkal is rendelkeznek. További hatásfokot növelő tényező, hogy az állam olyan jogszabályi és alkalmazási környezetet tud teremteni, melyek ez irányú tevékenységüket támogatják.

Azonban fenyegetések nem csak ellenérdekelt országok szervezeteinek irányából érkezhetnek, mert az információs infrastruktúrát személyek, irreguláris szervezetek, vagy kibertérben működő terrorcsoportok is megközelíthetik rosszindulatúan, jogellenes módon azzal a szándékkal, hogy annak szolgáltatásait akadályozzák, az abban tárolt információkat megszerezzék, megsemmisítsék, manipulálják.

A támadótevékenységet, azon túl, hogy a jogszabályi környezet büntetni rendeli, az is nehezíti, hogy a potenciális elkövetők számára a megfelelő professzionális céleszközök legtöbb esetben haditechnikai eszközöknek minősülnek, így beszerzésük – a nagy anyagi ráfordításon túl – gyakorlatilag meg sem valósítható. Ugyanakkor az elkövetőknek motiváltságuk mélységétől függően jogi és erkölcsi aggályai is egyre kevésbe vannak, így nem veszik figyelembe a jogszabályok tiltásait, tettük büntetőjogi következményeivel érdemben nem számolnak, így az információs infrastruktúrák elleni jogellenes cselekményt a birtokukba lévő információkkal, a rendelkezésükre álló eszközökkel – céljaik elérése érdekében – mindenképpen végrehajtják.

A potenciális elkövetőket számos körülmény segíti, hiszen az információs társadalom által használt információs rendszerekben – kisebb-nagyobb mértékű idő- és pénz ráfordításával – elérhető információtömeg, szolgáltatás és egyéb más lehetőség mind-mind felhasználható. Egyrészt az információs infrastruktúrákat nem csak a bennük tárolt információk tartalma által támadhatók, hanem más egyéb jellemző, paraméter által is, másrészt pedig érdemi és hasznos

információkat szerezhetnek meg az érintett infrastruktúráról, a beépített berendezésekről, az alkalmazott technológiákról az ott foglalkoztatott személyekről. Az előzőeken túl megnyerhetnek ügyüknek szimpatizánsokat, megteremthetik anyagi lehetőségeiket is, de megszerezhetik azokat az ismereteket is, elsajátíthatják azokat a módszereket, melyek egy sikeres támadáshoz elengedhetetlenek.

A jogellenes cselekményeket továbbá az is segíti, hogy számos olyan fizikai hatáson alapuló és logikai eszköz és módszer áll rendelkezésre, melyek birtokában az információs infrastruktúrák működésébe bele lehet avatkozni. A fizikai hatáson alapuló eszközök egy részének kereskedelme, birtoklása jogszabályokba ütközik, ám számos közülük kereskedelmi forgalomban elérhető alkatrészekből megalkotható, vagy épp kereskedelmi forgalomban kapható más berendezések átalakítása révén kiváltható.
A logikai eszközök (támadókódok) tekintetében, a fizikai hatáson alapuló eszközökhöz képest az információs infrastruktúra támadói könnyebb helyzetben vannak. A végrehajtás eszköze, a számítógép mindenki számára elérhető, e kategóriába tartozó logikai eszközök létezése a fizikai térben nem érzékelhető, birtoklásuk gyakorlatilag ellenőrizhetetlen, ugyanakkor megalkotásukhoz mélyreható szakismeretre van szükség, azonban alkalmazásukra már közel sem. Számos program már „alkalmazásra kész" formában elérhető, és már csak a célpont meghatározására van szükség, de a különböző toolkit-ekből összeállítható támadókódok és egyéb elérhető, megvásárolható sérülékenységek is komoly fenyegetést jelenthetnek az információs infrastruktúrákra.

Tekintettel az információs infrastruktúráknak az információs társadalomban betöltött szerepére, folyamatosan biztosítani kell az információk megszerzését, áramlását és felhasználását, illetve e műveleteket végző rendszerek, berendezések és átviteli csatornák folyamatos rendelkezésre állását, valamint ezek háttérfeltételeit. Azonban a folyamatosságra, az üzembiztonságra, illetve az általánosságban értendő biztonságra számos – az üzemeltetők által befolyásolható, vagy épp nem befolyásolható – körülmény van kihatással.
Az információs infrastruktúrák védelmét nehezíti az, hogy számos olyan körülmény létezik, melyről konkrét megjelenéséig vagy nem is tudnak, vagy bekövetkeztével érdemben nem számolnak, vagy épp az infrastruktúra megalkotásakor még nem is létezett. Ezért a védelmi intézkedések kidolgozásakor, a védelmi alrendszerek tervezésekor a lehető legmesszebbmenőkig előrelátva a biztonsági szakterületek mindegyikének vonatkozásában

meg kell jósolni a várható veszélyeket, fenyegetéseket, melynek elengedhetetlen feltétele a jelenlegi állapotok ismerete, a várható tendenciák helyes prognosztizálása.

A biztonság fenntartása mind a fizikai, mind pedig a kibertérben kihívást jelent. A biztonságot befolyásoló körülmények rendkívül összetettek. Lehetnek belső és külső körülmények, melyeknek állapota kihatással van az információs infrastruktúra biztonsági helyzetére, de lehet egy, a külső és belső körülmények együtthatásának eredője is olyan jelenség, mely negatívan hat ki a biztonságra.

Azonban az infrastruktúrák biztonságos működése nem csak az üzemeltetők érdeke, hanem az információs társadalom tagjait képviselő államé is, így e területen az illetékes szervekre, szervezetekre és hatóságokra is feladat hárul. A védelem területén az érintettek már együttműködnek, együttműködni kényszerülnek, azonban a felek eltérő érdekei, lehetőségei – illetve azok hiánya miatt – nem az ideális állapot gyors kialakulásának irányába hatnak.

Fentiek tükrében a tudomány eszközire van szükség annak érdekében, hogy megvizsgáljuk a fenti tényezők együttes összefüggéseit, kölcsönhatásait. **Tudományos kutatást igényel az, hogy az információs társadalom tagjai milyen feltételek, hatások mellett léphetnek a kiberterrorizmus útjára, ekkor az információs infrastruktúrákban kezelt információ mely tulajdonságait, milyen módszerekkel és eszközökkel támadhatják, valamint azt is vizsgálni kell, hogy az infrastruktúra üzemeltetőinek, illetve az államnak milyen lehetőségei, új módszerei lehetnek a védekezésben, továbbá vannak-e olyan egyéb körülmények, melyek a biztonság ellen hatnak.**

Hipotézisek

Az információs infrastruktúrákban kezelt, általánosságban értelmezett információnak, vagy ezen információnak a feldolgozásához kapcsolódó, ideiglenesen létező egyéb információknak a tartalmán túl vannak olyan egyéb minőségi jellemzői, tulajdonságai, melyek manipulálása révén a kiberterrorizmus akadályozni tudja az infrastruktúrák rendeltetésszerű működését, a bennük zajló információs folyamatokat.

Az információs társadalom tagjait érő és őket befolyásoló szociológiai hatások, valamint a számukra a kibertérben elérhető lehetőségek, rendelkezésükre álló eszközök, megszerezhető információk megkönnyítik azt, hogy egy személy – az őt ért hatások megfelelő konstellációjában – kiberterroristává váljon. Ugyanakkor ezek a szociológiai hatások nagy valószínűséggel azt is predesztinálják, hogy az érintett személy, milyen infrastruktúrák ellen, milyen célzattal és milyen módszerrel hajt végre támadást.

A komplex információbiztonság sémájához kapcsolódóan – az üzemeltetők és az állami szervek részéről – be lehet vezetni olyan új szempontokat, munkafolyamatokat, melyek növelik az információs infrastruktúrák biztonság szintjét.

Az információs infrastruktúrák üzemeltetéséhez és védelméhez kapcsolódó jellemzők tanulmányozása révén fel lehet tárni olyan összefüggéseket és kockázatokat a saját belső folyamatokban, illetve más kapcsolódó infrastruktúrák vonatkozásában, melyek kihatással lehetnek a biztonsági helyzetre. E tényezők aktuális állapotának, illetve esetleges változásainak folyamatos nyomon követése mindenképpen szükséges annak érdekében, hogy a biztonsági helyzetben negatív változás ne álljon be.

Célkitűzések

Az információ azon jellemzőinek feltárása, melyek manipulálása révén a kiberterrorizmus elérheti az információs infrastruktúrák működésének, illetve a felhasználók tevékenységének zavarát.

A potenciális elkövetők vonatkozásában annak meghatározása, hogy a kibertérben végrehajtott jogellenes cselekmények, kibertámadások esetében az elköteleződés, a „végrehajtani akarás" mértéke elkövetőnkként miként változhat, milyen összefüggésben lehet az érintett személyek – általános, vagy éppen megélt – szociális folyamataival, hátterével.

Annak eldöntése, hogy a szociális folyamatok, hátterek vizsgálata indokolt-e abban az esetben, amikor egy adott személyi kör, társadalmi réteg jelentette veszélyt, támadási potenciálját kell felmérni, illetve a szociális alapú vizsgálat indirekt módon is használható-e, tehát egy adott funkciót betöltő információs infrastruktúra esetében felmérhető-e az, hogy milyen szociális háttérrel rendelkező személy kör – például képzettségük, szélsőséges politikai nézeteik és/vagy anyagi helyzetük okán – jelenti rájuk a legnagyobb veszélyt.

A kiberterrorizmus keretei között értelmezett tevékenységek, különböző módszerek csoportosítása, valamint a kiberterroristák által felhasználható fizikai hatáson alapuló és logikai eszközök osztályozása.

Az állam és az üzemeltetők részéről a megelőzés és fenyegetések felderítése terén végrehajtandó intézkedések meghatározása, illetve a potenciális együttműködési felületek azonosítása, és annak feltárása, hogy melyek a szorosabb együttműködés, a folyamatosság, a biztonság és a védelem ellen ható tényezők.

Olyan metódusok kidolgozása, melyek mind az üzemeltetői, mind pedig az állami oldal részéről elősegítik a védelmi intézkedések hatékonyságának növekedését, vagy a kockázatok csökkentését.

Kutatási módszerek

A választott témakör ismeretanyagának előzetes áttekintése során már felismerhető volt, hogy a kiberterrorizmus, illetve az ellene történő védekezés különböző aspektusainak felméréséhez több kutatási módszer kombinatív alkalmazására lesz szükség.

A kutatómunka során a nemzetközi és hazai szakirodalmat, illetve joganyagokat, továbbá a mérvadónak tekinthető média publikációit elektronikus és írott formában tanulmányoztam, mely a látókör bővítése, más forrásból származó információk visszaigazolása tekintetében, valamint az esettanulmányok szempontjából kiemelt jelentőséggel bírt.

A tudományos konferenciákon és szakmai összejöveteleken (workshop, fókuszcsoportos beszélgetés) szakértők részéről elhangzott információkat összegyűjtöttem, ami folyamatosan orientálta a kutatási tevékenységem irányát.

A munkavégzésem során a kiberterrorizmus vonatkozásában birtokomba került információkat elemeztem, értékeltem, a megszerzett tapasztalatokra, következtetésekre tudományos választ kerestem.

A munkavégzés során a hazai társszervekkel, illetve a külföldi partnerszolgálatokkal történt együttműködés során felmerült információkat és tapasztalatokat – a szakirodalomban lévő állítások, következtetések összevetésével, megállapításaim megerősítése, illetve megcáfolása érdekében – elemeztem.

A munkavégzésem során strukturált interjúkat készítettem információs infrastruktúrák üzemeltetésének különböző szakterületein foglalkozatott, különböző vezetői szintekhez tartozó személyekkel, akiknek tapasztalatait, információt elemeztem, értékeltem és felhasználtam a kutatómunka során. A munkavégzéshez kapcsolódóan interjúkat készítettem olyan személyekkel is, akik a kibertérben végrehajtott különböző bűncselekményekben voltak érintettek, mely információkat, tapasztalatok felhasználásra kerültek a kutatómunka során.

A fent bemutatott kutatási módszerekkel nyert információk szintetizálásával és értékelésével fogalmaztam meg részkövetkeztetéseimet, amelyek elvezettek a tudományos probléma megválaszolásáig.

I. Az információ és az információs társadalom

I. 1. Az információs társadalom

A kiberterrorizmus vizsgálatának megkezdése előtt szükséges megvizsgálni az információs társadalmat, azt a társadalmi közeget, környezetet, amiben a terrorizmusnak e formája megjelenik és értelmezhető. Az információs társadalom definiálása tudományáganként eltér, tükrözve az adott tudományág sajátosságait, azonban ezek között analitikailag ötféle megközelítést lehet megkülönböztetni, amelyek mindegyike kritériumokat tartalmaz annak azonosítására, hogy mi is az új ebben a társadalmi formában. Ezek a következő típusokba sorolhatók: technológiai, gazdasági, foglalkoztatási, térszemléletű és kulturális meghatározások. [1]

Az információs társadalom megfogalmazására használt leggyakoribb definíciók a látványos technológiai innovációra helyezik a hangsúlyt. A vezérgondolat szerint az információ feldolgozása, tárolása, továbbítása és megjelenítése terén történt fejlődések a társadalom gyakorlatilag valamennyi területén az információs technológiák széles körű elterjedéséhez vezettek. Ezt a számítógépek árának dinamikus csökkenése, illetve teljesítményük exponenciális növekedése segítette elő, mivel ez lehetővé tette széleskörű alkalmazásukat a hétköznapi eszközökben. A technológiai innováció pedig olyan nagyságrendű társadalmi változásokat indukált, mely révén új korszakba lépett az emberiség.

A gazdasági megközelítések alapvetően a közgazdaságtan egyik ágazatára, az információ gazdaságtanára helyezik a hangsúlyt. A tudományág megalapítója, Fritz Machlup öt fő csoportra osztotta fel az információs ágazatot:

- oktatás (egyetemek, főiskolák, könyvtárak, egyéb tudásközpontok, stb.),
- kommunikációs médiumok (műsorszórás, stb.),
- információs gépek (számítógépes berendezések, hálózatok, stb.),
- információs szolgáltatások (kereskedelmi, pénzügyi szektor, stb.),
- más információs tevékenységek (kutatás-fejlesztés, non-profit tevékenységek). [2]

Machlup a különböző kategóriákhoz gazdasági értékeket rendelt, melyek révén lehetőség nyílt annak nyomon követésére, hogy az éves nemzeti össztermékhez (GDP) az egyes kategóriák milyen mértékben járulnak hozzá. A kategóriák értékeinek változásából (növekedéséből), a

GDP-ben mutatott arányaikból pedig következtetéseket lehet levonni az információs társadalom fejlődésére, fejlettségére.

A foglalkoztatási meghatározások a gazdasági meghatározásokkal az elvek szintjén nagyfokú egyezést mutatnak, csak itt az információs ágazatokban foglalkoztatott munkavállalók számának változását elemzik.

A térszemléletű meghatározások szintén a közgazdaságtanra, illetve a szociológiára építenek, de ezeknek a centrumában a fizikai tér áll. A különböző helyszíneket az információs hálózatok kötik össze, így a társadalom tagjainak életére – tér és idő érzékelésére – fejtenek ki hatást. A térszemléletű definíciók közül kiemelhető John Goddard elgondolása, miszerint az információs társadalom fejlődésében négy, egymással összefüggő elem jelenik meg markánsan: [3]

- Az információ stratégiai erőforrásként központi helyet foglal el a társadalomban.
- Informatikai rendszerek és kommunikációs technológiák biztosítják azt az infrastruktúrát, ami lehetővé teszi az információk kezelését, illetve a rendelkezésre álló információk növekedését.
- A társadalomnak az „eladható információkkal” foglalkozó szektorainak teljesítménye dinamikus növekedésnek indul.
- A társadalom információssá fejlődése fokozottan elősegíti a globális, a nemzeti és a regionális gazdaság integrációját.

A fenti trendek pedig azt mutatják, hogy az információs infrastruktúrák az információs társadalom életében központi szerepet töltenek be.

A kulturális meghatározások a társadalomban keringő információk mennyiségével, illetve annak folyamatos növekedésével kapcsolatosak. A modern társadalom tagjait egyre több helyen, egyre több típusú, egyre növekvő számú információs csatornán – újságokon, plakátokon, rádiókon, televíziókon, telefonokon, Interneten, illetve annak számtalan szolgáltatásán – keresztül érik el szinte minden időpillanatukban, sok esetben oly módon, hogy ezekre az ingerek nem is válaszolhatnak, így ez a fajta médiainvázió elérte azt, hogy az információ a társadalom tagjainak részévé vált. A társadalom tagjai számára ugyanakkor megnyílt annak a lehetősége, hogy ezt a jelenséget egyfajta önkifejezési módként használják fel és önmagukról, nézeteikről, tevékenységükről, céljaikról információkat osszanak meg szűkebb – tágabb körben.

A fenti megközelítések konklúziója, hogy az információs társadalom kialakulásának feltétele az információ fontosságának tudatosulása, vagyis jelentőségének felismerése. Ezt a különböző definíciók kisebb-nagyobb hangsúllyal ugyan, de egyértelműen deklarálják, ugyanakkor csak kevés definícióban történik arra utalás – mivel ez a puszta definícióalkotáson alapvetően már túlmutat – hogy nem csak az információnak a megléte a döntő a társadalom működése szempontjából, hanem – sok más tulajdonság mellett – annak elérhetősége és megbízhatósága is. E fontosság oka, hogy az információ a megfelelő helyen, a szükséges időben és a kellő formában való rendelkezésre állása esetén válik csak a társadalom tagjainak számára értékké, olyan vagyonná, mely a társadalmi folyamatok szempontjából már erőforrásként fogható fel.

Tény, hogy a gazdasági tevékenység, az államigazgatás, a kultúra, a tudomány, egészségügy, a vallás és oktatásügy, és általában minden társadalmi tevékenység és szervezet rendkívül bonyolulttá vált, működése során egyre több információt termel, egyre változatosabb formában és műfajban, az irányításhoz, egyáltalán kielégítő működéséhez egyre több információt igényel. [4] Tehát a tudásalapú társadalmunk belső folyamatainak működéséhez a kellő mennyiségű információ megléte elengedhetetlen, illetve a fejlődéshez egyre többre van szükség belőle, ugyanakkor a rendelkezésre álló információ mennyisége az idővel exponenciálisan nő, mivel az a feldolgozás folyamán nem semmisül meg, tehát többszörösen – akár más folyamatban – újrafelhasználható. Tehát fejlett korunkban a társadalmi, a gazdasági, illetve a rendvédelmi szektor működésében az információ központi szerepet tölt be, így annak szükséges mennyisége és megfelelő minősége elengedhetetlenül fontos ahhoz, hogy a döntés-előkészítő, a döntéshozó, illetve a végrehajtó folyamatok hatékonysága az elvárásoknak megfelelő legyen.
Ahhoz, hogy az egyének, illetve szervezeteik, szerveződéseik az életüket, tevékenységüket hatékonyan, gazdaságosan és célszerűen tudják irányítani, információkra van szükségük, mégpedig pontosan azokra az információkra, amelyek ezekhez a feltételekhez szükségesek. Az információnak – hogy szerepét, fontosságát betöltse – mindig a megfelelő helyen, a kellő időben, a kívánt tartalommal és célszerű formátumban kell rendelkezésre állnia.

Mint látható, a felhasználó szempontjából több feltétel egyidejű megléte esetén hasznosítható csak az információ. Ha az információ, illetve annak valamely tulajdonsága nem felel meg a felhasználó – legyen az egy személy, vagy akár egy szervezet – igényeinek, akkor az hatással lesz a döntés kimenetelére, továbbá a végrehajtás minőségére, illetve a magára az elérni kívánt eredményre is. Az információk elsődleges felhasználási területe tehát a döntéshozatali

folyamatok támogatása, azonban a döntéshozatal mégis több mint az adatok összegyűjtése és a legjobb eredmény kiválasztása.

Az új társadalmi forma előnyei mellett azonban – annak fejlődésével szinkronban – megjelentek új, illetve már korábban is létező fenyegetések információs társadalomra „adaptált" változatai is. Ezek a fenyegetések az információ tartalmának megszerzése, manipulálása, illetve az információ tulajdonságainak módosítása révén jelentenek közvetlen veszélyt a társadalomra. E fenyegetések az Európai Bizottság a következő kategóriák szerint javasolja csoportosítani [5]:

- haszonszerzés céljából elkövetett cselekmények (például a gazdasági és politikai kémkedésre, személyazonosság lopás, kereskedelmi rendszerek vagy kormányzati informatikai rendszerek ellen irányuló támadások);
- szolgáltatások megzavarására irányuló cselekmények (például szolgáltatás megtagadással járó támadások, a botneteken keresztül történő kéretlen spamelés);
- pusztító célzattal végrehajtott tevékenységek (például infrastruktúrák fizikai megsemmisítése);

Azonban e felsorolást szükséges lenne még kiegészíteni azokkal a fenyegetésekkel, melyek a társadalom kognitív dimenzióit veszik célba, és egyéb módon jelentenek veszélyt (például rémhírek és terrorista propaganda terjesztése, személyes adatokkal visszaélés).

A fenyegetések hátterében az áll, hogy az információ a keletkezéstől a felhasználásig számos munkafolyamaton megy keresztül, ahol az eltérő indíttatású támadóknak – munkafázisonként különböző módszerrel, akár technikai, akár kognitív dimenzióban – lehetőségük van arra, hogy az adatot, az információt és különböző jellemzőit módosítsák, ezáltal gyakorolva hatást az információs társadalom tagjainak adatgyűjtő, elemző, döntéshozó és végrehajtó folyamataira.

Ezért az információt, annak tartalmát és minőségi jellemzőit, valamint az információs folyamatok lebonyolítására hívatott infrastruktúrát az érintett szervezeteknek, állami szereplőknek védenie kell, hogy azok rendeltetésüket maradéktalanul betölthessék. Azonban a biztonságra való igény kisebb entitások, az egyének szintjén is jelen van, hiszen az ő vonatkozásukban is értelmezhetők azok a követelmények, melyeket az összetettebb szervezetek elvárnak az információs infrastruktúráktól.

Az információ védelme annak kezelésében érintett valamennyi entitás feladata, ugyanakkor ez nem az egyedi végrehajtás szintjén valósul meg hatékonyan, hanem akkor, amikor az

érintettek együttműködve, egyfajta biztonsági ökoszisztémát hoznak létre. Ennek fontosságát az információs társadalom fejlődésének viszonylag korai szakaszában felismerték, például az ENSZ már 1994-ben megjelent informatikai bűnözéssel foglalkozó tanulmányában kijelentette, hogy az országok szintjén tett erőfeszítések nem elegendőek az e körbe tartozó bűnözés megállításához, mivel a jogellenes cselekmények földrajzi kiterjedtsége a globális információs rendszerek egészét átfoghatja. [6]

Az információs társadalom tanulmányozásakor azonban szükséges megvizsgálni azt a közeget, a kiberteret is, ahol ez a társadalmi forma értelmet nyer. A kibernetika szót a második világháború alatt a légvédelmi rendszerek irányításának matematikai modelljét kutató amerikai matematikus, Norbert Wiener 1946-ban alkotta meg a görög kübernétész (kormányos) szóból. Az új tudományos irányzat egy olyan összetett, interdiszciplináris tudományág lett, amely a szabályozás, a vezérlés, az információfeldolgozás és továbbítás általános törvényeit kutatja a műszaki, a biológiai és a gazdasági tudományok területén.
A kibertér fogalmával pedig először William Ford Gibson amerikai író Sprawl-triológiájának 1984-ben megjelent első kötetében, a Neuromancer című cyberpunk regényében lehetett találkozni, ahol előrevetítették a ma formálódó globális Internet-társadalom, a kibernetikai közösségek, a vizuális kultúrák és a ma már fékezhetetlenül terjedő virtuális bűnözés vízióját.
A Neuromancer megjelenése óta a kifejezést a legkülönbözőbb csoportok használják saját céljaikhoz igazított jelentéstartalommal, ami arra enged következtetni, hogy gyors ütemben formálódnak a számítógépes kommunikáció és a virtuális valóság fajtái. A kibertér általában ott jelentkezik a maga térkínálatával, ahol valamilyen igényt elégíthet ki, vagyis a kibertér tértípusai és alakzatai teljes egészében társadalmi eredetűek, bár ma még gyakran nincsenek megjelenítve, de egyre több informatikus tartja fontosnak, hogy láthatóvá tegye ezeket a téralakzatokat, éppen azért, hogy segítse jobban megérteni azokat.

Adatokkal bizonyítható, hogy a kibertér átalakítja a kulturális és társadalmi viszonyokat, alapvetően fontos kérdés azonban az, hogy mennyire és hogyan. A kibertérben folyó interaktív társadalmi érintkezés jelentős hatással van egyes emberekre, megváltoztatja a világnézetüket és értékeiket - véli Kateri McRae. [7] A személyes, a két ember közötti kapcsolatok háttérbe szorulnak, a köztük lévő interakciókat érzelemmentes rendszerelemek továbbítják, közvetítik, így felszínessé válnak az emberi kapcsolatok. Ugyanakkor lehetőség van a földrajzi távolságok által eddig megnehezített kapcsolattartások intenzívebbé tételére, illetve egységnyi idő alatt az adott információt nagy tömegek számára történő közvetítésre, de

a vélemények anonim vagy transzparens megosztására is. A sok féle hatás eredőjeként új társadalmi struktúrák alakulnak ki.

Meg kell említeni, hogy a kibertér polgári és katonai értelmezése, megközelítése némileg eltér egymástól. A civil terminológia szerint a kibertér az elektronikus kommunikációs eszközök és rendszerek (számítógép-hálózatok, telefonvonalak, műholdas rendszerek stb.) és a rajtuk található szolgáltatások, információk alkotta virtuális tér vagy világ összefoglaló neve. [8] Jellemzője, hogy a tértől és az időtől függetlenséget biztosít a modern társadalmunk minden tagja számára, segítve, vagy éppen megfosztva őket a távolságok, a tér és idő valós érzékelésétől, ami miatt a kibernetikus tér és idő eseményei valóságként élhetőek át. Mindegy hogy mikor, éppen hol vannak felhasználók, mikor, honnan és hogyan jönnek az információk, azok a fény sebességével azonnal áthidalják a távolságokat.

A kibernetikus tér katonai értelmezése a polgári terminológiánál szélesebb, kiterjeszti ezt a dimenziót, és nemcsak a számítógép-hálózatok működési környezetét érti alatta. A harctéren elektronikai eszközökből (pl. rádiók, radarok, navigációs eszközök, harctéri azonosító berendezések stb.) és számítógépekből olyan hálózatokat hoznak létre, ahol igen nehéz különválasztani egymástól a rendszert alkotó komponenseket, így a kibernetikus tér magába foglal minden olyan valós és virtuális teret, helyet, eszközt, rendszert, ahol az információ megszerzésével, előállításával, feldolgozásával, tárolásával és megosztásával foglalkoznak. [8] A kibernetikus térben folyó katonai műveletek során a hálózatos képességek saját oldalon való kialakítása, fenntartása, illetve ellenség oldalán való gyengítése, lerontása döntő fontosságú, ennek elérése érdekében három egymással szoros kapcsolatban lévő elemre van szükség:

1. A különböző hálózatba kapcsolt elektronikai rendszerekkel az információ megszerzése a kialakult és a várható helyzetről. Ez egyrészt jelenti a szembenálló fél elektronikai rendszereinek felderítését, képességeinek felmérését, másrészt a saját erők helyzetéről szóló információk elektronikus feldolgozását, tárolását és továbbítását, harmadrészt pedig a harctéri környezetről szóló adatok elektronikai rendszerekkel, eszközökkel való megszerzését, feldolgozását, továbbítását.
2. A megtámadott elektronikus információs rendszerek működésének korlátozása, akadályozása. Ez alatt egyrészt az elektronikai hadviselés keretében végrehajtott ellentevékenységi módszereket értjük, másrészt a számítógép-hálózati hadviselés

keretében az ellenséges számítógép-hálózatokba való behatolást, és ennek eredményeképp adatbázisok tönkretételét, módosítását, programfutási hibák előidézését jelenti.

3. A saját információs képességek kihasználása és megóvása az ellenérdekelt fél elektronikus úton végrehajtott különböző támadásaival szemben. Ez magába foglalja a saját hálózatos információs rendszereinkben rejlő lehetőségek maximális kihasználását, vagyis a hálózat nyújtotta képességek kialakítását és fenntartását illetve e rendszereink elektronikai- és számítógép-hálózati védelmét. [8]

A kibertér katonai értelmezését követően kijelenthető, hogy az itt folytatott műveletek – a köztudatban kialakult vélekedéssel ellentétben – a számítógép-hálózati hadviselésnél sokkal többet jelentenek, mivel ide sorolhatóak a navigációs és kommunikációs hálózatok pusztítása, lehallgatása, zavarása, a rendszerek elleni elektronikai ellentevékenység különböző formái, a számítógép-hálózatok feltérképezése, az azokba történő behatolás, az ott található adatbázisok, vagy az azokban lévő adatok tönkretétele, manipulálása, elérhetetlenné tétele, valamint az infrastruktúrák elemeinek túlterhelése, továbbá a támogató jellegű infrastruktúrák támadása is. E módszereken túl ide értendők még az információs infrastruktúrákat működtető személyzet különböző módszerekkel – akár a kibertérben, akár a fizikai térben történő – támadása, „zaklatása” is, mivel ezeknek hatása megjelenik a kibertérben.

A kibertér katonai megközelítése a kiberterrorizmus „filozófiájához” jobban illeszkedik, ugyanakkor a kiberterrorizmus számára a kibertér a katonai megközelítésen túl számos olyan lehetőséget nyújt még, melyet a katonai szervezetek tevékenységük és hadműveleteik során nem használnak (például finanszírozási források legális és illegális megteremtése).

I. 2. Az információ értelmezése és annak tulajdonságai

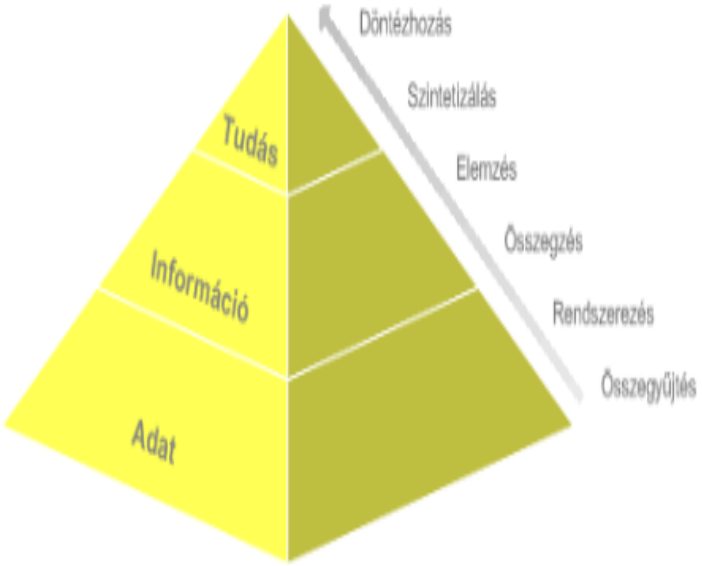
Az információs infrastruktúrák hatékony védelmének kidolgozása érdekében azonban meg kell értenünk az információ mibenlétét, létrejöttét, felépítését és jellemzőit is. A latin eredetű információ szó hírt, üzenetet, értesülést jelent, és egyben ez a szó az informatika alapfogalma is. Egyértelműen elfogadott definíciója nem ismert, mivel a különböző tudományágak más-más szempontok alapján értelmezik, így különbözőképpen is definiálják. Ugyanakkor a különböző definícióknak közös része, hogy információnak azt az adatot (hírt) tekintjük, amely a fogadó érdeklődésére számot tart és egyben ismerethiányt, bizonytalanságot is csökkent. [9]

Fontos feltétel, hogy az információ a fogadó számára érthető formában kerül átadásra, és valamilyen formában felhasználásra is kerül, ennek megfelelően igen sokféle formában lehet megjelenítve, különböző technológiájú adathordozón rögzítve létezhet. Az információ, hasonlóan fontos szerepet játszik a világban, mint az anyag és az energia. [10]

Az legegyszerűbb megfogalmazás szerint az információ a valóság számunkra érdekes részének leképzése. Az adat magában sem jelentéstartalommal, sem információval nem bír. [11] A különböző információelméletek szerint a jelentéstartalom az adatra vonatkozó valamilyen értelmezési szabályokat feltételez, és az adat ilyen szabályok szerinti értelmezése vezet a jelentéstartalomhoz. A jelentéstartalom pedig csak akkor szolgál információval az értelmező számára, ha azzal ő új ismeret birtokába kerül, tehát az értelmező bizonytalanságát csökkenti. [12]

Az anyagi világ jelenségeihez képest alapvető különbség viszont, hogy az információra nem érvényesek a megmaradási törvények, az információ megsemmisíthető (a leíró jelsorozat törölhető) és létrehozható. Bármilyen döntés meghozatala során környezetünk érzékelésére van szükség, akár egyszerű fizikai, kémiai, biológiai, vagy akár elvontabb társadalmi, gazdasági jelenségek észleléséről is van szó. Környezetünk fizikai észlelését érzékszerveink, illetve ezek fejletlenségéből és korlátozottságából, vagy épp a környezet „barátságtalan" mivoltából adódóan technikai észlelőrendszerek végzik. Érzékszerveink által megfigyelt jeleknek véges hosszúságú darabjait üzeneteknek nevezzük. Az információ az üzenet hírtartalmát jelenti.
Az információ meghatározásából következik, hogy az információt az üzenet, az üzenetet pedig jelek hordozzák, tehát az információt jelekkel is leírhatjuk. A jelek meghatározott szabályok szerinti rögzített formáját nevezzük adatnak. Az információ nem egyenlő az adattal, hanem az adatoknak az ismerettartalma az információ. Meghatározott információk előállításához meghatározott adatokra van szükség. Az adatokból információt előállító folyamatot adatfeldolgozási folyamatnak nevezzük, de ide értjük azokat a folyamatokat is, amelyek során az adatokból újabb adatokat állítunk elő, és ezek az adatok később, más folyamatban válnak információvá.
Az embereket, eljárásokat, adatokat, szoftvereket és hardvereket tartalmazó információs rendszer információtechnológiai megoldásokat alkalmaz egy, vagy több szervezeti folyamatban használt információ előállítására, továbbítására, tárolására, előkeresésére, kezelésére vagy megjelenítésére. [13]

Az információs rendszer tehát adatokból – különböző munkafolyamatok keresztül – állítja elő az információt, mely a valós világot képezi le a róla megszerzett ismeretek alapján:



1. ábra Az információ feldolgozása [13]

A gyakorlati hasznosítás szempontjából azonban elengedhetetlenül szükséges az információ funkcionális jelentését, illetve minőségi követelményeit is megtekinteni. Az információ analizálása során több jellemzőt lehet, illetve kell megvizsgálni, melyekből következtetni lehet annak minőségére, használhatóságára, valamint az információs rendszerben betöltött fontosságára. [14]

Az információs rendszerek kiépítése és működtetése előtt az üzemeltetőnek fel kell mérnie, hogy a szervezet számára melyek a fontosnak minősülő információk, és azoknak melyek azok a tulajdonságai, amik befolyásolhatják a szervezet hatékonyságát, eredményességét. Továbbá azonosítani kell azokat a fenyegetéseket is, melyek negatívan befolyásolhatják a rendszer biztonságát, illetve azokat a módszereket, megoldásokat, amelyekkel ezek kiküszöbölhetők.

Az információs rendszerek, illetve az azokban tárolt információk más-más indíttatás okán ki vannak téve különböző egyének, csoportok, szervezetek támadó, ártó szándékú tevékenységének. Egy potenciális támadó céljainak függvényében az információs rendszerben kezelt információk különböző tulajdonságainak manipulálásával jelentősen képes befolyásolni az úgynevezett – a későbbiekben bemutatásra kerülő – vezetési ciklus különböző állomásainak eredményességét, így – az egymásra-épülés jellegéből adódóan – egy sikeresen generált hiba a ciklus következő állomásán már esetleg hatványozottan jelentkező hibát okoz.

A kérdéses vezetési ciklust kiszolgáló infokommunikációs rendszer sebezhetőségi pontjainak ismeretében a támadó felmérheti, hogy az információ mely tulajdonságainak vonatkozásában lehet érdemi lehetősége arra, hogy beavatkozzon az ellenérdekelt fél információs tevékenységébe. Ilyen tulajdonságok lehetnek például – a teljesség igény nélkül – az alábbiak:

Időszerűség: Az információt akkor kell szolgáltatni, amikor arra szükség van, azaz a kérdésre adott válasznak a kérdező által megkívánt időtartományon belül kell megérkeznie.

E paraméter kapcsán a támadónak – amennyiben az információ rendelkezésre állási és felhasználási helye nem egyezik meg – a továbbítást végző infokommunikációs rendszer manipulációja révén érhet el eredményeket. A kommunikáció akadályozása mindkét irányba kiterjedhet, vagy a kérdés, vagy a válasz ne érjen célba, illetve csak olyan jelentős időveszteséggel, hogy az az információ e tulajdonságával szemben támasztott követelményt már ne elégítse ki, így a döntéshozó nem lesz birtokában minden szükséges információnak. Az infokommunikációs rendszer támadása során az ellenérdekelt fél széles palettáról választhat, a fizikai pusztítás eszközeitől kezdve, az elektronikai ellentevékenységen át, akár a számítógép-hálózati hadviselés eszközrendszeréig.

Aktualitás: Az adott identitásról érvényes, naprakész információt kell szolgáltatni, vagyis a válaszadó ne olyan információt szolgáltasson, mely már nem a valós állapotot tükrözi.

Az aktualitás tulajdonságnál is hatékonyan használhatók az időszerűségnél vázolt támadási módok, melyek a kommunikációt akadályozzák, azonban ezek itt még kiegészíthetőek olyan módszerekkel, melyek arra irányulnak, hogy az információs rendszer első lépcsőjeként is értelmezhető adatgyűjtő, érzékelő mechanizmusok ne tudjanak rendeltetésszerűen működni, illetve meg legyenek tévesztve.

Gyakoriság: Az információt olyan intenzitással kell szolgáltatni, amilyen gyakorisággal igénylik azt, tehát e tulajdonság esetén is a kommunikációt akadályozó támadási módszerek használhatók.

Időperiódus: Az információ érvényességére vonatkozó időtartam, ami vonatkozhat múltra, jelenre és jövőre. Az információs folyamatok szempontjából rendkívül fontos, hogy az adatok megszerzésének gyakorisága illeszkedjen a leírni kívánt környezeti jellemző változásának gyakoriságával, mivel csak ez garantálja azt, hogy aktuális információ legyen a birtokunkba. A múltra, illetve a jelenre vonatkozó pontos információk segítenek a jövőre vonatkozó tendenciák, becslések minél pontosabb meghatározásában.

Elérhetőség: Az a paraméter, mely megmutatja, hogy az információra vonatkozó kérdésre milyen gyorsan és milyen könnyen vagy nehezen szerezhető meg a válasz.

A támadó célja e paraméter esetében az, hogy a válasz megszerzésének idejét oly annyira elnyújtsa, hogy mire az a döntéshozóhoz ér, már ne a valóságot tükrözze. Ezt elérheti az információs folyamatok (információszerzés, továbbítás, feldolgozás) lassításával, vagy amennyiben erre lehetősége van, az információgyűjtés tárgyát képező entitás módosításával.

Megbízhatóság: Az információnak a benne előforduló hibákból származtatott minőségi jellemzője. A hibamentesség, bár minden rendszerben alapkövetelmény, azonban nem minden esetben biztosítható, így az információ felhasználása során egyfajta tűréshatárt kell bevezetni, melynek keretein belül fel lehet készülni az esetleges eltérésekre és azok hatásait kezelni lehet. Egy hatékony információs rendszerben elemezni kell a hibás adatok révén megvalósuló esetleges következményeket is.

A megbízhatóság az információ egyik legsarkalatosabb jellemzője, így ez a támadások egyik legfontosabb célja. Az információ megbízhatósága – melyen sok esetben a pontosságot is érthetjük – több ponton is támadható. Az információszerzés folyamatában már a keletkezés szakaszában lehetőség

van a megbízhatóságot befolyásolni, mely egyrészt elérhető, a környezeti jellemzők módosításával, hogy az adatgyűjtő-rendszerek ne a valóságot észleljék, másrészt pedig az adatgyűjtő-rendszerek műszaki paramétereinek befolyásolásával is. Megfelelő támadópotenciál birtokában az információs rendszerben kezelt adatok megbízhatósága manipulálható a továbbítás és a tárolás szakaszaiban is. Ugyanakkor az adatok, információk módosítása esetén figyelembe kell venni azt, hogy a túlzott torzítás (dezinformálás/dezorientálás) a támadás tényét azonnal leleplezheti.

Jelentőség: A felhasználó valódi információigényéhez kapcsolódó fogalom, ami a felhasználó számára az információ fontosságát jelzi, melyet becsülni lehet abból, hogy az információ megszerzésére mekkora erőforrásokat szabadítanak fel egy szervezeten belül.

Ezen paraméter támadása abszurd módon a megszerezni kívánt információ védelmével érhető el, ha az ellenérdekelt felet lehetőségeinkhez mérten elzárjuk az őt érdeklő adatoktól. Ez az elzárás jelentheti azt, hogy védjük saját információinkat, de jelentheti azt is, hogy az ellenérdekelt felet olyan más információs infrastruktúráktól szigeteljük el (akár a kérdéses struktúra támadásával), ahonnan információk átkerülnének saját rendszerébe. További közvetett támadási mód lehet, ha a szervezetet elvágjuk azoktól az erőforrásoktól, melyeket az információ megszerzésére tudna fordítani.

Teljesség: Fontos szempont, hogy minden információ rendelkezésre álljon a döntéshozatal során. Hogy a teljesség a követelményeknek megfeleljen fontos, hogy minden egyes részinformáció eljusson a döntéshozóhoz, így tulajdonság támadása gyakorlatilag magának az információnak a támadásával egyezik meg.

A teljesség problematikájához tartozik az is, hogy ha egy információ egy másik információra hivatkozik, akkor a hivatkozott információnak is elérhetőnek kell lennie. A teljesség hiány a döntéshozó bizonytalanságát erősíti.

Tömörség: Csak a szükséges információt kell szolgáltatni, mivel a fölösleges információk a befogadó feldolgozásért felelős rendszereit leterhelhetik, ami lassíthatja a döntéshozatali folyamatokat.

Igazolhatóság: Ugyanarra a kérdéskörre különböző helyekről, válaszadóktól, információs csatornákból származó válaszok mennyiben egyeznek meg, illetve mennyire térnek el, ami az információk ellenőrzöttségére, felhasználhatóságára vonatkozhatnak. Az igazolhatóság nem megfelelő szintje szintén a döntéshozó bizonytalanságát növeli.

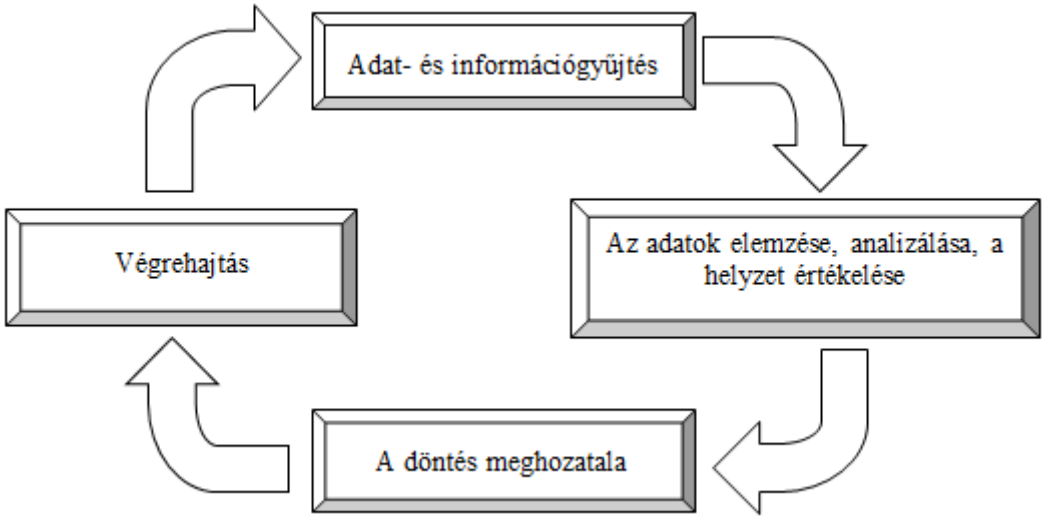
Az igazolhatóság a teljességhez hasonlóan egy olyan paraméter, mely egy párhuzamosan futó, gyakorlatilag azzal megegyező információs folyamattól függ, így támadása magának az információnak a támadásával egyezik meg.

Bizalmasság: Az információ e tulajdonsága azt hivatott biztosítani, hogy ha az ellenérdekelt fél már részben eredményesen támadta az információs rendszer valamely folyamatát (például továbbítást, tárolást) az információ akkor is csak az arra felhatalmazottak számára legyen elérhető, érthető.

A támadó, megszerezve a titkosított információkat, megfelelő szakértelem és elegendő számítási kapacitás birtokában kriptográfiai módszerek segítségével juthat hozzá a kívánt információhoz.

Az információs rendszerek ellen folytatott ártó szándékú tevékenységek során alkalmazott különböző eljárások, módszerek arra irányulnak, hogy a fenti minőségi jellemzők manipulálása révén az ellenérdekelt fél döntéshozatali folyamataira ráhatással legyenek. Elérni kívánt cél az, hogy az ellenérdekelt fél a szükséges információkhoz ne jusson hozzá (elérhetőség), ne a szükséges időben kapja meg az információt (időszerűség és aktualitás), a kapott információk pontatlanok legyenek (pontosság) és ne legyenek ellenőrizhetők (megbízhatóság, igazolhatóság), stb.. Általánosságban kijelenthető, hogy amennyiben az alkalmazott eljárás, vagy eljárások összessége minél több minőségi jellemzőt érint, annál eredményesebbnek tekinthető az információ elleni támadás.

A különböző entitások az adatokkal, az információkkal kapcsolatos tevékenységüket az információs környezet különböző dimenzióiban végzik. A számukra szükséges információkat különböző tulajdonságú, pontosságú és megbízhatóságú forrásokból szerzik be, amelyeket aztán saját szempontrendszerük alapján feldolgozzák, elemzik, értékelik. Az értékelési szakaszt követően az egyének, illetve a szervezetek céljaik elérése, küldetésük betöltése érdekében döntési alternatívákat állítanak fel, majd a rendelkezésre álló erőforrásaik, lehetőségeik függvényében meghozzák a számukra legoptimálisabbnak tűnő döntést.
A döntési folyamat lezárultával kezdődnek el a célok elérése érdekében kezdeményezett műveletek, melyeket akár a fizikai, akár az információs térben egyaránt végrehajthatnak. A végrehajtás minőségét, hatékonyságát a pontos és hiteles információk nagyban képesek növelni. [15:167] A végrehajtott műveletek értelemszerűen hatást gyakorolnak a környezet különböző dimenzióira, melyből lehet következtetni a műveletek eredményére. A hatás felmérése, illetve a további intézkedések megtétele érdekében a fentebb vázolt információgyűjtés - értékelés - döntés - végrehajtás – az úgynevezett vezetési ciklus – újrakezdődik:



2. ábra Vezetési ciklus folyamata [15:167]

A ciklusban feltüntetett pontokon végzett munka eredményességére kihatással van az előző folyamatok tevékenységének, információinak minősége. A ciklusba bekerülő adatok, információk pontossága, hitelessége a feldolgozás során torzulhat.

A ciklus meghatározott idő alatt zajlik le, mely nagyban összefügg az entitás információgyűjtő lehetőségeivel, a helyzetet elemző, értékelő szakemberek képzettségével, a vezetők tapasztalatával és a végrehajtók rutinjával, képességeivel, valamint a minden

munkafázis mögött meghúzódó technikai, informatikai, kommunikációs eszközök fejlettségével. Amennyiben a környezet a vezetési ciklus időintervallumánál gyorsabban változik, akkor a döntéshozatal során meghozott döntések már nem a valós helyzetre reagálnak, és ez a körülmény a végrehajtás hatékonyságát is jelentősen ronthatja, illetve akár hatástalanná is teheti, így ahhoz, hogy egy szervezet saját helyzetét, pozícióját a saját környezetében pontosan ismerje a fenti ciklust a lehetőségeinek függvényében minél többször szükséges végrehajtania.

Az információs folyamatokba történő beavatkozások eredményét három tényező befolyásolhatja jelentősen [16]:

- A kiberterrorista mekkora támadási potenciál birtokában van, mely azt mutatja meg, hogy a fenyegető tényezők összessége mennyire képes kompromittálni az információs rendszer biztonságát. A potenciál mértékét befolyásolja a kiberterrorista szakértelme, a rendelkezésére álló erőforrások és technikai eszközök, valamint motivációja.

  A támadási potenciál annál nagyobb:

  - minél nagyobb szakértelem birtokában van a kiberterrorista,
  - minél több erőforrás és fejlettebb technikai eszköz áll rendelkezésére,
  - valamint minél motiváltabb (elszántabb) a támadás végrehajtására.

  A támadási potenciál mértékére kihatással van, hogy mekkora a támadás végrehajtásához szükséges, illetve a valójában rendelkezésre álló idő aránya, tovább az is, hogy a kiberterrorista a rendszerről előzetesen mekkora ismeretanyaggal rendelkezik.
- A kérdéses információs rendszer milyen sérülékenységi pontokkal rendelkezik. Olyan véletlenül, vagy szándékosan létrejövő adminisztratív és technikai hibák és gyengeségek összessége, melyet a támadók kihasználhatnak. A sérülékenységi pontok feltérképezésére három lehetőség van:

  - a sérülékenységi pontokat a támadó az információs rendszer előzetes ismerete nélkül kísérli meg azonosítani,
  - részleges adatok állnak rendelkezésére,
  - illetve a rendszer teljes felépítésére, működési elvére vonatkozó információk, folyamatábrák a birtokában vannak.

  Az utóbbi két esetben feltételezhető, hogy a támadó a műveletek előkészítése során akár különböző technikai eszközök, akár humán információszerző források alkalmazásával feltérképezte a sérülékenységi pontokat.
- Milyen adminisztratív és technikai védelmi intézkedéseket milyen minőségben foganatosítottak. Az információs rendszerek biztonságára nagymértékben kihatnak az

üzemeltetésükkel kapcsolatos belső utasítások, melyeknek azonban mindig illeszkednie kell a szervezet tevékenységi köréhez és belső struktúrájához, mivel ellenkező esetben a munkafolyamatokban bizonytalanságok, hiányosságok és biztonsági rések jelentkezhetnek, melyek segíthetik a támadót.

I. 3. Információs infrastruktúrák értelmezése

Az infrastruktúra definíciójának sokféle megfogalmazása létezik. A kifejezés leginkább műszaki tartalmat hordoz, mégis a modern gazdaságfejlesztés egyik leggyakrabban használt és egyben leginkább vitatott fogalma. A latin eredetű szó magyar fordításban alapszerkezetet, alapépítményt, általában alapot jelent. Logikai jelentését tekintve valami kialakulásának, létrejöttének, fejlődésének alapja, előzménye, illetve előfeltétele.

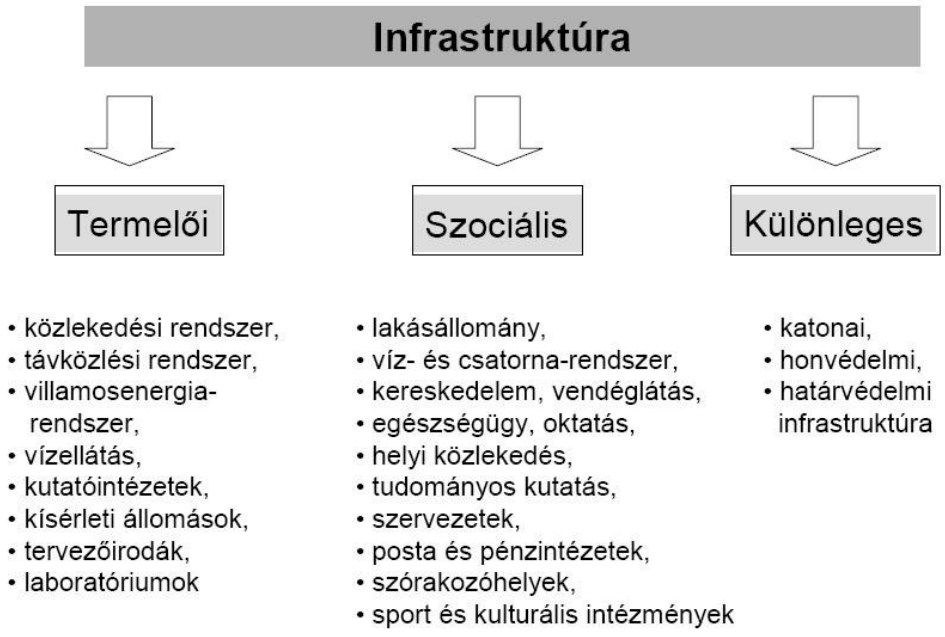
A témában keletkezett forrásmunkák tanúsága szerint először a napóleoni háborúk időszakából való írásokban vélik felfedezni különböző katonai berendezések – kaszárnyák, utak, hidak – gyűjtőneveként, más kutatások szerint viszont csak a II. világháború idején az Egyesült Államokban a hadsereg hadtáp-szolgálatában használták az infrastruktúra fogalmát. [17:6] Később, 1997-ben az amerikai kormányzat illetékes bizottsága általánosságban az alábbiak szerint definiálta az infrastruktúra fogalmát: „Az infrastruktúrák olyan egymástól függő hálózatok és rendszerek összessége, amelyek meghatározott ipari létesítményeket, intézményeket (beleértve az őket működtető személyzetet és metódusokat), illetve elosztó képességeket foglalják magukba. Mindezek biztosítják a termékek megbízható áramlását és az Egyesült Államok védelmi és gazdasági biztonságának fenntartása, valamint a minden szinten zavartalan kormányzati munka és a társadalom egész érdekében". [18]

Az Európai Unió 2008/114/EK. számú irányelvének szűkebb megfogalmazása szerint pedig „az infrastruktúra a tagállamokban található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna valamely tagállamban". [19]

A szakterület egyik korai nagy kutatója, Nyikolaj A. Utyenkov az 1970-es években az infrastrukturális állományt a termelői, a szociális és a különleges (honvédelmi) infrastruktúra részekre osztotta fel. Szerepének jelentőségét kiemelte az új területek fejlesztése során. „Az új

körzetek ipari fejlesztése során szerzett tapasztalatok azt mutatják, hogy akkor lehet eredményes az új területek bevonása a gazdasági tevékenységbe, ha a szükséges termelői és szociális infrastruktúra egy időben biztosított."

Az ő felosztása és felfogása szerint a termelői infrastruktúra a műszaki létesítmények olyan komplexuma, amely biztosítja egy adott területen a mezőgazdasági és ipari vállalatok telepítéséhez és eredményes működéséhez szükséges műszaki-anyagi feltételeket. Elsősorban magában foglalja a közlekedési rendszer létesítményeit, a villamosenergia-rendszert, a telefon-távíró távközlési rendszert, a vállalatok vízellátásához szükséges csővezetékeket és egyéb berendezéseket, az öntözési és lecsapolási rendszereket; ide kell sorolni továbbá a tervezőirodákat, a laboratóriumokat, a tudományos kutatóintézeteket és kísérleti állomásokat. A szociális infrastruktúrán létesítmények, vállalatok és intézmények olyan komplexumát érti, amelyek egy körzet társadalmi termelésben résztvevő népessége számára biztosítják a szükséges, megfelelő élet- és kulturális feltételeket. Lakások, kereskedelmi és vendéglátó-ipari vállalatok, helyi közlekedés, vízellátási és szennyvíz-elvezetési rendszerek, különböző egészségügyi intézmények, bölcsődék, óvodák, iskolák, speciális közép- és felsőfokú oktatási intézmények, tudományos kutatási szervezetek, posta- és távíróhivatalok, pénzintézetek, szórakozóhelyek, sportpályák, kulturális célú létesítmények és épületek alkotják elemeit. [20]



3. ábra Infrastruktúrák felosztása N. A. Utyenkov szerint [17:19]

Utyenkov megállapításaiból leszűrhető, hogy az egymáshoz kapcsolódó, egymással összefüggő infrastruktúrák zavartalan és hatékony működése csak közel azonos fejlettségi szintek esetében képzelhető el. Ennek következtében egy elavult infrastruktúra az

interdependencia okán negatív irányba hat más infrastruktúrák működésére, illetve egy kiugróan fejlett infrastruktúra sem éri el a kívánt célt, ha a hozzá kapcsolódó más rendszerek nem tudják igényeit kiszolgálni, vagy képességeit kihasználni.

Az infrastruktúra elemek funkcionális szempontból történő rendszerezése is elterjedt a szakirodalomban, mely a német közgazdász, Reimut Jochimsen nevéhez fűződik. Ez a felosztás alapján anyagi, intézményi és személyi-szellemi infrastruktúrákat különböztethetünk meg [21]:

1. Anyagi infrastruktúra

   Azon berendezések, felszerelések, eszközök összessége, amelyek nem vesznek részt a javak termelésében, hanem annak feltételét képezik: energiaellátás, közlekedés-hírközléstől kezdve az oktatás – képzés - tudományos kutatáson keresztül az egészségügyi és szociális ellátásig. Ezek a létesítményei a termelést és fogyasztást egyaránt szolgálják.

2. Intézményi infrastruktúra

   A történelmi-gazdasági fejlődés folyamán kialakult társadalmi szokások, normák, eljárási módok, amelyek a gazdasági folyamatok keretéül szolgálnak. Céljuk, hogy egy adott társadalom számára egyenlő jogokat, kötelességeket és egyenlő elbánást biztosítsanak. Ide tartoznak például a jogrend, az adórendszer, a pénzügyi szabályozás, szervezetek, intézmények, állami apparátus, közigazgatás, munkavállalók, munkáltatók szervezetei, a munkaerőpiac intézményei, morális szabályok stb..

3. Személyi-szellemi infrastruktúra

   A munkamegosztás különböző funkcióit betöltő emberek általános és szakmai képzettsége, kvalifikáltsága, ágazati, területi, vállalat-, és üzemnagyság szerinti megoszlásuk, valamint együttműködő készségük, megbízhatóságuk, konfliktus-megoldó képességük, továbbá rugalmasságuk, adaptivitásuk.

Jochimsen felosztása pedig azért releváns, kiemelendő, mert korán felismerte, hogy az infrastruktúrák elengedhetetlen részét képezik humán erőforrások, ezek minősége pedig áttételesen kihat a társadalom működésére.

Az infrastruktúra kiterjedtsége és szerkezete alapján megkülönböztethető vonalas és pontszerű infrastruktúra. A vonalas infrastruktúrához tartoznak az utak, vasutak, elektromos, gáz-, olaj-, távhő-, víz- és távközlési vezetékek Ezek végső soron a különböző földrajzi pontok közötti áru, személy, információ továbbítását szolgálják. A pontszerű infrastruktúra elemei az építmények, épületek, pl. repülőterek, kórházak, pályaudvarok, iskolák, közigazgatási épületek.

Az infrastruktúrák jelenlegi fejlettségi szintjén a termeléshez (előállításhoz) és a fogyasztáshoz (igénybevevőkhöz) nincs külön infrastruktúra rendelve, az infrastruktúra egyszerre szolgálja mindkettőt, akár közvetlenül, akár közvetve, de elválaszthatatlanul. Az infrastruktúra létrehozásában és működtetésében a társadalom egésze érdekelt, az állam, a hazai és a külföldi vállalkozások, az intézmények, az önkormányzatok, valamint a lakosság. Másképpen alakul azonban az érintettek és érdekeltek körének részvétele, teherviselése az infrastruktúrák létrehozásában, fenntartásában. Az infrastruktúrák körébe tartozó tevékenységek alacsony, vagy éppen negatív jövedelmezőséggel rendelkeznek, ezzel szemben tőkeigényük nagy, megtérülési idejük hosszú és ezért az üzleti szektor számára nem mindig jelentenek vonzó befektetési lehetőséget, ugyanakkor létezésük fontos, vagy akár elengedhetetlen, ezért e szolgáltatások jelentős hányadát az állam vállalja magára. Kitüntetett jelentősége van ebből a szempontból a közlekedési hálózatnak, az energiaellátásnak, egészségügynek és az oktatásnak. [17:15]

Az infrastruktúrák általában valamilyen kapcsolatban, illetve összefüggésben állnak egymással, így kiterjedtségük alapján is lehet osztályozni őket [22]:

- globális (világméretű)
- regionális (kontinentális (pl.: európai)
- nemzeti (országos)

A globális információs infrastruktúrák alatt összekapcsolt információs rendszerek és az őket összekapcsoló rendszerek világméretű összességét értjük, melyek magukba foglalják a kommunikációs infrastruktúrákat, számítógépeket és egyéb berendezéseket, szoftvereket, alkalmazásokat, az információtartalmat; az infrastruktúra összetevőit fejlesztő, gyártó, forgalmazó és szervizelő szervezeteket és személyeket, valamint az infrastruktúrákat használó szervezeteket. A regionális információs infrastruktúrák a globális információs infrastruktúrák szerves részének tekinthetők; a világot behálózó információs infrastruktúrák régiókra bonthatók, melyek lehetnek például kontinensek, vagy különböző szövetségi rendszerek által

meghatározott határvonalak. A nemzeti információs infrastruktúrák alatt különböző szervezetek, eszközök és erőforrások széles körben hozzáférhető egységes rendszerét értjük, melyeknek elsődleges rendeltetése, hogy egy adott ország kormányzati, rendészeti, gazdálkodási, illetve egyéb szervezetei és állampolgárai alapvető információ- és információs szolgáltatás-igényeinek elsősorban az adott ország határain belüli kielégítése.

Az információs infrastruktúrák értelemszerűen az infrastruktúrák halmazának egy szűkebb részét alkotják, melyek – tekintettel az információs társadalom jellegére és fejlettségi szintjére – valamilyen módon minden más infrastruktúra működtetésében részt vesznek. Az információs infrastruktúrákban zajló folyamatok alapvetően öt fő tevékenységi területhez – információs lánchoz – kapcsolódnak:

1. Információszerzés:

   A számítógépes hálózatok, a kommunikációs rendszerek ma már szerves részei az információszerzés folyamatának, mind technikai, mind pedig humán dimenzióban egyaránt. Adatok keletkeznek a különböző érzékelő-észlelő, tájékoztató, navigációs rendszerekben, stb., továbbá a humán forrásból származó információk – különböző technikai eszközök alkalmazása révén – is e szakaszban kerülnek be a vezetési ciklusba. Ebben a szakaszban felmerülhet a különböző információs rendszerek közötti interdependencia is, mivel előfordulhat, hogy egy információs rendszer információszerző képessége részben vagy nagyban összefügg egy másik rendszer információ szolgáltatási kapacitásával, lehetőségével.

2. Továbbítás:

   Szinte minden információs folyamatra, vezetési ciklusra jellemző, hogy az adatokat nem a megszerzés helyén fogják feldolgozni, illetve a származtatott információk birtokában megint csak máshol fognak dönteni az optimális intézkedésekről, valamint az intézkedések konkrét végrehajtásáról, így a különböző állomások között az információt továbbítani szükséges, mely háttérfunkcióval szemben a különböző szervezetek – alaprendeltetésük függvényében – más-más szintű elvárásokat támasztanak.

3. Tárolás:

   Ez a funkció az előző ponthoz hasonlóan, azonban attól eltérően, nem a földrajzi eltolódásokat hivatott kiküszöbölni, hanem az időbelieket. Alapvető követelmény, hogy a ciklusban lévő munkafolyamatok egymásutániságából adódó, illetve

információtechnológiai és más okokból (például folyamatos gyűjtés vagy későbbi felhasználásból) létrejövő szünetekben az információk ne vesszenek el.

4. Feldolgozás:

   A modern döntéshozatali folyamatokban már olyan nagy mennyiségű és sokrétű információ van jelen, hogy a számítógépes rendszerek alkalmazása nélkül – melyek az adatokat rendszerezik, összefűzik, keresik – már nem is lehetne hatékony információfeldolgozást megvalósítani. Egy olyan szervezet életében, mely a vezetési ciklus időperiódusának csökkentésére törekszik, nem engedheti meg, hogy a rendelkezésére álló információk feldolgozását végző rendszereire ne kiemelt figyelemmel tekintsen.

5. Megosztás:

   Az információs folyamat legutolsó fázisa, amikor is a feldolgozott információ különböző technológiai megoldások révén a jogosultsági szinteknek megfelelően eljut a megfelelő döntéshozói, illetve végrehajtói körhöz. [23]

Az információs infrastruktúráknak létrehozásuk célja alapján alapvetően kettő változata van. Egyrészt az információs társadalom szempontjából legfontosabbak a funkcionális információs infrastruktúrák, „információs közművek”, melyek szabványos elemekből felépülve a társadalom számára nyújtanak általános, bárki által igénybe vehető szolgáltatásokat. Másrészt információs infrastruktúrákat hozhatnak létre a társadalom különböző entitásai is (például gazdasági társaságok, államigazgatási szervek), akik saját információs igényeikhez igazodva, tehát tevékenységük, szervezeti felépítésük és működési környezetük függvényében – anyagi, jogi lehetőségeik, elvárt hatékonysági mutatók függvényében optimalizálva – építik ki rendszereiket. Ezek az információs rendszerek alapvetően szabványos hardver és szoftver elemekből kerülnek kialakításra, és a legtöbb, de nem minden esetben – több-kevesebb felületen keresztül – kapcsolódnak az információs közművek által, piaci alapon nyújtott szolgáltatásaihoz (például adatátvitel, tárolás, levelezés).

Az új technológiák bevezetésével és azok folyamatos fejlődése révén – amik nagyságrendekkel növelték meg az adatátvitel sebességét, a tároló- és számítókapacitásokat – megjelentek a különböző felhő-alapú technológiákat nyújtó szolgáltatások is, amik utat nyitottak az információs infrastruktúrák olyan hibrid megoldásaihoz, ahol a szervezet információs rendszerének bizonyos szegmensei (például adattárolás, adatfeldolgozás)

különböző, főleg gazdasági okok miatt áthelyeződnek egy, vagy több szolgáltatóhoz. A szolgáltatásokat beruházási költségek nélkül veheti igénybe az előfizetők. A „pay-as-you-grow" (felhasználás alapú fizetési mód) rendszereknek köszönhetően gyakorlatilag mindenki annyit és azt vesz igénybe, amire szüksége van – és csak annyit fizet érte, amennyit ténylegesen használ a felhő szolgáltatásai közül. [24]

A kiszervezésből adódóan a szervezetnek az érintett szegmensek üzemeltetését végző hardver-szoftver komponensek felett pedig teljes mértékben megszűnik kontrollja, ami egyfajta kiszolgáltatottságot jelent. Márpedig ha egy szervezet minél jobban kiszervezi információs tevékenységét külső szolgáltatók számára, annál kevesebb lehetősége van befolyásolni a számára fontos paramétereket, illetve annál jobban kiszolgáltatottá válik a külső infrastruktúra üzemeltetőjének, így nem fogja maradéktalanul ismerni a várható fenyegetettségeket, illetve azok szintjét, amiből adódóan a várható zavarokra sem fog tudni kellő mértékben felkészülni.

A zavarok – és természetesen a rendeltetés – okán megkülönböztethetőek funkcionális és támogató infrastruktúrák is. A funkcionális információs infrastruktúrák fizikai síkon biztosítják azt, hogy a társadalom valamely információs igénye kielégítésre kerüljön, tehát infrastrukturális alapon általános információs alapszolgáltatásokat nyújtanak. Ezek olyan szolgáltatásokat és információkat nyújtanak, melyeket más információs infrastruktúrák és entitások vesznek igénybe információs folyamataik (információszerzés, továbbítás, tárolás, feldolgozás, megjelenítés) során. A funkcionális információs infrastruktúrák a túlnyomó részben a különböző infokommunikációs rendszerek köré csoportosíthatók:

- különböző kiterjedtségű számítógépes hálózatok (LAN, MAN, WAN, WWW);
- vezetékes távközlő rendszerek (analóg, ISDN);
- vezeték nélküli távközlő rendszerek;
- mobiltelefon rendszerek (GSM);
- diszpécser mobil földi hálózatok (TETRA);
- műholdas távközlési rendszerek,
- műholdas navigációs rendszerek (GPS, GALILEO)
- személyhívó rendszerek. [15:74]

A támogató információs infrastruktúrák létrehozzák és folyamatosan biztosítják a funkcionális információs infrastruktúrák kiterjedt halmazainak zavartalan működéséhez, fejlődéséhez szükséges anyagi és szellemi feltételeket, illetve egyéb támogatási háttereket.
A támogató infrastruktúrák lehetnek:

- elektronikai és informatikai vállalatok;
- elektronikai és informatikai kutatóintézetek;
- raktárak és nagykereskedelmi ellátó szervezetek;
- elektronikai és informatikai képzéssel foglalkozó intézmények. [25]

A két infrastruktúra típus megkülönböztetése az információs társadalom vonatkozásában megjelenő fenyegetettségek okán azért indokolható, mert az információ és a rendszerelemek ellen intézett támadások a funkcionális infrastruktúrák esetében azonnal érzékelhető, akár súlyos zavarként jelennek meg, addig a támogató infrastruktúrák esetében ez az azonnaliság az információs társadalom szintjén nem érzékelhető.

Az infrastruktúrákra meghatározott definíciót ugyanakkor ki lehet bővíteni az adott infrastruktúra kritikusságára vonatkozó ismérvekkel is, melyek tudományáganként, szakterületenként jelentősen eltérhetnek. A szakirodalom általában három jellemző köré csoportosítva vizsgálja a kritikusság mibenlétét:

Kiterjedés: az érintett infrastruktúra földrajzi kiterjedésének tekintetében tanulmányozza a működés korlátozása, illetve megsemmisítése következtében fellépő hatást, mely lehet helyi, regionális, nemzeti, nemzetközi, vagy globális.

Súlyosság: vagy a hatás nagyságrendjét, vagy kieséséből fakadó hatás mértékét jelenti. A hatás mértékét többféleképpen lehet értékelni (például nincs hatás, minimális, mérsékelt vagy jelentős), de a megállapítás során több szempontot kell vizsgálni:

- társadalmi hatás (a szolgáltatást igénybevevők száma);
- gazdasági hatás (a gazdasági veszteség mértéke, illetve a termékek vagy szolgáltatások színvonalának romlásának mértéke; az infrastruktúra fizikai sérüléséből, elvesztéséből fakadó közvetlen – sérült infrastruktúra értéke, pótlásának költsége – vagy közvetett, piacra gyakorolt hatás, károk);

- államigazgatási hatás (állami szervek működőképességének csökkenése a létfontosságú szolgáltatások nyújtásának garantálása tekintetében);
- rendészeti, közbiztonsági és honvédelmi hatás (rendészeti és fegyveres erőinek működésére, illetve ez által az állam szuverenitására és biztonságára való ráhatás);
- politikai hatás (az államba, valamint intézményeibe vetett bizalom csökkenése);
- környezetvédelmi hatás (a környezetre gyakorolt hatás, kár mértéke);
- közegészségügyi hatás (áldozatok, betegségek, súlyos sérülések száma, illetve az ellátás minőségének romlása);
- interdependencia (az infrastruktúrák kölcsönös egymásra hatása, kiemelt kapcsolódási pontok elemzése és mértékének értékelése, az adott infrastruktúra, adott szektor, más szektor, illetve nemzeti és nemzetközi viszonylatában felmerülő függések vizsgálata; a függőségek vizsgálata elősegíti a fenyegetések potenciális hatásának értékelését is);

Időbeli hatás: az a paraméter, mely megmutatja, hogy az infrastruktúra, vagy valamely elemének kiesése mennyi idő múlva fejti ki hatását (például: azonnal, 1 óra, 24 óra, 1 hét), illetve mennyi ideig érezhető. [26] [27]

Az Európai Unió meghatározása szerint a kritikus infrastruktúrákhoz, azok a fizikai erőforrások, szolgáltatások és információtechnológiai létesítmények, hálózatok és infrastrukturális berendezések tartoznak, melyek működésének zavara, megsemmisülése komoly következményekkel járna az állampolgárok egészségére, biztonságára, védelmére, gazdasági jólétére, illetve az államigazgatás hatékonyságára. A meghatározás szerint az Európai Unió illetékes bizottsága a kritikus infrastruktúrák közé sorolja az alábbiakat:

- energiatermelés és hálózat (áramszolgáltatás, olaj- és gáztermelés, energiatárolók, energia átadó- és elosztórendszerek);
- kommunikáció és információtechnológia (távközlés, műsorszórás, szoftver és hardver hálózatok, ez alatt értve az Internetet is);
- pénzügyi szektor (bankhálózatok, ügyeletek);
- egészségügy (kórházak, egészségügyi ellátó rendszerek, laboratóriumok, gyógyszertárak, mentőszolgálatok);
- élelmiszerellátás (élelmiszerbiztonság, termelés és ellátás);
- vízellátás (vízelosztás, tisztítás, víztározók);

- közlekedés (repterek, kikötők, vasúti és tömegközlekedési hálózatok, illetve az ezek irányító rendszerek);
- veszélyes áruk termelése, tárolása, szállítása (kémiai, biológiai, radiológiai és nukleáris anyagok);
- kormányzat (kritikus szolgáltatások, létesítmények, információs hálózatok és eszközei). [28] [29]

A magyar szabályozás összhangban az uniós irányelvekkel, csak más elnevezéssel, létfontosságú rendszerek és létesítmények szófordulattal sorolja fel az említett infrastruktúrákat. [30]

I. 4. Információs infrastruktúrákat veszélyeztető események, tevékenységek

A modern információs társadalmak működése szinte elválaszthatatlan módon kapcsolódik az információs infrastruktúrákhoz, illetve az általuk nyújtott szolgáltatásokhoz. Az állampolgárok, illetve a különböző társadalmi, állami szervezetek ezeknek a rendszerek létezését eredendőnek tekintik, működésüket természetesnek tartják. A társadalmak entitásait körbevevő információs világot nagyszámú, bonyolult, komplex módon felépített, egymással szorosan együttműködő, egymásra épülő infrastruktúrák alkotják, így ezekben fellépő zavarok különböző mértékben kihatnak a többi működésére is, további zavarokat indukálnak, illetve bizonyos esetekben teljes leállást okozhatnak. A kritikus információs infrastruktúrák vonatkozásában az alábbi veszélyeket különböztethetjük meg:

- szándékos, illetve ártó jellegű cselekményekkel, tevékenységekkel összefüggő veszélyek:
    - bűncselekmények (gyújtogatás, rongálás, lopás, rablás, szabotázs, számítástechnikai rendszer és adatok elleni bűncselekmény, közérdekű üzem működésének megzavarása);
    - gazdasági, vagy politikai indítékból, kritikus informatikai rendszerek és hálózatok ellen elkövetett visszaélések, illetve kibertámadások;
    - terrorcselekmények és annak eszköz, illetve járulékos cselekményei (kiemelten robbanóanyaggal, lőfegyverrel való visszaélés, CBRN támadások);
    - fegyveres konfliktusok (háború, fegyveres csoportok támadása, polgárháború);
- természeti eredetű veszélyek, melyek az emberi tevékenységtől függetlenül, klímaváltozás, a természet erőinek hatására, elemi csapásként fordulnak elő:

    - árvíz, belvíz;
    - földrengés, földcsuszamlás;
    - erdőtűz;
    - szélsőséges időjárási viszonyok (szélvihar, felhőszakadás, hosszan tartó aszály, rendkívüli hideg, hőség, nagy havazások, hófúvások);
    - ónos eső, tartós köd, intenzív zúzmaraképződés;
- civilizációs eredetű, technológiai veszélyek, melyek az emberi tevékenységgel összefüggésben, helytelen emberi beavatkozás, mulasztás, figyelmetlenség, vagy technikai, konstrukciós hibák hatására következnek be:
    - számítógépes programozási hiba;
    - tervezési, konstrukciós hiba;
    - űrobjektum becsapódása;
    - közúti, vasúti, vízi és légi közlekedési baleset;
    - környezetkárosodás, felszíni vizek szennyeződése, légszennyeződés;
    - veszélyes ipari létesítményekben, szénhidrogén kitermelésében, veszélyes anyag tárolása és szállítása közben bekövetkező baleset;
    - ipari létesítményekben bekövetkező műszaki-technikai baleset, zavar;
    - nukleáris baleset;
    - tűzvész. [31]

Amennyiben a vizsgált körbe tartozó rendszerek a támadások célpontjai, úgy az eredményesség függvényében a társadalom egyre szélesebb rétegeire lehetnek kihatással. A társadalom belső viszonyait teljesen szétzilálhatja a közlekedési, a kommunikációs, a gazdasági-pénzügyi rendszerek egyes elemeinek funkcionális kiesése, mivel a begyakorolt napi rutin megoldások megszűnésére nincsenek felkészítve az emberek és szervezetek. Például a közlekedés szervezését irányító rendszerek funkcióinak zavara jelentősen kihat a társadalom működésére. A lakosság mozgásának nehézségei miatt más infrastruktúrák üzemeltetésében résztvevő személyek nem jutnak el munkahelyükre, az áruszállítás akadályoztatásából adódóan az infrastruktúrák zavartalan működéséhez szükséges anyagok, áruk, szolgáltatások nem érnek célba, így a hatás más rendszerekre is kiterjedhet, átterjedhet.

A villamos energia-elosztó rendszerek kiesése, erre fel nem készített infrastruktúrák esetében szinte minden más infrastruktúra működésére, illetve azok szolgáltatására kihatással lehet. Itt

nem elhanyagolható az időbeli hatás sem, ami különösen kritikussá teszi az ágazatot, mert hatása szinte azonnal jelentkezik más rendszereknél. Más infrastruktúrák az áramszolgáltatás átmeneti kiesésére általában rövidebb-hosszabb ideig fel vannak készítve (például egészségügyi intézményekben lévő áramfejlesztők lépnek üzembe áramkimaradás esetén), azonban ebben az esetben is más energiahordozókra vannak utalva (például egy kórház esetében az áramfejlesztők szénhidrogénekkel működhetnek), és amennyiben azok működésében is zavarok jelentkeznek, akkor a kérdéses rendszer, illetve infrastruktúra működésében szintén zavarok jelentkezhetnek. [32]

Az információs infrastruktúrái ellen intézett támadások előkészítése, megszervezése és végrehajtása a kibertéren keresztül rendkívül összetett és összehangolt tevékenységet feltételez, mely alatt egyrészt technikai, másrészt pedig humán oldali összetevőket kell érteni. A támadók akcióik sikeressége érdekében három pillérre építhetnek:

- az információs infrastruktúrát alkotó elemek, részegységek műszaki hibáira, sérülékenységére,
- az adminisztrációs, fizikai, logikai és elektronikai védelem gyengeségeire,
- a védelmi intézkedések elhanyagolására,
- valamint a rendszerben foglalkoztatott humánerőforrások jelentette kockázatokra.

Az információs rendszerek üzemzavarainak „előidézése” mögött számos motiváció meghúzódhat, így a fenti kockázatokra vonatkozó információk megszerzését és értékelését követően a kiberterroristák mérlegelhetik, hogy a feltárt gyengeségekből adódó lehetőségek ismeretében, illetve rendelkezésre álló képességeik, módszerek és eszközök birtokában milyen reálisan elérhető és ideológiájukkal összeegyeztethető célt tűzhetnek ki a kiválasztott infrastruktúra, vagy annak elemei vonatkozásában.

Ugyanakkor a „hagyományos” háborús helyzetekben a célok kötöttebbek. Ekkor a hadviselő országok a másik fél kommunikációs rendszereinek zavarásával, pusztításával káoszt idézhetnek elő a csapatvezetési és fegyverirányítási rendszerekben, a közlekedési és közművek infrastruktúrájának támadásával az ellenség logisztikai és utánpótlási lehetőségeit szűkítik. Katonai szempontból a legfontosabb információs infrastruktúrák a szembenálló fél:

- vezetési rendszerelemei (eszközök, vezetési pontok, vezetők),
- fegyverirányító rendszerei és fegyverei,
- felderítő rendszerei,
- elektronikai hadviselési rendszerei,
- kommunikációs és híradórendszerei,

- informatikai eszközeit és rendszerei,
- támogató és egyéb infrastrukturális létesítményei. [15:218]

Továbbá a műsorszóró, tömegtájékoztató rendszerek működésének korlátozásával a lakosság tájékoztatását, irányítását (pl. a sorkötelesek mozgósítását, óvóhelyek megnyitására vonatkozó adatok közlését) akadályozhatják, illetve e tájékoztatást szolgáló rendszerek feletti részleges, vagy teljes uralom megszerzésével, a pszichológiai hadviselés részeként befolyásolni is tudják az ellenség katonáinak, illetve a hátország lakosságának morálját. A katonai műveletek esetében azonban alapvetően nem a civil információs infrastruktúrák jelentik a hadműveletek főirányát, ellenben a hatásalapú tervezés keretében az interdependencia továbbgyűrűző hatását kihasználhatják más rendszerek irányába. A kibertérben végrehajtott katonai műveletek alapelve az, hogy a fenti célpontokon, célobjektumokon keresztül a katonai és – adott esetben – polgári, kormányzati, közigazgatási, ellátás-szervezési funkciókat is lehet, illetve szükséges támadni. Az elv szerint nem a kibertámadás közvetlen célpontjai jelentik a valódi célt, hanem azokon keresztül a befolyásolásra kiválasztott, tervezett vezetési funkciók akadályozása, korlátozása. [15:169]

Az információs infrastruktúrákra azonban nem csak katonai szervezetek, hanem hacker-ek (számítógépes hálózatokat feltörők), hacktivisták (politikai indíttatású hacker-ek), cracker-ek (programfeltörők, szoftverkalózok), jerk-ek (vandálok), phreak-ek (kommunikációs hálózatokat feltörők), számítógépes bűnözők, ipari kémek, sértődött alkalmazottak és kiberterroristák célpontjai lehetnek. A felsoroltak bár sok esetben ugyanazokat az eszközöket és módszereket használják, de alapjaiban különböznek motivációik, eltérőek képességeik és lehetőségeik, ezért célszerű is megkülönböztetni őket:

- Hackerek

  Az ácsolni, barkácsolni jelentő angol hack igéből származtatott kifejezés, de a szó az informatikában átvitt értelemben kódfaragót jelent. Az 50-es évekből eredeztethető, amikor is a Massachusetts Institute of Technology számítógépeit programozó diákjai és szakemberei kezdték magukra használni ezt a kifejezést, mégpedig azért, mert az akkori, mai szemmel nézve kezdetleges számítógépek korlátaival találkozva, munkahelyi vezetőik engedélye nélkül igyekeztek az optimális működés érdekében a lehető legkisebbre tömöríteni a programok és operációs rendszerek kódjait. A hacker minél hatékonyabban tömörítette a kódot – tehát „faragott” le annak méretéből – annál nagyobb elismerés, tekintély illette.

Ugyanakkor a számítástechnika és a média fejlődésével párhuzamosan a hacker szó jelentése is átalakult. Korábban kimagasló számítástechnikai ismeretekkel rendelkező személyt jelentett, aki segítő jelleggel tárta fel a számítógépes rendszerek, hálózatok és alkalmazások sérülékenységeit, hibáit, illetőleg felhívta ezek létezésére a figyelmet. Azonban a média a hacker szót a számítógépes bűnöző (betörő) szinonimájaként – a cracker kifejezés helyett – használja, és eredeti tartalom az etikus hacker, vagy a fehérkalapos („white-hat") hacker kifejezés mögé szorult. Feketekalapos („black-hat") hackernek pedig azokat a hackereket nevezik, akik különböző motivációktól vezérelve, tudásukkal visszaélve jogosulatlanul törnek be számítógépekbe, illetve számítógép-hálózatokba. Használatos még a szürkekalapos („grey-hat") hacker elnevezés is, mely gyakorlatilag a fehér- és a feketekalapos hacker közötti átmenetet jelent. A szürkekalapos hacker egy biztonsági résre rábukkanva kihasználja azt, majd a sérülékenységről értesíti a rendszer üzemeltetőjét, és akár segítségét is felajánlja a hiba elhárítása érdekében. Létezik még egy kékkalapos („blue-hat") hacker elnevezés is, melyet a szakirodalom a megjelenés előtt álló programok, technológiák tesztelőire használják. [33]

A feketekalapos hackerek társadalmában több „szociológiai" státuszt is használnak, melynek alapja az illető szakértelme. A „neophyte", „n00b", vagy „newbie" kifejezést a teljesen kezdő és tudatlan hackerekre használják. A „script kiddie", light-hacker, a wannabe-hacker, trollok a komoly szaktudással nem rendelkező, más hackerek által megírt programokat, kidolgozott eljárásokat önállóan használó hackerek gyűjtőnevei. [34] Az abszolút felsőkaszt az „elit hackerek", akik már mélyreható szakismeretekkel rendelkeznek az infokommunikációs rendszerekről, és képesek azokat a támadókódokat megalkotni, eljárásokat kifejleszteni, melyek birtokában hatékonyan végre tudják hajtani a támadásokat.

- Hacktivisták

A hacktivizmus általában logikai vagy fizikai hatáson alapuló eszközökkel végrehajtott proaktív politikai aktivizmus, egyfajta demonstratív figyelemfelkeltés

a kibertérben, melyet legtöbb esetben a szólásszabadság, az emberi jogok, a környezetvédelem és az információ szabadsága ellen megjelenő vélt, vagy valós veszély generál.
Célja, hogy az információs társadalomban a megfelelő képviseletet nélkülöző csoportok problémáira, illetve a válaszul adható megoldásokra felhívja a figyelmet. A hacktivista gyakorlatilag egy hacker és egy aktivista tulajdonságait, képességeit ötvözi, és rendszerint politikai motivációval rendelkezik [35:135].

A hacktivisták akcióik során az általuk képviselt témával, konkrét esetekkel kapcsolatos honlapokat törik fel, megváltoztatják annak kinézetét, adatokat lopnak el és megosztják a nyilvánossággal azokat, illetve akadályozzák a honlapok működését. Nem egy esetben tevékenységük már a kiberterrorizmus határait is feszegeti. Egyes vélemények szerint pedig a hacktivizmus és a kiberterrorizmus nem különbözik egymástól, eszközrendszerét és célját tekintve legalábbis rokon területekről lehet beszélni, hiszen az eszközök „nem erőszakos" használata az infrastruktúrák összefüggése miatt könnyen „nem szándékosan erőszakos", de mégis valós következményekkel járó eredménnyel járhat. [36]

- Számítógépes bűnözők

Napjainkra a számítógépes bűnözés egyre elterjedtebbé és egyben egyre jelentősebbé is vált, ugyanakkor még nincsen egységesen elfogadott fogalma. aminek oka a jelenség változékonyságában és sokszínűségében keresendő. Általánosságban azon bűncselekmények összessége, amelyek információ-technológiai eszközök, rendszerek, illetve rendszerelemek ellen irányulnak vagy információ-technológiai eszközöket, rendszereket használnak a bűncselekmény elkövetésének eszközeként.

Az országok jogalkotásában egyre terjedő tendencia, hogy nem is próbálnak meg egy általános definíciót alkotni az e fajta jogsértésekre, hanem magát a konkrét jogellenes tevékenységet leírva definiálják azt (például bankkártya-csalás, adatlopás, kommunikációs hálózatok elérhetetlenné tétele, stb.). A számítógépes bűnözésnek számos osztályozása létezik, azonban a vizsgált témához

kapcsolódóan az osztrák Gabriele Schmölzer és Peter Schichk által az alábbiak szerint felosztott illegális magatartási formái illeszkednek legjobban:

1. támadás a hardver ellen:
   - jogosulatlan belépés,
   - gépidőlopás,
   - a mikrochip jogtalan másolása;
2. támadás a szoftver ellen:
   - szoftverlopás,
   - programmanipuláció;
3. támadás az adat ellen:
   - adatmanipuláció,
   - adatlopás,
   - visszaélés az adatfeldolgozási tevékenységgel. [37]

Számítógépes bűnözés tevékenységi köréhez sorolhatók azok az elkövetési formák is, amikor egy információs rendszer sérülékenységeire vonatkozó adatokat a rendszer üzemeltetőinek, vagy másoknak megvételre felkínálják. Trendként érzékelhető a különböző zsarolóprogramok alkalmazása is, amikor a megtámadott számítógépen lévő felhasználói állományokat titkosítják, amit csak „váltságdíj” fejében oldanak fel.

Ugyanakkor már a hagyományos szervezett bűnözői körök is felismerték és használják is a számítógépes bűnözés módszereit tevékenységük hatékonyságának növelése érdekében, illetve az illegális jövedelem legalizálása érdekében.

A számítógépes bűncselekményeket végrehajtó személyek gyakran igen magas szintű hálózati és számítógépes ismeretekkel rendelkező elkövetők, akiknek elsődleges motivációja a pénzszerzés. A hackerek eszköztárában is megtalálható, vagy sokszor azok köréből származó rosszindulatú szoftverek, illetve eljárások alkalmazása révén hajtják végre akcióikat. A számítógépes bűnözők által elkövetett bűncselekmények, illetve az ezekkel okozott károk nagysága folyamatosan emelkedik.

- Ipari kémek

  Az ipari kémkedés definíció szerint olyan adat-, vagy információszerző tevékenység, illetve a jog által tiltott vagy etikailag kifogásolható viszony, viselkedésforma, amelynek célja a gazdaság, a tudomány, a kereskedelem, az üzleti élet területén jelentkező, esetleg a későbbi várható versenyhelyzetben való szinten maradás fenntartása, a konkurenssel szemben meglévő lemaradás leküzdése, behozása. [38]

  Az ipari szektorban ez a fajta jogellenes információszerző tevékenység azonban nem a XXI. század találmánya, hiszen már az iparosodás előtt is jelen volt céhek életében, azonban ahogy a számítógépek betörtek ide is, az ipari kémkedés módszerei is átalakultak. A számítógépes tervezés, irányítás és rendszerfelügyelet magában hordozza azt a lehetőséget, hogy a számítógépeken tárolt, vagy a hálózatokon áramoltatott adatokat és információkat illetéktelenek - ebben az esetben ipari kémek: konkurens cégek alkalmazottai, vagy éppen az előbb említett számítógépes bűnözők, akik a megszerzett adatok piacra dobásával üzletelnek - szerzik meg. Megjelent tehát egy új, elektronikus csatorna az illegális adatszerzők kezében, amelyen keresztül hatalmas mennyiségű adatot képesek szerezni, amely ráadásul nemcsak polgári cégek adataiban merülhet ki, hanem katonai technológiák adatainak a megszerzésére is irányulhatnak, amelyek esetenként sokkal több pénzt is érnek bizonyos piacokon. [39.]

  Talán e motiváció esetében jelenik meg legmarkánsabban az a követelmény, hogy a jogellenes cselekmény elkövetésének ténye titokban is maradjon. Míg a többi típusú elkövető esetében az elkövetés tényének titokban maradásához nem fűződik kiemelt érdek, vagy épp az a cél, addig az ipari kémek esetében rendkívül fontos az, hogy az ellenérdekelt fél ne is szerezzen tudomást arról, hogy információs rendszerét támadás érte, mivel az esetlegesen bevezetett intézkedések eredményeképpen a megszerzett adatok értéktelenné válhatnak.

- Munkatársak és külső szakértők

  Az információs infrastruktúrák tulajdonosai – főként a profitorientált gazdasági társaságok – sok esetben külső, erre a feladatra specializált szakértőkre bízzák az

információs hálózatuk kialakítását, valamint üzemeltetési feladataikat (outsourcing). A kétségbevonhatatlan előnyök mellett azonban a nagyfokú kiszolgáltatottság is megjelenik, mivel az üzemeltetés során olyan érzékeny információk kerülhetnek a külső szakértők birtokába az érintett rendszerről, az abban tárolt információkról, illetve magát az információt is megszerezhetik, melyekkel visszaélve súlyos károkat okozhatnak.

A fenti probléma megjelenik az egyre nagyobb mértékben elterjedőben lévő, különböző típusú felhő szolgáltatások esetében is, ahol a szolgáltató munkatársai szintén visszaélhetnek a birtokukba kerülő információkkal, illetve maguknak a szolgáltatásoknak a rendelkezésre bocsátásával.

Az informatikai biztonságot vizsgáló cégek statisztikái szerint a betörések megközelítőleg nyolcvan százalékát a szervezetek saját alkalmazottai követik el. A sértődött vagy elbocsátott emberek, a rendszerről meglévő ismereteik révén nagy károkat okozhatnak. Az okok általában irigység, sértettség, bosszú, vandál pusztítási vágy, rosszindulat, hirtelen felindulás, hírszerzés és ipari kémkedés támogatása, információszerzés anyagi vagy egyéb előnyökért. [40]

- Kiberterroristák

Az előzőekben bemutatott szereplőket követően kell megemlítenünk a terroristákat is, hiszen ők is használják az információs infrastruktúrákat. Attól függően, hogy milyen célból használják az információtechnológiát, két csoportra oszthatóak. „Az első csoportba, azok a terrorista szervezetek tartoznak, amelyek a propaganda, toborzási és adatszerzési célokra használják e rendszereket. A másik - sokkal veszélyesebb - csoportba azok a terroristák tartoznak, akik nemcsak ilyen úgynevezett "soft" tevékenységre kívánják használni a rendszereket, hanem azt, illetve azon keresztül rombolni vagy egyéb erőszakos, "hard" cselekményeket is végre akarnak hajtani”. [35:139]

Az előzőekben vázolt sokrétűségből következik, hogy a kiberterrorizmus esetében – a katonai megközelítéstől eltérően – rendkívül nehéz pontosan felsorolni a potenciálisan veszélyeztetett infrastruktúrák körét. Ennek fő oka, hogy a modern információs társadalom jellegéből

adódóan a társadalmi közhangulatban – akár nemzeti, akár nemzetközi szinten – olyan hirtelen változások (például gazdasági, politikai erőviszonyok felborulása, környezeti katasztrófák, stb.) következhetnek be, melyek eredményeképpen szükséges átgondolni az adott pillanatban potenciálisan veszélyeztetett információs infrastruktúrák körét. Például a korábban veszélyeztetett infrastruktúrák körét egy társadalmi csoportot hátrányosan érintő politikai, gazdasági döntés látványosan felülírhatja, és az érintett párthoz, gazdasági szervezethez (bank, iparvállalat) kapcsolódó rendszerek támadására lehet nagy valószínűséggel számítani, még ha csak átmenetileg is.

Ugyanakkor fontos momentum, hogy egy információs infrastruktúra elleni terrortámadás végrehajtása – a technikai megvalósítás terén – többszörösen összetett feladat. Egy hatékony támadás csak több frontos, azaz egy időben több rendszerelem, de akár több információs infrastruktúra támadását feltételezi. Továbbá van néhány olyan – ma már nagyon jól védett – kritikus információs infrastruktúra, ami hatékonyan nem is támadható információs oldalról, azaz a támadás hagyományos eszközöket – fizikai (kinetikus, termikus) pusztítást, rombolást – feltételez. A kritikus információs infrastruktúrák kisebb elemei (például a telekommunikációs átjátszóállomások tornyai) lényegesen kisebb fizikai védelemmel vannak ellátva, így azokat közelről, helyből primitív eszközökkel is tudják rombolni a terrorcsoport tagjai, akik cselekményeikkel az elem fontosságából adódóan a teljes rendszerben csak kisebb kiterjedésű zavarokat okozhatnak, bár ez a zavar a támadott elemek számának növelésével fokozható. Ezzel szemben egy bonyolult felépítésű, összetett rendszer (például egy légi irányítási komplexum) lényegesen nagyobb védelmet élvez, így azt csak távolabbról, összetettebb fegyverek alkalmazásával lehet sikeresen pusztítani, azonban egy eredményes támadás esetében mind a fizikai kár, mind a területi hatás lényegesen nagyobb lehet.

Egy sikeres kibertámadás feltételei között, a humán oldali összetevőknél kiemelt helyen kell gondolni a szükséges felkészültség meglétére. A rendkívül bonyolult, a legfejlettebb információtechnológiai és védelmi megoldásokat alkalmazó rendszerek támadása igen magasan képzett és gyakorlott szakemberek rendelkezésre állását igényli, akik kiképzése, vagy épp megnyerése, szolgáltatásaik megvásárlása (terror by proxy) rendkívül nehéz feladat lehet a terrorszervezetek számára. Ugyanakkor legalább annyira fontos az – bármennyire is triviálisnak tűnik – hogy ez a felkészült szakembergárda mind az támadások végrehajtásakor, mind pedig annak esetleges elhárításakor a megfelelő helyen és időben, a megfelelő létszámban és a szükséges szakismeret arányában rendelkezésre is álljon.

Mindezek mellett a XXI. században a modern fegyveres erők és gazdasági szervezetek által működtetett információs infrastruktúrák elterjedten használják ki az elektromágneses tér által nyújtott lehetőségeket a kommunikáció, navigálás, fegyverirányítás, ellenőrzés, felderítés során. Ezen a területen alkalmazott kifinomult, különböző rendeltetésű elektronikai eszközök jelentős mértékben tudják növelni a szervezetek hatékonyságát, illetve támaszkodnak is rájuk feladatok végrehajtása során, ebből kifolyólag egy információs infrastruktúra elleni hatékony támadás során megkerülhetetlen az alkalmazott elektronikai eszközök elektromágneses energiák által történő támadása.

I. 5. Összegzés, részkövetkeztetések

Az információs társadalom kialakulásának egyik mérföldköve az volt, hogy felismerték, hogy az információ a társadalom tagjai számára érték, és ez az érték további értékteremtésre is alkalmas. Az értékteremtésnek egyik feltétele, hogy a rendelkezésre álló információ mennyisége folyamatosan növekedjen, ami értelemszerűen azt is jelenti, hogy az ezt kiszolgáló infrastruktúrák száma folyamatos növekedést, képességei pedig folyamatos fejlesztést igényelnek.
Az információs társadalom fejlődésével arányban azonban a fenyegetések száma is arányosan növekszik, és az új típusú kihívások mellett a konvencionális társadalmi modellben értelmezhető fenyegetések mindegyike fel is bukkan az információs társadalom fő megjelenési helyén, a kibertérben.

Az infrastruktúrákra veszélyt jelentő szándékos, illetve ártó jellegű cselekmények, tevékenységek végrehajtóinak motivációi és támadói potenciáljai jelentős mértékben eltérnek, így az információ tartalmára, tulajdonságaira, illetve áttételesen pedig a vezetési ciklus különböző állomásaira eltérő veszélyt jelentenek. Az információs társadalom különböző megközelítései mindegyikének esetében meg lehet találni azt az elkövetői típust, illetve jogellenes cselekményt, mely illeszkedik az adott megközelítésre, vagy megközelítésekre. Például míg a terroristapropagandát a kulturális megközelítéssel lehet kapcsolatba hozni, addig az infrastruktúrák pusztítása a technológiai és a térszemléletű megközelítéshez kapcsolódik.

Mivel az információ jelenti az alapját az információs, vagy más néven tudásalapú társadalomnak, ezért értelmezése, tulajdonságainak meghatározása, valamint azok vizsgálata

az információs rendszerek fejlődésének szempontjából elengedhetetlenül fontos. A különböző tudományterületek sajátosságaik függvényében az információt különbözőképpen határozzák meg, de a definíciók közös része az az, hogy az információ általánosságban új, a vizsgáló számára releváns ismeretet hordoz.

A társadalom folyamatos működése érdekében az információnak folyamatosan rendelkezésre kell állnia, és az információs társadalom fejlődéséhez pedig egyre nagyobb mennyiségű elérhető információra van szükség. A társadalmi és döntéshozatali folyamatok hatékony monitorozásának, irányításának igénye az információval szemben nem csak mennyiségi, hanem minőségi, illetve egyéb más követelményeket is támaszt. Az információnak, hogy azt fel lehessen használni, a megfelelő helyen, a megfelelő időben és a felhasználó számára értelmezhető formában kell megjelennie.

Tekintettel arra, hogy a komplex információs folyamatokban kezelt információmennyiség már oly mértékű, illetve olyan gyorsan kell megszerezni, továbbítani, feldolgozni, hogy ezt informatikai eszközök nélkül hatékonyan már nem lehetne megoldani, így evidens, hogy az információs társadalom működése a kiterjedt infokommunikációs hálózatok nélkül elképzelhetetlen, ezért ezek a hálózatok a fő célpontjai a kibertérben végrehajtott támadásoknak. A társadalom funkcióinak – információs folyamatainak – támogatása, illetve azok folytonosságának fenntartása érdekében a társadalom bizonyos entitásai különböző információs infrastruktúrákat hoznak létre, egyrészt saját, másrészt pedig más entitások igényeinek kiszolgálása érdekében. Utyenkov és Jochimsen gondolatát egyesítve, az infrastruktúra feladata tehát, hogy biztosítsa egy adott ország államigazgatásának, rendészeti szerveinek és gazdasági szervezeteinek rendeltetésszerű működését, a termelés, a fogyasztás és az elosztás folyamatát a gazdaság mindenkori fejlettségének megfelelő szellemi, humán és technikai színvonalon. A XXI. században már egy ország infrastruktúráinak elemzésekor azok alrendszereinek összességét is figyelembe kell venni, mivel kölcsönösen összekapcsolódnak, függnek egymástól, egymás meglétét, zavartalan működését feltételezik.

A közgazdasági és műszaki tudományok dinamikus fejlődése, illetve a gazdasági, társadalmi kapcsolatok átalakulása ellenére az infrastruktúra definíciójának meghatározása alapvetően nem módosul, de a kifejezés, illetve annak jelentéstartalma állandóan bővül, hiszen a műszaki fejlesztéseknek, technológiai újításoknak, társadalmi igényeknek köszönhetően újabb és újabb infrastruktúraelemek, típusok jelennek meg. Napjainkban pedig éppen az infokommunikációs

infrastruktúrák minden területet érintő térnyerése, valamint a más infrastruktúrákra gyakorolt hatása miatt válik aktuálissá meghatározásának kibővítése.

Mivel az információ értékét – a tartalmán (hírértékén) túl – a felhasználó számára releváns tulajdonságai határozzák meg, és ez miatt a különböző káros, ártó hatásokkal, támadásokkal szemben védenie kell. Azonban nem csak az információt szükséges megvédeni, hanem az azt kezelő infrastruktúrát is meg kell óvni, mivel a megfelelő minőségű információ, illetve az azt hatékonyan feldolgozni képes infrastruktúra együttes rendelkezésre állása biztosítja azokat az előnyöket, melyek az entitások számára értékkel bírnak.

A nagy földrajzi kiterjedtségű, vagy a funkcionalitásában összetett infrastruktúrahalmazok bármelyik tagjának, vagy alrendszereiknek kiesése, súlyos működési zavara a kölcsönös függőség révén más infrastruktúrarendszerekben is problémákat indukálhat, azok hatásfokát leronthatja, vagy akár szolgáltatásaikat is megbéníthatja, ami az információs társadalom működésében széles társadalmi rétegeket érintő nem kívánt hatásokat idéz elő. E negatív hatások tükrében kijelenthető, hogy a kritikus információs infrastruktúrák védelme kiemelt prioritást kell, hogy élvezzen mind az üzemeltetők, mind pedig az állam részéről.

A megelőzés, a hatékony védelem kialakítása érdekében azonban első lépésben fel kell mérni azokat a veszélyeket, fenyegetéseket, melyek az információs infrastruktúrákra potenciális veszélyt jelenthetnek. A tudomány mai fejlettségi szintjén a természeti eredetű veszélyek viszonylag nagy pontossággal előre jelezhetők, kiküszöbölhetők, a civilizációs eredetű technológiai veszélyek egyes pontjai megfelelő körültekintéssel megelőzhetőek. A legnagyobb veszélyt azonban az ártó jellegű tevékenységek jelentik az információs infrastruktúrákra, mivel míg az előző pontokban az információ tartalmának és tulajdonságainak módosulása, valamint az infrastruktúra integritásának sérülése, szolgáltatásainak kiesése csak következmény, addig az ártó jellegű tevékenységeknél ez a kifejezett cél, és ez a célirányosság fokozottan növelheti az ártó szándék infrastruktúrára gyakorolt negatív hatását.

Az információs infrastruktúrák támadóinak köre igen tág lehet, a professzionálisan felszerelt és vezetett reguláris, katonai jellegű szervezetektől, hírszerző és biztonsági szolgálatoktól kezdve a szervezett bűnözői csoportokig, azonban az információs infrastruktúrák vonatkozásában a kiberterrorizmus az a fenyegetés, mely legszélesebb körben hasznosítja az

azok által nyújtott lehetőségeket, előnyöket, illetve a sérülékenységeinek kihasználásával a társadalom nagy tömegeinek életére lehetnek hatással. További kockázat lehet a kibertérben elkövetett terrorcselekmények eszkalálódása. Míg bizonyos támadók (például ipari kémek, kiberbűnözők) jogellenes tevékenységüket igyekeznek „minimalizálni", leplezetten, titokban és célhoz kötötten végrehajtani, addig a kiberterroristák cselekményeik következményeivel nem számolva, az interdependencia miatt eredeti terveiken jelentősen túlmutató károkat, veszélyhelyzeteket indukálhatnak.

Ugyanakkor információs infrastruktúrák ellen terrorcsoportok részéről indított és napvilágra került kibertámadások jellemzőinek tanulmányozása alapján kijelenthető, hogy ez a hatásalapú megközelítés a kiber-terrortámadások esetében nem jelenik meg ennyire markánsan, komplexen, ott jellemzően csak a kiválasztott információs infrastruktúra közvetlen támadása a cél, tehát az interdependencia, az infrastruktúrák összefüggéseinek, összefonódásainak felderítése, felmérése mélyrehatóan nem történik meg.

II. A kiberterrorizmus

II. 1. A terrorizmus értelmezése

Az információs társadalmat érintő legnagyobb fenyegetés, a kiberterrorizmus mibenlétének megértése, illetve jellegzetességeinek felismerése céljából szükséges magát a terrorizmust tanulmányozni, mivel a kiberterrorizmus gyökerei innen erednek, még ha megjelenési módjai a hagyományostól, a megszokottól eltérőek.

A terrorizmusnak az általános definiálása, konkrét, szövegszerűen behatárolható fogalommá tétele rendkívül nehéz, annak ellenére, hogy napjainkban a különböző médiaszolgáltatások révén, napi szinten – akár véres valójában – is láthatja a társadalom ezt a sokszor értelmezhetetlen, megmagyarázhatatlan jelenséget. Ugyanakkor ez a jelenség, amelyet terrorizmusként azonosítunk már a történelem hajnalán megjelent, gyakorlatilag az emberiséggel egyidős. Az idők során a mögötte álló ideológia folyamatosan változott, az alkalmazott eszközök és módszerek – a technológiai fejlődéssel összhangban – egyre fejlettebbé és hatékonyabbá váltak, kiterjedése pedig olykor gigantikus méreteket öltött és korszakokon ívelt át. A célpontok, a szenvedő alanyok, az eszközök, a módszerek folyamatosan változtak, azonban a terrorizmus lényege mindig ugyanaz maradt, a félelemkeltés.

Ahogy a terrorizmus történelmét nyomon követjük, úgy annak különböző megnyilvánulási formáiból kirajzolódnak fajtái, illetve azt is tetten érhetjük, hogy koronként melyek domináltak:

- Egyéni terrorizmus

  A terrorizmus e válfaja, bár a történelemben mindig fel-felbukkan, de tömeges mértékben csak a 19. század vége felé jelenik meg, amikor is magányos anarchisták, nihilisták hajtottak végre merényleteket, jellemzően európai országokban. Ezeket a cselekményeket legtöbb esetben a bosszú motiválta, és a hatalmat jelképező személyek ellen irányultak, uralkodók, politikusok, illetve a fennálló hatalmat kiszolgáló prominensek voltak a célpontjaik, akiket az elnyomásukért, rossz életükért felelősnek tartottak, ami révén zavart, félelmet igyekeztek kelteni az elnyomó gépezetben, és ez által meggyengíteni azt.

- Szervezetek, csoportok terrorizmusa

  A különböző titkos és illegális szervezetek, csoportok által megszervezett és kivitelezett terrorcselekmények esetén beszélünk szervezett terrorizmusról. Egy

szervezet terrorcselekmények végrehajtását akkor kezdeményezi, ha kilátástalannak látja az általa képviselt értékrend helyzetét, más eszközökkel érdemi tárgyalásra már nem tudja rábírni a hatalom képviselőit, és így az erőszakos cselekmények révén kívánja elérni jogos, vagy jogosnak vélt követeléseinek teljesítését.

A 20. század folyamán különböző ideológiák mentén terrorcsoportok sokasága alakult ki és működött, megalakulásuk az alábbi vonalak mentén történt:

- Politikai;
- Nemzeti és etnikai;
- Vallási;
- Kiberterrorizmus;
- Egyéb (például a radikális környezetvédők „zöld terrorizmusa", nukleáris, vegyi terrorizmus).

Napjaink világában tetten érhető terrorizmus alapvetően etnikai-vallási indíttatású, legjelentősebb, legveszélyesebb megjelenési formája a globalizálódó iszlamista, dzsihádista terrorizmus, ami a muszlim vallási fundamentalizmushoz kapcsolódik, melynek legismertebb példái lehetnek az al-Kaida és az Iszlám Állam terrorszervezet.

- Államterrorizmus

Amikor egy állam igyekszik a belső vagy külső ellenfeleit erőszakkal, fegyverrel, illetve egyéb eszközökkel megrémiszteni, meghátráltatni, akkor államterrorizmusról beszélhetünk. Az erőszak jellemzően az érintett állam belső ellenségének tekintett, hátrányosan megkülönböztetett csoportok, főként kisebbségként élő nemzetiségek ellen irányul, akik jogaikért küzdenek. Ezt a küzdelmet az állam hatalmának megkérdőjelezéseként, kiváltságai megszüntetésére irányuló törekvésként éli meg, ezért a vele szembehelyezkedők különböző eszközökkel, módszerekkel történő megfélemlítésére törekszik. E típus esetében is fontos ismérv, hogy az adott állam – a terrorcsoportokhoz hasonlóan – saját erőszakos tevékenységét nem tekinti terrorizmusnak, sőt sok esetben épp terrorellenes harcként kommunikálják műveleteiket. Az államterrorizmus fogalma a nemzetközi jog előtt ismeretlen, így fellépni ellene rendkívül körülményes, széleskörű nemzetközi összefogást igényel. [41]

A terrorizmus fogalmát körülírni igyekvő politikai és tudományos próbálkozások rendre megakadnak magán a definíción, azon a kísérleten, hogy a terrorizmust megkülönböztessék a köztörvényes erőszaktól és a harci cselekedetektől. Sok képes arra, hogy összeállítsa a jogi meghatározások tucatnyi tételből álló listáját, majd a végére illessze a sajátját. Az egyik ismert elemzés egy egész fejezetet szentel a kérdésnek, a másik száznál is több definíciót sorakoztat fel, majd azzal zárja a felsorolást, hogy az „adekvát" meghatározás még mindig hiányzik. Hogy miért ez a bizonytalanság? Azért, mert címkézésről van szó. Szinte egyetlen személy, vagy csoport sem nevezte magát önként terroristának. A megnevezést mások – mindenekelőtt az általuk megtámadott államok kormányai – ragasztják rájuk. Erőszakos ellenfeleiket a kormányok sietnek terroristának bélyegezni, főleg azért, mert a fogalom magában hordozza a kriminalitásnak, az embertelenségnek, valamint – mindenekfölött – a tényleges politikai támogatottság hiányának mellékjelentéseit. [42:9]

Fentiekből következik, hogy minden érintett állam a saját történelmének, tapasztalatainak tükrében, saját politikai és társadalmi körülményeinek, olykor pedig szövetségi rendszerekben történő részvétele során megfogalmazódó elvárások függvényében definiálja a terrorizmust. A kormányzatok értelemszerűen igyekeznek olyan jogszabályi környezetet alkotni, mellyel megítélésük szerint leghatékonyabban lehet fellépni a terrorizmus általuk tapasztalt alakja, módja ellen. A kormányzati ideológia legfőbb érve az, hogy az állam a legitim fizikai erőszak monopóliumának birtokosa, így törvényes módon kilátásba helyezheti a fizikai hátrány alkalmazását, és konkrét esetben erőszak alkalmazásával szerezhet érvényt akaratának. [43] Az előző állításból következik, hogy az állam automatikusan törvénytelennek minősíti minden, az államnál kisebb szerveződés – terrorcsoport – ez irányú tevékenységét, és mint olyat igyekszik felszámolni.

A terrorcsoportok szemszögéből viszont levezethető annak a nézőpontnak az igazolhatósága, hogy az állam által törvénytelennek minősített erőszakos cselekedeteik nem igazságtalanok. Ez az ellentmondás pedig megalapozza azt az öröknek tűnő igazságot, hogy „aki az egyik oldalon terrorista, az a másikon oldalon szabadságharcos". Sunil Khilnani, a King's College London politológus professzora szerint a terror pusztán taktika, a véletlenszerű erőszak módszere, amelyet éppúgy használhat egy ámokfutó, mint az állam, azonban napjaink terrorizmusa a modern politikai tevékenység egy elkülönült formája, melyet annak érdekében alkalmaznak, hogy meggyengítse egy állam azon képességébe vetett hitet, hogy állampolgárai

biztonságát szavatolni tudja. Ebben a megfogalmazásban rejlő igazság vissza is tükröződik a különböző államok által megfogalmazott terrorizmus-definíciókban.

A különböző, ámde nyugati értékrenddel bíró országok terror definícióit áttekintve észrevehetjük, hogy azok nagyfokú eltérést nem mutatnak, ugyanazon logika szerint vezetik le maguk definíciót.
A terrorizmus elleni nemzetközi harc legmarkánsabb képviselőjének, az Egyesült Államoknak a Szövetségi Törvénykönyve szerint „a terrorizmus az erő vagy erőszak törvénytelen alkalmazása a kormányzat, a polgári lakosság vagy azok bármely csoportja ellen, valamilyen politikai vagy társadalmi cél elérése érdekében". [44] Az Egyesült Államok Büntetőtörvénykönyvének bűncselekményekre és büntetőeljárásokra vonatkozó 18. fejezete ennél már jóval részletesebben határozza meg a terrorizmus fogalmát:

Erőszakos vagy emberi életet veszélyeztető (…) cselekmények (…), melyek láthatólag azzal a szándékkal kerülnek végrehajtásra, hogy:

I. megfélemlítsék vagy valamire kényszerítsék a polgári lakosságot;
II. megfélemlítés vagy kényszerítés által befolyásolják egy kormány politikáját;
III. tömegpusztítás, merénylet, vagy emberrablás végrehajtásával hassanak egy kormány tevékenységére. [45]

Az Egyesült Államok jogrendjét áttekintve megállapíthatjuk, hogy számos kormányzati szervezet és jogszabály (Védelmi Minisztérium, Szövetségi Katasztrófavédelmi Szolgálat, Nemzeti Terrorelhárító-központ, Nemzetbiztonsági Stratégia, Hazafias Törvény, Terrorizmus Elleni Biztosításról Szóló Törvény) önállóan definiálja a terrorizmus fogalmát, azonban ezek gyakorlatilag a fentebb részletezett törvényi definíciók a specifikus területre vetített átiratai.

Az Európai Unió jogi, illetve hivatalos célra a 2002-es, a terrorizmus elleni küzdelemről szóló tanácsi kerethatározatában definiálta a terrorizmust. A meghatározás szerint elsősorban azok a súlyos személy- és vagyon elleni bűncselekmények minősülnek terrorcselekményeknek, „amelyek az elkövetés módja vagy összefüggéseik folytán egy államot vagy nemzetközi szervezetet komolyan károsíthatnak, ha azokat azzal a céllal követik el, hogy:

- a lakosságot komolyan megfélemlítsék;
- állami szervet vagy nemzetközi szervezetet jogellenesen arra kényszerítsenek, hogy valamely intézkedést megtegyen, vagy épp ne tegyen meg;

- egy állam vagy nemzetközi szervezet alapvető politikai, alkotmányos, gazdasági vagy társadalmi rendjét súlyosan megzavarják vagy lerombolják". [46]

Az Országgyűlés – igazodva a globális terrorizmus elleni harc keretében támasztott nemzetközi elvárásokhoz – 2012-ben a Büntető Törvénykönyv módosításakor definiálta újra a terrorizmust, és határozta meg azokat a magatartásformákat, elkövetési módokat, melyek révén megvalósítható egy terrorcselekmény [47]:

Aki abból a célból, hogy

a) állami szervet, más államot vagy nemzetközi szervezetet arra kényszerítsen, hogy valamit tegyen, ne tegyen vagy eltűrjön,
b) a lakosságot megfélemlítse,
c) más állam alkotmányos, társadalmi vagy gazdasági rendjét megváltoztassa vagy megzavarja, illetve nemzetközi szervezet működését megzavarja,

(…) információs rendszer vagy adat elleni erőszakos, közveszélyt okozó vagy fegyverrel kapcsolatos bűncselekményt követ el.

A Büntető Törvénykönyv továbbá rendelkezik arról is, hogy aki terrorcselekmény elkövetésével fenyeget, vagy aki terrorcselekmény elkövetésére felhív, ajánlkozik, vállalkozik, a közös elkövetésben megállapodik, vagy az elkövetés elősegítése céljából az ehhez szükséges vagy ezt könnyítő feltételeket biztosítja szintén bűncselekményt követ el.

A jogszabály ugyanakkor rendelkezik még a terrorcselekmények finanszírozásának szankcionálásáról is, mivel kimondja, hogy aki terrorcselekmény feltételeinek biztosításához anyagi eszközt szolgáltat vagy gyűjt, vagy terrorcselekmény elkövetésére készülő személyt vagy rá tekintettel mást anyagi eszközzel támogat.

A magyar szabályozás definícióit vizsgálva megállapítható, hogy azok fő irányukat tekintve követik az ország szövetségi rendszereiben lévő más tagországok leiratait, azonban ezeken túlmenően azokat a konkrét jogellenes magatartási formákat is meghatározza, amelyeket a megfelelő szándékkal végrehajtva – az alapbűncselekményen túl – magát a terrorcselekményt is megvalósítják.

A nyugati kultúrkör terrorizmus definícióinak vizsgálatakor azonban kitűnik az a törekvés, hogy a politikusok, a különböző intézmények, illetve a jogalkotók igyekeznek olyan általános tényállásokat megfogalmazni, mely mögé egy adott cselekmény bekategorizálható, azonban ez sok esetben nem vezet célra, mivel a terrorcselekmény nem egy konkrét cselekmény,

cselekménysorozat végrehajtása révén valósul meg, hanem az az mögött meghúzódó – jellemzően vallási vagy politikai – szándék teszi azzá.

Sok esetben párhuzamot lehet vonni a terrorizmus és háború között. Egyértelmű, hogy terrorista akciók egy része – emberrablások, merényletek, repülőgép-eltérítések – nem, vagy csak különleges esetekben jelenik meg a hagyományos katonai hadviselés repertoárjában. A háború és a terror hasonlóságai nyilvánvalóak, mivel nehéz elképzelni olyan háborút, amely nem kelt félelmet a lakosságban, nem az ellenséges ország kormányát akarja befolyásolni, és ez gyakran nemcsak az erőszak mellékhatása, hanem az egyik elsődleges cél. A történelem során az elfoglalt területek lakosságát egyebek mellett azért fosztották és irtották ki, hogy megfélemlítsék más városok, erődítések fegyveres és fegyvertelen lakosságát, ezzel törve meg ellenállásukat annak érdekében, hogy az elhúzódó harcokat a támadó elkerülje. [42:12]

A terrorizmusra sok elemző az aszimmetrikus hadviselés egy formájaként tekint, azonban ez a gondolatmenet alapvetően hibás. A katonai és a nemzetbiztonsági területeken értelmezve az aszimmetria gyakorlatilag, a szembenálló féltől eltérő cselekvési változatokat (műveleteket), szervezeteket, és gondolkodási módot képvisel, abból a célból, hogy maximalizálja a saját előnyeit, és kiaknázza az ellenség gyengeségeit, valamint megragadja a kezdeményezést, vagy nagyobb cselekvési szabadságot nyerjen. Az aszimmetria lehet politikai, diplomáciai, vagy katonai stratégia, illetve ezek kombinációja is. [48] A definícióból levezethető, hogy a terrorizmus és a jellemzően a gerilla-hadviseléssel vont párhuzam alapvetően téves, bár egyik „módszer” sem vállalja a hosszas nyílt konfrontációt, ütközetet az elnyomóként azonosított erőkkel, azonban a gerilla-hadviselés esetében – noha az nem felel meg a reguláris hadviselés kritériumainak – a hagyományos katonai logika mindenképp felfedezhető az ellenség irányába végrehajtott műveletek mögött. [49] Ezzel szemben a terrorizmus – ami nem vállalja fel a nyílt összecsapást – igyekszik célpontjait úgy kiválasztani, a műveleteiket olyan módszerekkel végrehajtani és úgy időzíteni, hogy a megtámadott fél részéről kizárja a védekezés lehetőségét. A gerilla-hadműveletekkel szemben a terrorcselekmények egyik fontos jellemzője, hogy nem csak az elnyomónak tekintett erők ellen hajt végre műveleteket, hanem véletlennek tűnő helyszíneken, harcuk szempontjából semleges célpontok ellen is végrehajt támadásokat.

A terrorizmus elleni hosszú távú, hatékony védekezés érdekében elengedhetetlenül fontos megjósolni annak várható fejlődését, azonban ezt számos körülmény nehezíti. A témában

készült prognózisok alapvetően két tematika köré épülnek, az egyik kifejezetten a terrorizmus várható alakulásával, minőségének, jellegének módosulásával, a másik a nemzeti és/vagy a nemzetközi terrorizmus jövőjét közvetve befolyásoló feltételrendszerrel – társadalmi, politikai, civilizációs, gazdasági, etnikai, vallási, természeti, környezeti, stb. változásokkal – kapcsolatos, azonban valamennyi előrejelzés a nemzetközi terrorizmus globalizálódását, a terrorszervezetek irányításának virtuálissá válását, eszköz- és módszertárának folyamatos megújulását jelzi. [50]

A terrorizmus jövőjével foglalkozó elemzések szinte mindegyikében szó esik arról, illetve prognosztizálják azt, hogy XXI. század exponenciálisan fejlődő tudományágainak vívmányait a terroristák – a korábbi gyakorlathoz hasonlóan – igyekeznek majd „repertoárjukba" bevonni, a pusztítás és a megfélemlítés szolgálatába állítani. Ennek tükrében pedig a terroristák eszközrendszerében a közeli jövőben várhatóan fel fognak bukkanni a biológia (például a génmanipulált vírusokból előállított biológiai fegyverek), a kémia (vegyi fegyverek) és a műszaki tudományok – ezen belül pedig az elektronika, az informatika és a kommunikáció – legújabb eredményei. Ámde ez utóbbiak azok a tudományágak, melyek eszközeivel, megoldásaival a társadalom tagjai legtöbbször találkoznak, mely magánéletüket, interperszonális kapcsolataikat, munkájukat és létüket legjobban átszövik, ezért a jövő hadviselésének színtere szűkebb értelemben az információs szupersztráda, maga az Internet, tágabb értelemben pedig az információs tér, illetve annak szűkebb szelete, a kibertér lesz.

II. 2. A kiberterrorizmus értelmezése, definíciói

A médiában egyre több hírben esik szó a különböző okokból, különböző módon és módszerrel végrehajtott terrortámadásokról, illetve azok elkövetőiről. Napjainkban ezen akciók döntő hányada még a „hagyományos" fizikai térben, „szokványos" módon kivitelezett támadás, azonban egyre nagyobb részben jelennek meg olyan hírek, melyek mögé tekintve riasztó perspektívák rajzolódnak ki a terrorizmus várható fejlődésében. E fejlődésnek talán egyik legbeszédesebb, legtöbbször idézett, Frank Cillufotól az USA Belbiztonsági Minisztériumának munkatársától származó leírása a „Míg Bin Laden ujja egy AK 47-es ravaszán van, addig unokaöccséé egy számítógépes egéren." mottó, melyben jól körvonalazódik a terrorizmusban várható generációváltás, illetve annak iránya. [51] [52]

Míg a politika, illetve annak változása főleg a terrorizmus ideológiájára van kihatással, addig a technikai-technológiai fejlődés a terrorcselekmények végrehajtásának módjában és részben a célpont-kiválasztásában érhető nyomon. Minden műszaki vívmány, elterjedő, elérhető technológia szinte azonnal megjelenik a terrorista módszerek tárházában is, ezért a jelenség vizsgálatakor szükséges azt is elemezni, hogy a technikai-technológiai fejlődés miként befolyásolja terrorizmus módszereit és milyen hatással van az elkövetők személyi körének összetételére. Napjainkban az infokommunikációs eszközök és technológiák térhódításának lehetünk tanúi, és az ezekből adódó új lehetőségek már meg is jelentek a terroristák repertoárjában.

A társadalmat, illetve annak tagjait fenyegetni, félelemben tartani pedig több féle módon lehet. Szinte evidens, hogy korunk információs társadalmára legnagyobb hatással az annak zavartalan működését biztosító információs rendszereken keresztül lehet elérni, és tekintettel arra, hogy napjainkban minden infrastruktúra működését információs alrendszerek támogatásával végzik, a fenti állítás fokozottan igaz. A kiberterrorizmusnak – annak okán, hogy viszonylag új jelenségről beszélünk – még nincs kiforrott, az információtechnológiai szakterület által egységesen elfogadott definíciója, azonban a szakirodalom tanulmányozása során két meghatározás körvonalazódik, melyet az amerikai FBI, illetve Kevin Coleman biztonsági szakértő fogalmazott meg.
Az FBI szerint "a kiberterrorizmus egy erőszakba torkolló, szolgáltatásokat megzavaró és/vagy megsemmisítő, számítógépekkel és telekommunikációs eszközökkel elkövetett bűncselekmény, amely zavar- és bizonytalanságérzet keltés révén félelmet gerjeszt egy adott populációban azzal a céllal, hogy a kormányt vagy a lakosságot egy konkrét politikai, társadalmi vagy ideológiai állásponttal való azonosulásra bírja".
Coleman meglátása szerint viszont a "számítógépek és/vagy hálózatok ellen ártó szándékkal, illetve társadalmi, ideológiai, vallási, politikai vagy hasonló célok elősegítése céljából történő zavaró akciók előre megfontolt végrehajtása, illetve mások ilyen célok előremozdításától való eltántorítása" jelenti a kiberterrorizmust. [53]

A 2018-as RSA Conference elnevezésű, nemzetközi kiberbiztonsági rendezvény kiadványában a kiberterrorizmust oly módon definiálják, hogy „kiberképességek használata a bomlasztó, romboló és pusztító katonai jellegű műveletek során a kibertérben, hogy a félelem és az erőszak fenyegetésével politikai változásokat érjenek el”. [54]

A tallini NATO Kibervédelmi Kiválósági Központ fogalomjegyzékének kiberterrorizmusra vonatkozó részében a különböző országok definícióit tanulmányozva megállapítható, hogy a jelenségre még nincs olyan körülhatárolt „tevékenységlista", vagy ismertetőjegy, mely az egységes fogalom megalkotásának irányába mutatna. A különböző definíciók terjedelmükben jelentős mértékben eltérnek egymástól, szemléletmódjuk is sok esetben különbözik, azonban az egyetlen közös vonás, hogy a terrorizmus, vagy annak fő motívumai (például a félelemkeltés) mindig megjelennek. Ugyanakkor a kibertér számos definícióban meg sem jelenik, csak áttételesen utalnak arra, hogy a jogellenes cselekményeket e dimenzióban értelmezik (például internet, hálózatok, számítógépek).

A leghosszabb, osztrák definíció szerint „A számítógépes terrorizmus az állam és/vagy nem állami szereplők politikai indíttatású bűncselekménye számítógépek, hálózatok és a bennük tárolt információk ellen. Célja a közélet súlyos vagy hosszú távú megzavarása, a gazdasági tevékenység súlyos károsítása, a lakosság megfélemlítése, illetve az állam vagy nemzetközi szervezet politikai, alkotmányos, gazdasági vagy társadalmi alapjainak mélyreható megzavarása vagy megsemmisítése, továbbá hatóságok vagy nemzetközi szervezetek kényszerítése annak érdekében, hogy bizonyos cselekményeket végrehajtsanak, eltűrjenek. Ezek a cselekedetek a politikai-fundamentalista csoportok vagy az egyéni elkövetők által okozott szervezett számítógépes szabotázsok révén valósítják meg."

A legrövidebb, lengyel megfogalmazás pedig „a kibertérben elkövetett terrorista természetű bűncselekményként" hivatkozik a kiberterrorizmusra.

A magyar definíciók legtöbbjét az a leírás foglalhatja össze, miszerint a kiberterrorizmus előre megfontolt, megtervezett, politikailag motivált erőszakos cselekmény, melyet nem háborúban, különböző jellegű célpontok (civil lakosság, hadsereg, politikai és gazdasági rendszerek, egyes objektumok) ellen, a célpontok által telepített számítógépeken, különböző hálózatokon keresztül hajtanak végre. [55]

Azonban ha mélyrehatóan vizsgáljuk a terrorcsoportok kiberteret érintő aktivitását, akkor látható, hogy a fenti definiciók önmagukban nem fedik le teljes mértékben a jelenséget, mivel vagy túl általánosan fogalmaznak, vagy csak egy-egy tevékenységtípusra vannak kihegyezve. Egyes megközelítések arra helyezik a hangsúlyt, hogy a kiberterrorizmus az informatikai eszközökkel végrehajtott terrortámadás, más definíciók pedig arra, hogy ezek az eszközök a

célpontjai a támadásnak, továbbá a megfogalmazások nem térnek ki a terrorizmus kísérőjelenségeire (propaganda, finanszírozás, toborzás, stb.) sem. Meglátásom szerint a különböző definíciótípusok egyesítése, további kibővítése lehet a pontos leírása a jelenségnek.

II. 4. Kiberterroristává válás

A kibertérben végrehajtott bűn- vagy terrorcselekmények esetében a tudósításokban, illetve kommentárokban az elkövetőket sokszor "közönséges" bűnözőként, terroristaként állítják be, azonban e személyek a társadalomban kialakult sztereotípiáktól eléggé távol állnak. Rendészeti szemlélettel a nyilatkozat mögé tekintve valóban igazolható, hogy a terroristák – főleg eszközcselekményként – elkövetnek olyan bűncselekményeket, melyek egyébként a szervezett bűnözés kategóriájába sorolhatók (embercsempészet, gépjárműlopás, illegális kábítószer-kereskedelem, emberrablás, pénzmosás stb.). A szervezeti hasonlóság is igen meggyőző módon igazolható, amennyiben összehasonlító elemzésnek vetjük alá a magyar büntetőtörvénykönyv bűnszervezetre és terrorszervezetre vonatkozó meghatározásait:

Terrorista csoport	**Bűnszervezet**
három vagy több személyből áll	három vagy több személyből áll
hosszabb időre szervezett	hosszabb időre szervezett
összehangoltan működő	összehangoltan működő
csoport	csoport
állam, nemzetközi szervezet kényszerítése, alkotmányos, társadalmi, gazdasági rend megzavarása, erőszakos megváltoztatása, lakosság megfélemlítése, személyek elleni erőszak alkalmazása, jelentős anyagi javak hatalomba kerítése, ezen célok eléréséért más meghatározott bűncselekmények elkövetése céljából	célja ötévi vagy azt meghaladó szabadságvesztéssel büntethető szándékos bűncselekmények elkövetése

Az eltérés tehát nem módszereikben, még csak nem is feltétlenül szervezeti felépítésükben, sokkal inkább okaikban, céljaikban és motívumaikban keresendő. [56]

A számítógépes bűnözők – tartva a következményektől – cselekményeiket igyekeznek titokban tartani, addig a kiberterroristák – a terrorizmus lényegéből fakadóan – igyekeznek "eredményeiket" minél szélesebb körben ismertté tenni. Bár az alkalmazott eszközök mindkét kör esetében megegyeznek – vagy legalább nagy átfedést mutatnak – ám a motivációik és céljaik jelentősen eltérnek. Míg a bűnözők és az ipari kémek túlnyomórészt anyagi haszonszerzés végett főleg a gazdasági (pénzintézeti) és a nagyvállalati (ipari) rendszereket támadják főként diszkrét módon, addig a terroristák transzparens formában zavar- és félelemkeltés érdekében rombolják, befolyásolják a kommunikációs, hírközlési, közlekedési és közműhálózatokat, konfliktusok idején pedig az ellenük felvonultatott rendvédelmi erők kommunikációját akadályozzák.

Az alkalmazott eszközök átfedéséből adódóan közös momentum, hogy a kibertérben végrehajtott bűn- és terrorcselekmények kitervelői, elkövetői – mint már utaltunk rá – rendkívül nagy szaktudással, általában felsőfokú végzettséggel rendelkeznek, akár rejtett, akár transzparens műveleteiket rendkívüli körültekintéssel tervezik meg és akár hónapokon át nagy türelemmel, fegyelemmel irányítják, amely során a részeredmények, valamint a pozitív és negatív tapasztalatok ismeretében módszerekeit finomítják.
Általában fiatal, magasan képzett, magas intelligenciájú, számítógépes szakemberek, akik nem ritkán 2-3 fős csoportokba szerveződve követik el a bűncselekményeket a globalizáció és a technika, elsősorban az Internet felhasználásával. Az esetek többségében sokoldalúan szocializált elkövetőkről beszélhetünk, akik tisztában vannak a jogaikkal, akik szakképzettségük miatt jellemzően jó egzisztenciális körülmények között élnek. [57] Ők tekinthetők a kiberterrorizmus felső kasztjának, a legveszélyesebb rétegének, mivel bár tetteik motivációja mögött értelemszerűen különböző okokból gerjesztett indulatok állnak, azonban meggondolatlan indulatkitörések helyett alaposan megtervezett döntéseket tudnak hozni, aminek során képesek a rendelkezésre álló erőforrásaikat, a célpont védelmi hiányosságait, az ésszerűen elérhető célt és természetesen a biztonsági intézkedéseiket optimalizálni. Képzettségük, tájékozottságuk okán tisztában vannak azzal, hogy tevékenységüket a jog miként minősíti, így akár arra is felkészülhetnek, hogy a konkrét terrorcselekményt alsóbb kasztokhoz tartozó, általában tájékozatlanabb, képzetlenebb és sok esetben indulatoktól erősen vezérelt személyek révén – akár azok tudta – hajtsák végre.

Ha külön kasztként nem is, de a felső kaszt egyfajta részeként megemlíthetők azok az elkövetők (legtöbb esetben alkalmazottak), akik közvetve jelentenek veszélyt, valamely

motiváció miatt a birtokukban lévő, az infrastruktúrára (annak egészére, részére, sérülékenységeire, stb.) vonatkozó érzékeny információkat jogellenesen felhasználják, közzéteszik, kiszivárogtatják, eladják, aminek révén veszélyeztetik annak biztonságát, rontják működésének hatékonyságát.

Másodlagos kasztnak azok az egyének tekinthetők, akik kiemelkedő informatikai tudással nem rendelkeznek, azonban azonosulva a terroristák céljaival, autodidakta módon fejlesztve magukat, vagy a felső kaszt által készített szoftvereszközökkel és azok iránymutatásával részt vesznek a támadások végrehajtásában, vagy azok előkészítésében. E kaszt esetében tipikus támadási forma a szolgáltatás-megtagadásos (DoS, DDoS) támadás, azonban számos olyan módszer is létezik és elérhető számukra, amikor a támadás eszközei a közforgalmú kereskedelemben is elérhető berendezésekkel, vagy azok módosításaival, vagy épp otthonukban megalkotható eszközökkel végrehajthatók, így e kaszt részéről számos eredménytelen, és kisebb-nagyobb zavart okozó próbálgatás várható.

A harmadik kasztba azok a személyek (troll-ok) sorolhatók, akik gyakorlatilag informatikai előképzettség nélkül – hirtelen felindulásból, ötlet- vagy kampányszerűen – kísérletezgetnek különböző rendszerek feltörésével.

A kibertérben elkövetett terrorcselekmények elemzése során is szükséges megvizsgálni, hogy kik lehetnek ezek kitervelői, végrehajtói, milyen úton jutottak el cselekményük végrehajtásáig. A kriminalisztikának széles területe foglalkozik a bűnözővé válás szociológiai hátterével, azzal a folyamattal, amelynek eredményeképp az egyén áthágja azokat a szociális magatartásformákat, normákat, értékeket, attitűdöket, melyek segítségével társadalmilag integrált személlyé vált.
A társadalmon belül társadalmi intézmények, szervezetek alakulnak, de az elsőleges társadalmi intézmény a család. A család az egyén és a társadalom közötti közvetítő kiscsoport; a családba a gyermek beleszületik, vagy bekerül, s a családon belüli intim viszonyok járulnak hozzá a testi és lelki védelemhez. A család tagjai egymással akár napi rendszerességgel, az életvitelüket alapjaiban is meghatározó kapcsolatban állnak egymással; a kölcsönös egymásra utaltságból következik, hogy a családtagok egymással többféle funkciót is betöltő, teljesítő ellátó és gondoskodó rendszert alkotnak. A család egy struktúra, egy rendszer, melynek vannak alrendszerei. Tehát az egyén viselkedésének, aktuális reagálásainak eredője messziről, a családból, illetve a neveléséből vezethető le. [58] Az egyén egész

életében részt vesz mikro-, és makroszociális csoportok életében, melyek vagy pozitív, vagy negatív hatással vannak rá. A gyermek az identifikáció során érzelmileg a hozzá közel álló személyekhez kötődik leginkább, azaz elsősorban a szüleihez, családjához, de később e személyek köre kibővül, és mindannyian más-más mértékben, és más formában hatnak az egyéniség, a viselkedésrepertoár és a szociális értékrendszer kialakulására.

A generációk tanulmányozása során megállapítható, hogy egy néhány évtizeddel ezelőtt a család ráható ereje erősebb volt az egyéniség kialakulásában, mint napjainkban, az információs társadalom korában. Jelenleg egyre jobban háttérbe szorulóban van a szülők által gyakorolt követendő pozitív minta, melynek okai lehetnek a csonkacsaládok nagy száma, a szülők folyamatos időhiánya, melyet a gyermekük nevelésére fordítanak. Az egyéniség kialakulását gyermek- vagy fiatalkorban nagymértékben befolyásolják különböző – akár virtuális, kibertérben létező – társaságok, csoportok ráható ereje, így terrorcsoportok propagandája is, mely idővel szinte fel is váltja az elsődleges szociális színtért, a családot. Ezt a tendenciát erősíti, hogy a fiatalok a kibertéren keresztül folyamatosan kapcsolatban vannak egymással, és így a család esetleges közvetlen formáló ereje már az otthonokban is csökken.

A kamasz fiatalok - életkorukra való tekintettel -, az adaptív kockázatkeresés korszakában vannak, amit az evolúciós pszichológia „fiatal férfi szindrómának” nevez. Az „együttes élmény” hiánya a szülővel, vagy barátokkal, fokozza a magány, a depresszió, az unalom érzését, ami növeli az internet függőség – így a virtuális térből érkező fenyegetésekre való fogékonyság – kockázatát. Lehetnek olyan időszakok ebben a korban, amikor valamilyen érzelmi, hangulati vagy impulzus-kontroll probléma miatt erős függőséget mutat egy fiatal, vágyik felfedezni önmagát, elkívánkozik a szülői felügyelet alól, és a családon kívül – a kibertérben (is) – keres és talál új kapcsolatokat. A névtelenség látszata alatt szívesen vállal kockázatot anélkül, hogy teljesen tisztában lenne a lehetséges következményekkel. Aggodalomra ad okot, hogy az interneten elérhető tengernyi információ - számtalan eset mutatja - csak súlyosbítja a fiatalok aggodalmait személyes problémáikkal kapcsolatban. [59]

Korai életszakaszokban a bűnelkövetés – kiberteret érintően is – jellemzően csoportokban történik, és elsődlegesen vagyon elleni bűncselekmények kerülnek előtérbe, mely jelenségnek több oka is van. Szerepet játszik a csoport ráható ereje, az egyén helye a csoporton belül, a kiforratlan személyiség, az unalom, vagy épp a kalandvágy. Későbbi életszakaszokban pedig az életkörülményekben bekövetkező változás, mint például a munkanélküliség, a nélkülözés

okozza azt, hogy valaki a bűnözés útjára lépjen, mivel úgy véli, hogy ez az egyetlen lehetősége arra, hogy életszínvonalát (például a tulajdonában lévő ingatlant megtartsa), vagy a családnak anyagi javakat biztosítson. [60] Kibertérben elkövetett terrorcselekményekre sarkalhatja a fiatalokat az a körülmény is, hogy a kibertér által biztosított anonimitásban egy félénk, gyenge testalkatú, elismerésre vágyó fiatal a virtuális térben – kellő magabiztossággal, agresszióval végrehajtott „stiklikkel" – akár egy csoport irányítója is lehet.

Napjainkban a tudomány egyre jobban fejlődik, mely jelenség megköveteli az oktatástól is, hogy lépést tartson vele, így egyre nagyobb hangsúly helyeződik az informatikára, melyhez a tanulók nagy része érdeklődéssel fordul. Ennek egyik oka, hogy az otthonában érzelmileg és fizikálisan elhanyagolt – akár jó, akár rossz szociális körülmények között élő – de unatkozó, kíváncsi gyermek, fiatal felnőtt számára kinyílik a tér az internet által. Részese lehet olyan kalandoknak, virtuális világoknak, mely a valós életéből hiányzik, tartozhat valahová a különféle közösségi oldalak révén. Szocializálódás folyamatában felerősödött a társaság szerepe, a bandába verődés, a galerik kialakulása, ugyanakkor megváltozik az elkövetett bűncselekmények jellege is.
Fontos tényező a kiberterrorizmus szempontjából, hogy a fiatalok az iskolában már akár ötleteket is kaphatnak egy-egy támadás, vagy egyéb módszer megvalósításához, továbbá az elkövetés eszköze, a számítógép mindenki számára elérhető.

További probléma, hogy számos szülők nem ért az informatikához, nem ismerik fel az abban rejlő veszélyeket, vagy ha vannak is elképzeléseik erről, akkor ezt hajlandóak elbagatellizálni, és inkább örülnek annak, hogy gyermekük a közelükben, vigyázó szemük előtt van, és nem az utcán „csatangol", „bandázik", holott a virtuális tér galerijei legalább ugyanannyira veszélyesek.

A fentieken túl meg kell említeni egy másik tényezőt is, mely bűnelkövetésre ösztönözheti az egyént. Ezek pedig azok a speciális helyzetek, melyek speciális viselkedésmódokat eredményeznek, és a magas kriminális potenciállal rendelkező személy egy kialakult szituációban hozhat olyan döntést, mely bűnelkövetést eredményez (például sértett alkalmazott). A kiberterroristák esetében itt külön kiemelhető momentum az egyén saját magát, vagy általa fontosnak tartott személyt, csoportot, vagy egyéb szimbólumot ért vélt vagy valós sérelemre történő megtorló jellegű reagálás, egyfajta igazságosztás, bosszú.

Hangsúlyozandó körülmény, hogy a kibertérben végrehajtott jogellenes cselekmények esetében az elkövetők hajlandóak tetteik súlyát elbagatellizálni, azt nem tekintik valódi, köztörvényes bűn-, vagy terrorcselekménynek. További bátorítást adhat számukra az is, hogy az anonimitást garantáló megoldások miatt biztosak lehetnek abban, hogy kilétük nagy valószínűséggel ismeretlen marad.

Kiberterrorizmus esetében – a jogellenes cselekmény speciális körülményeire tekintettel – a bűnelkövetők nem a társadalom alsóbb rétegeiből kerülnek ki, mivel az ehhez szükséges, általában a felsőoktatásban megszerezhető szaktudás és értékes high-tech eszközrendszerek jellemzően a középosztályhoz, illetve az attól magasabb társadalmi csoportokba tartozó fiatalok számára elérhetők, akik érdeklődésük és/vagy különleges szakértelmük birtokában akár specializálódhatnak is a különböző módszerekre, célpontokra (például hacker-ek, cracker-ek, phreak-ek, hacktivisták).

Tehát a specializálódás nagyban függ egyrészt az egyén személyiségjellemzőitől, melynek eredője determinálja azt, hogy milyen módszereket fog preferálni. A hevesebb, türelmetlenebb egyének hirtelen, indulatból reagálnak, akikhez így a transzparens, hacktivista jellegű cselekmények, vagy akár a fizikai pusztítás állnak közelebb, míg a zárkózottabb, aprólékosabb, türelmesebb egyének az átgondoltabb, lassabb, aprólékosan megtervezett akciókat (például támadókódok kifejlesztését, információk gyűjtését, csalások lebonyolítását, stb.) részesítik előnyben. A specializálódás másrészt pedig függ az őt befogadó csoportok világnézetétől, radikalizálódásának mértékétől, a csoport tagjainak iskolázottságától, végzettségeik típusától is. Például egy környezetvédelem köré szerveződő csoport tagjait – személyiségjegyeiktől függően – könnyen lehet radikalizálni egy természetkárosítás kapcsán gyanúba keveredett nagyvállalat ellen, amikor is tagok egyéni képességeik, motiváltságuk, elköteleződésük mértékében vonódnak be a jogellenes cselekménybe.

II. 5. Összegzés, részkövetkeztetések

Mint ahogy látható a történelemben a terrorizmus az emberiséggel egyidős, célja mit sem változott, ugyanakkor az adott kor által képviselt technikai színvonal, az új műszaki megoldásai mindig megjelentek a terrorizmus eszköztárában. Ez a momentum a XXI. században sem változott, így a kor egyik legdinamikusabban fejlődő tudományága, az infokommunikáció vívmányai is belekerültek a terrorizmus repertoárjába. Ugyanakkor új

jelenségként tűnik fel, hogy az információs infrastruktúrákra és szolgáltatásaikra már nem csak célpontként tekintenek, hanem eszközként is felhasználják őket, illetve célpontként tekintenek a rendszerekben kezelt információkra is, mint a terror eszközeként.

A terrorizmust általánosságban, illetve a kiberterrorizmust a különböző definíciók – az információhoz hasonlóan – sokrétűen írják le, mivel más-más szempontok alapján értelmezik. A megfogalmazást nehezíti, hogy a műszaki, technológiai fejlődés révén szinte naponta újabb és újabb megoldások, eszközök, módszerek jelennek meg az infokommunikáció szakterületén, így e képlékenység nem könnyíti meg a definiálást.
A jogi meghatározás is hasonló nehézségekkel küzd, mivel a rohamos technikai fejlődéssel a jogszabályalkotás sok esetben – különböző okok miatt – nem tud lépést tartani. A terrorizmussal kapcsolatos jogszabályok országonként eltérnek, mivel az államok saját tapasztalataikat, belső problémáikat, politikai állásfoglalásukat is „beleszövik" a megfogalmazásokba, de az érezhető, hogy a különböző szövetségi rendszerek tagállamai jogszabályaikat – a közös értelmezés és együttműködés megkönnyítése érdekében – nagyvonalakban „összehangolják".

A szociológiai vizsgálatok tükrében megállapítható, hogy egy egyén kiberterroristává válásának oka többrétű. Fontos az, hogy milyen magatartási mintákat közvetítettek felé a család és az őt befogadó csoportok élete folyamán, valamint hogy milyen speciális hatások és milyen gyakorisággal érték személyét, továbbá hogy informatikai szaktudásának birtokában erre miként reagál, ami végeredményben meghatározza a kiber-terrorcselekményekre vonatkozó támadópotenciálját is. Leszűrhető az, hogy az egyén személyiségjegyei és képességei inkább a módszert határozzák meg, míg csoporttagságai, illetve az őt, valamint az őt befogadó csoportokat ért hatások pedig a célpontokat határozzák meg. A kiberterroristává válást további speciális körülmények is segíthetik, úgymint a „büntetlenül" elérhető szaktudás és birtokolható eszközök, a nagyfokú anonimitás, a következmények elvontsága, veszélyérzet hiánya, a szinte korlátlan próbálkozások lehetősége.

Prognosztizálható, hogy a műszaki-technológiai fejlődésből adódóan a terrorizmus elleni harchoz újabb fegyverek, egyre újabb védelmi rendszerek, valamint új megközelítésű hírszerző-technológiák kifejlesztése lesz szükséges, mivel a civil lakosság körében elvegyülő, fegyverekkel, robbanóeszközökkel, akár tömegpusztító eszközökkel, valamint kiber-támadóképességekkel is rendelkező – olykor csak „alkalmi" – terroristák kiszűrése újszerű

kihívás elé fogja állítani a katonai, a rendvédelmi és a biztonsági szerveket. Ebből következik, hogy az érintett szervek számára rendkívül fontos az, hogy a kibertér új dimenzióiban is képesek legyenek a különböző fenyegetéseket azonosítani és azok elhárításához szükséges képességeket minden dimenzióban (például humánerőforrások, finanszírozás, technológiai, stb.) megszerezni, a műszaki fejlődéssel és a társadalmi változásokkal összhangban szinten tartani.

Ehhez azonban azonosítani és tanulmányozni kell az infrastruktúrákra fenyegetést jelentő támadókat, vizsgálni azokat a motivációkat, melyek jogellenes cselekményekre sarkallhatják a kiberterroristákat, mivel ezen ismeretek birtokában, ha csak közelítő pontossággal is, de becsülni lehet képességeiket, ennek tükrében pedig azt a veszélyt, amit az infrastruktúrákra jelentenek. Akár egy kibertérben, vagy akár egy „hagyományos" térben működő terrorcsoport motivációnak vizsgálata, képességeinek kutatása segíthet annak prognosztizálásában, hogy egy-egy információs infrastruktúra vonatkozásában a kibertéren keresztül milyen támadási módszert használnak.

III. A kiberterrorizmus módszerei

A terrorizmussal kapcsolatos, korábban már bemutatott törvényi meghatározások és definíciók között a célok mellett markánsan megjelennek azok a tevékenységi körök, melyek a jogellenes cselekményt képezik. Ezek a végrehajtáson túl még a terrorcselekmények támogatása, illetve finanszírozása.

Ezt a felosztás a hazai Büntető Törvénykönyvben is tetten érhető:

- végrehajtás: „(…) erőszakos, közveszélyt okozó vagy fegyverrel kapcsolatos bűncselekményt követ el.
- támogatás: „(…) terrorcselekmény elkövetésével fenyeget, vagy aki terrorcselekmény elkövetésére felhív, ajánlkozik, vállalkozik, a közös elkövetésben megállapodik, vagy az elkövetés elősegítése céljából az ehhez szükséges vagy ezt könnyítő feltételeket biztosítja”.
- finanszírozás: „(…) terrorcselekmény feltételeinek biztosításához anyagi eszközt szolgáltat vagy gyűjt, vagy terrorcselekmény elkövetésére készülő személyt vagy rá tekintettel mást anyagi eszközzel támogat”.

A fenti felosztást azonban szükséges a kiberterrorizmus vonatkozásában is értelmezni, hogy melyek azok a kibertérben értelmezhető cselekmények, melyek a fenti kategóriába besorolhatók, melyek felbukkanása, megléte esetén következtetni lehet a kiberterrorizmus valamely aspektusának megjelenésére. A különböző tevékenységek, módszerek kategóriákba történő besorolása indokolt a kiberterrorizmus elleni felderítő és védelmi intézkedések szempontjából is, mivel egy-egy módszer ellen más-más típusú felderítő és elhárító módszerek – szervezetek, szakemberek és eszközök – alkalmazása szükséges.

A jogalkalmazás szempontjából is indokolt lehet a felosztás, mivel ez (például nyomozati vagy bírósági szakaszban) segíthet azt meghatározni, hogy egy terrorcselekményben érintett személy milyen funkciót töltött be szervezetben, mennyire köteleződött el, a jogellenes cselekményekbe milyen módon és milyen mértékben kapcsolódott be.

III. 1. Támogató módszerek

Az e körbe tartozó, alapvetően propaganda jellegű módszerek, tevékenységek végrehajtása alapvetően nem feltétlenül kell, hogy törvénytelenek legyenek, azonban az arra fogékony személyeket elindíthatják azon az úton, minek eredményeképpen majd jogellenes

cselekményeket hajtanak végre. A jogi megfogalmazás – „aki terrorcselekmény elkövetésére felhív, ajánlkozik, vállalkozik, a közös elkövetésben megállapodik, vagy az elkövetés elősegítése céljából az ehhez szükséges vagy ezt könnyítő feltételeket biztosítja" – mögé nézve személyek közötti, bizalmon alapuló kapcsolatokat láthatunk (például valaki ajánlkozik valakinek, valaki segítséget nyújt valakinek), melyek kialakítására, elmélyítésére a támogató módszerek alkalmasak, mivel képesek a terrorcsoportok céljait pozitívan megjeleníteni, szimpatizánsokat és jogellenes cselekményekbe bevonható személyeket megnyerni ügyüknek.

Ennek oka, hogy a terrorizmus módszereire, napjainkban kialakult és várhatóan a jövőben kialakuló formáira nagy hatást gyakorol a média, illetve az a körülmény, hogy a technikai fejlődés révén a hírek egyre hamarabb, szinte már valós időben, egyre nagyobb tömegeket érnek el, így szállítva a terroristák üzeneteit az információs társadalom tagjaihoz. A terroristák „csapdát" állítanak a média számára, és amikor az ráveti magát az elé helyezett történetre, azt kell észrevennie, hogy idegen üzenet került a rendszerbe. A terroristák taktikája lényegében kivédhetetlen, mivel a szabad médiában piaci verseny uralkodik, és a médiaipar egyik szereplője sem engedheti meg magának, hogy ne vegyen tudomást a terroristák által rendezett drámákról. Így olyan témák kerülnek reflektorfénybe, melyek korábban nem léteztek a média „valóságában", illetve a hivatalos politika részéről száműzve voltak onnan. [61]
A XXI. század terroristái már tudatosan használják fel és ki az információs társadalom információs infrastruktúráit, valamint az azokon elérhető szolgáltatásokat céljaik elérése érdekében, illetve ezek révén aktívan kutatják az új támadási és támogatási lehetőségeket.
Egy céllal rendelkező szervezetnek, így egy terrorcsoportnak is rendkívül fontos az, hogy környezetével pozitív viszonyt alakítson, tehát tevékenységét elismerjék, pozitívan értékeljék, mivel így elnézik hibáit, túlkapásait, anyagi és erkölcsi támogatáshoz juthat, ugyanakkor pedig el kell érniük azt, hogy a velük szemben álló feleket, csoportokat, szervezeteket rossz színben tüntessék fel, elutasítassák azokat, vagy legalábbis irányukba közömbössé tegyék a társadalom tagjait. „Hasznos" lehet az ellenfél gyűlölete, miként ennek felkeltését a háborúzó felek propagandistái mindig megkísérlik. A gyűlölet ugyanis erősíti a konfliktus érzelmi töltetét, s ennél fogva a cél elérésére irányuló készséget is fölerősíti. [62]
Előzőek miatt a modern terrorcsoportok propaganda műveleteikre már-már tudományos alapossággal készülnek, feltérképezve a megcélzott társadalom, vagy társadalmi réteg kor (generációs), egzisztenciális és vallási jellegzetességeit. A műveleteik kidolgozása során tehát figyelembe veszik azokat az egyedi sajátosságokat, melyek révén a megtámadottak körében a legnagyobb hatást (félelmet, anyagi kárt, stb.) érhetik el, illetve maximalizálhatják

támogatottságukat abban a társadalomban, társadalmi közegben, ahol működnek, tehát tudatos PR tevékenységet végeznek.

III. 1. 1. Ideológia terjesztése

Az új technológiákat – kommunikációs és közösségi megoldásokat – felhasználva, saját honlapokat üzemeltetve a terrorcsoportok képesek aktívan kommunikálni motivációikat, céljaikat, megszólítani a társadalmat, illetve passzív módon elérhetik azt is, hogy ezeken a fórumokon (például blogok, hírcsatornák, műsorszórás) beszéljenek róluk, céljaikról, tetteikről, ami szintén az ismertség egy fajtájaként fogható fel.

Fentiek érdekében azonban fel kell mérniük, hogy melyek azok a fórumok, közösségi csatornák, internetes felületek, ahol a megszólítani kívánt célcsoportok jelen vannak, hol kommunikálnak egymással, hol fejtik ki a legnagyobb aktivitást, és ehhez milyen eszközöket, alkalmazásokat használnak. A hatékony ideológiaterjesztés érdekében a terrorcsoportoknak alkalmazkodni kell az adott média, az adott felület profiljához, illetve a megcélzott korosztály értékrendjéhez, az általuk használt stílushoz, szlenghez, mivel csak így érhető az el, hogy üzeneteik eljussanak a célcsoport tagjaihoz és ott meghallgatásra találjanak. Ennek következtében figyelhető meg az az egyre nagyobb mértékben terjedő jelenség, hogy a nagyobb, „tőkeerősebb”, és így magasan képzett műszaki szakemberek alkalmazására is képes terrorcsoportok külön televízió- és rádió- és videócsatornákat üzemeltetnek, de ugyanakkor jelen vannak a civil szféra más szereplői által működtetett zene-, fénykép- és video-megosztó portálokon, blog- és mikroblog-csatornákon. [63]

Az üzeneteket a megcélzott célközönség, generációk szociális érzékenységéhez, „igényeihez” és „média fogyasztási szokásaihoz” igazítják, tudósításaik, publikációik révén igyekeznek szimpátiát kiváltani a nézőkből, az olvasókból, az mellett, hogy ellenségeiket démonizálják, negatív színben tüntetik fel. E PR területen a terrorszervezetek viszonylag nagyfokú „rugalmasságot” mutatnak, mivel a könnyen módosítható és manipulálható elektronikus propagandájukat akár országonként – kultúránként, nyelvenként – is képesek változtatni üzeneteikben. E rugalmasság megmutatkozik abban is, hogy némely esetekben a szimpátia kiváltása érdekében még saját ideológiájukkal össze nem egyeztethető eszközöket is bevetnek, mint például a szélsőséges iszlamisták esetében a dzsihádista rap-et, a nasheed-ot. [64]

A kérdéses televízió- és rádiócsatornák azonban túlnyomó részben csak a kibertéren keresztül érhetőek el, mivel legálisan – a konkrét fizikai térben – nem működhetnének, mert üldözésük, pusztításuk könnyebb lenne, ugyanakkor a kibertérben a nagyobb biztonság mellett nincs egy adóhoz kötött földrajzi kötöttség sem, így műsorszóró tevékenységük globális lehet. Ugyanakkor a jogellenes csoportok publikus felületeit, csatornáit a tartalomszolgáltatók – a joghatóságot gyakorló állam nyomásra – rendszerint rövid időn belül törlik, ami azt eredményezi, hogy a szervezet más néven, esetleg más országban, más szolgáltatónál indítja újra propagandáját, így az ideológiai terjesztését akadályozni csak átmenetileg lehet. Más ország joghatósága alatt működő tartalomszolgáltató esetében a terrorszervezet által fenyegetett államnak lehetőségei korlátozottabbak. Amennyiben a két állam azonos szövetségi rendszerhez tartozik, vagy kibertér eseményeire vonatkozóan van köztük jogsegélyegyezmény, akkor lehet kérni a kifogásolt tartalom törlését, ha pedig nincs ilyen együttműködés az országok között, akkor marad a törvénytelennek tartott tartalom saját fennhatósága alatt működő szolgáltatók révén történő – kevésbé hatékony – blokkolása, azonban ez a módszer különböző szolgáltatásokkal (proxy, TOR) viszonylag könnyen kijátszható. Továbbá a tartalmak TOR-on is megjeleníthetőek, bár ezzel a módszerrel a tartalom csak a dark-web-en járatos publikum előtt lesz elérhető, a széles tömegek ezzel nem tudnak élni.

III. 1. 2. Támogatók toborzása

A tagok toborzása az ideológia terjesztésére irányuló törekvésen túlmutat, itt a terrorcsoport számára már nem az a fő cél, hogy a potenciális tagjelöltekkel megismertessék ideológiájukat és rokonszenvet ébresszenek bennük, hanem az, hogy velük egyfajta interakciót alakítsanak ki. Az e körbe tartozó módszerek kiváló lehetőséget biztosítanak arra, hogy a jogellenes tevékenységet folytató csoportok kapcsolatba lépjenek az ideológiájukkal szimpatizáló személyekkel, tőlük visszacsatolást kapjanak, az aktívabb, szerepvállalásra kész, elkötelezettebbeket perifériku s cselekményeikbe bevonják, vagy akár magába a csoportba is befogadják. [65]

Toborzásra az információs társadalom korában kiválóan alkalmasak a különböző közösségi felületek (például Facebook, Twitter), melyek az érintettek ideológiai beállítottságának manipulálásán, felmérésén, ellenőrzésén túl arra is kiválóan megfelelnek, hogy személyükről, kapcsolati és érdeklődési körükről, megnyilatkozásaikról, értelmi képességeikről előzetes információt szerezzenek be. [66]

Az ideológia terjesztésénél alkalmazott műszaki megoldások, illetve az azok által nyújtott biztonsági szint e módszer esetében már nem elegendő, mivel a kapcsolatfelvétel és kommunikáció tényét nagy valószínűséggel már rejteni szükséges, tekintettel arra, hogy számos országban már a terrorszervezetté nyilvánított csoportokkal, azok tagjaival való kapcsolatfelvételt, kapcsolattartást is büntetik. A titkos elektronikus összeköttetések megvalósítása érdekében a terrorszervezetek több módszert is alkalmaznak, de legtöbb esetben a szimpatizánsokkal, illetve a jogellenes cselekményekbe már bevont tagokkal különböző formában kommunikálnak. Ennek oka, hogy a szimpatizánsok esetében azok elköteleződésére, megbízhatóságára, illetve magának a személyazonosságukra vonatkozóan még nem rendelkeznek kellő mennyiségű és mélységű megbízható információval, így biztonsági megfontolásokból kifolyólag őket kizárják a terrorcsoport belső, érzékeny információk közlésére alkalmas fórumaiból.

A különböző alkalmazásboltokban (Google, Apple, stb.) számos olyan alkalmazás elérhető, melyek titkosított kommunikációt kínálnak a végpontok között, illetve szinte már minden közösségi felület alapszolgáltatása a bizalmas, privátüzenetek váltásának lehetősége, így a terrorcsoportnak azonnal alkalma is van kapcsolatba lépni az adott szimpatizánssal, melyre rendszerint fiktív személyi adatokkal, és konkrét személlyel összefüggésbe nem hozható IP címről létrehozott profillal tesznek kísérletet.

Ugyanakkor a kifejezetten csak a kibertérben működő terror- és bűnözői csoportok – akiknek egyáltalán nincs a fizikai dimenzióban kimutatható aktivitása – toborzótevékenysége eltér az olyan csoportokétól, melyek alapvetően a kibertér adta lehetőségeknek csak szűkebb spektrumát használják, és többnyire csak tevékenységtámogató jellegű felhasználási módokkal élnek.

A kizárólag a kibertérben működő terrorcsoportok esetében előfordulhat az is, hogy azok tagjai személyesen nem is ismerik egymást (vagy csak néhány tag, alapító ismeri egymást), és valódi kilétük a jogellenes tevékenységre irányuló együttműködés során is rejtve marad. Ez a specialitás azonban rá is nyomja a bélyegét a csoport működésére, mivel a toborzás során nincs lehetőség a leendő tag teljes körű ellenőrzésére, így a „felvétel alapja” a már eddig végrehajtott illegális tevékenységek hitelt érdemlő igazolása, vagy a csoport által kreált jogellenes próbafeladatok sikeres végrehajtása, mellyel bizonyítják elköteleződésüket a csoport irányba.

III. 2. Finanszírozási és logisztikai módszerek

Az e körbe tartozó módszerek a kibertérben működő terrorszervezetek finanszírozhatóságának, szervezettségének és működő- vagy akcióképességének fenntartását biztosítják. A kibertérben tevékenykedő terrorcsoportok számára is elengedhetetlenül fontos az, hogy megfelelő finanszírozási háttérrel rendelkezzenek, mivel ez egyaránt fontos mind biztonságuk, mind eszközeik megteremtése, mind műveleteik végrehajtása, mind kommunikációjuk és összességében pedig törekvéseik megvalósítása érdekében. E feltételek biztosítása céljából szükségük lehet olyan erőforrásokra, szolgáltatásokra, amelyeket vagy folyamatosan, vagy ideiglenesen birtokukba kell, hogy tartsanak, amiket megszerezhetnek támogatóiktól, vagy illegálisan más entitásoktól.
E tevékenység szempontjából erőforrásként értelmezhető minden olyan célfeladatra gyártott, vagy átalakított eszköz, ellopható, megvásárolható szolgáltatás, információ, melyet fel lehet használni a kibertérben, vagy épp előzetesen a fizikai dimenzióban, ahhoz, hogy céljaikat elérjék. Utoljára, de nem utolsó sorban erőforrásként értelmezhetőek a valós vagy épp virtuális pénzügyi források is, melyeket a tevékenység finanszírozása érdekében felhasználhatók.

A fenti körbe tartozó tevékenységeket a jogalkotó az „aki terrorcselekmény feltételeinek biztosításához anyagi eszközt szolgáltat vagy gyűjt, vagy terrorcselekmény elkövetésére készülő személyt vagy rá tekintettel mást anyagi eszközzel támogat” definícióval szankcionálja, azonban ennek felderítése, bizonyítása, bizonyíthatósága a kibertér vonatkozásában erősen kétséges. Ennek fő oka, hogy egy kibertérben folyó tevékenységről előzetesen – hacsak nincs ezt megalapozó konkrét információ, vagy egyéb egyértelműsítő körülmény – szinte lehetetlen azt eldönteni, hogy azt egy későbbi terrorcselekmény támogatása érdekében folytatják, például egy titkosított kommunikációt biztosító alkalmazásról nem lehet kijelenteni előzetesen, hogy azért készítették, hogy azon terrorcselekményt szervezzenek meg.

A logisztikai tevékenységek esetében megjegyzendő, hogy határaik – illegális tevékenység mibenlétének, céljának függvényében – elmosódhatnak, tehát egy módszerrel, eszközzel akár több féle logisztikai tevékenység is megvalósítható.

III. 2. 1. Kommunikáció, információk megosztása

Mint fentebb már utaltunk rá, a terrorcsoportok számára a szervezettség fenntartása, vagy a tagok toborzása esetén rendkívül fontos, hogy a potenciális jelöltekkel biztonságos és egyértelmű azonosításra alkalmas csatornákat építsenek ki a kibertérben.

A kibertérben kialakított logisztikai hátérrel, megfelelő módszerekkel a tagok biztonságos és személytelen kommunikációja, információ-megosztása könnyen megvalósítható, mivel az információtechnológia dinamikus fejlődése ezt lehetővé tette:

- Napjainkban egyrészt már minden operációs rendszer – az alkalmazásboltjain keresztül – kínál olyan sajátfejlesztésű, platform-független megoldásokat (például Windows (Microsoft) – Skype, Android (Google) - Hangouts), melyek lehetővé teszik a felek közötti titkosított kommunikáció lebonyolítását, információk megosztását. Ezt a megoldást főleg az operációs rendszert fejlesztő céget befogadó ország érdekszféráján és joghatóságán (szövetségi rendszerén) kívüli személyek, csoportok kedvelik, aminek fő oka az lehet, hogy bíznak abban, hogy tevékenységük az érintett befogadó ország számára irreleváns, így nem fognak erőforrásokat arra fordítani, hogy az ő kommunikációjukat elfogják, feldolgozzák, illetve ez irányban kialakított képességeik meglétét, mértékét kívülálló szervezetekkel megosszák. A feltevés alapja, hogy e képességeket egyrészt pusztán létük, másrészt a felhasználók bizalmának megőrzése (értsd, a keletkező információfolyam folyamatos biztosítása) érdekében titkolni szükséges, így az ilyen hírszerzőrendszerekből származó „hasznok” megőrzése érdekében az érintett országok az információkat nem osztják meg érdekszférájukon kívüli és sokszor azon belüli szereplőkkel sem.

  Ezt a feltevést támasztja alá a Snowden-botrányként elhíresült incidens is, amikor a világ számára is nyilvánvalóvá vált – amit a biztonsági szektor szakemberei már tényként kezeltek – hogy az Egyesült Államokban működő technológiai – hardver- és szoftvergyártó – nagyvállalatok online összeköttetésben állnak a helyi biztonsági szervekkel, és ennek keretében megosztották adatbázisaikat, meta-adataikat, illetve bizony esetekben a támadás sikerének garantálása érdekében hardver-, illetve szoftvermódosításokat is eszközöltek termékeikben.

  Az efféle tevékenység ugyanakkor vélhetően nemcsak az Egyesült Államok sajátja, hanem minden olyan országra is jellemző, mely a fejlett technológiák birtokában elektronikai eszközöket gyárt, exportál. Erre példa lehet Kína, mivel esetükben rendre felmerül annak gyanúja, hogy az általuk gyártott eszközökön keresztül képesek

megfigyelni a felhasználók tevékenységét, adatait, de példa lehet Oroszország is, ahol pedig a legnagyobb, világszínvonalat képviselő, internet-biztonsági megoldásokat szállító szoftvercég esetében merült fel annak gyanúja, hogy az orosz biztonsági szolgálatok nyomására hátsó kapukat helyeztek el termékeiben.

- Az információcsere és megosztás megvalósítható külön, jellemzően szintén platform-független, végpontok közötti titkosítást biztosító kommunikációs szoftverrel is (például Viber, Signal, Telegram, stb.), mely besorolását illetően nagyfokú hasonlóságot mutat az előző ponttal, azonban ez lehetőséget biztosít arra, hogy a kommunikációt függetlenítsék az operációs rendszer gyártójától, ezáltal kizárják, illetve minimálisra csökkentsék a rajta keresztül történő „kényelmes" megfigyelés lehetőségét. [67]

  További előny kovácsolható abból is, ha egy szoftver nyílt forráskódú, ami szakértő kezekben könnyen testre szabható, átírható, mivel így a kommunikáció kompromittálódása esetén a forráskód megváltoztatásával (protokollok, titkosítási módszer cseréjével) gyorsan új alapokra lehet helyezni a kapcsolattartást. A módszer esetében is valószínűsíthető, hogy a biztonság növelése érdekében a felhasználók viselkedése illeszkedik az előző pontban vázolt érdekszférák, joghatóságok elemzéséhez, a vélt vagy valós biztonsági kockázatok elkerüléséhez.

- Főleg csak a kibertérben tényked ő, tehát nagy informatikai know-how birtokában lévő, illetve tőkeerős, tehát ilyen know-how-t megvásárolni képes szervezetek repertoárjában jelenik meg az a módszer, amikor a csoport tagjai saját biztonságukat szem előtt tartva egyedi, csak és kizárólag saját maguk kommunikációja érdekében kifejlesztett alkalmazásokat használnak az információk megosztására.

  Az egyediség garantálja a szoftverkód tisztaságát, tehát hogy hátsó kapukat, fölösleges, a program méretét indokolatlanul megnövelő funkciókat (akár potenciális hibalehetőségeket, sebezhetőségeket) nem építenek bele. Az egyediség némi biztonságot is nyújt, mivel csak a csoporttagok rendelkeznek az alkalmazással, így ennek ténye, megoldásai rejtve maradnak, illetve egy csoporttag esetleges kompromittálódásáról – a beépített biztonsági megoldások révén – a többi csoporttag értesülhet, és így kommunikációs szoftvert, titkosítási kulcsot, vagy akár módszert is válhatnak.

Az alkalmazásokban használt egyedi megoldások (protokollok, titkosítási módszerek, elérési pontok, stb.) pedig sok esetben alkalmasak lehetnek arra is, hogy a csoport tagjait figyelő biztonsági szolgálatok a kommunikáció tényét – főleg rövid üzeneteknél – ne is észleljék, illetve azt ne személyek közötti kommunikációként azonosítsák. Az egyedi kommunikáció pedig, amennyiben ennek ténye mégis hatóságok tudomására jut, rendkívül nagy terhet róhat az érintett biztonsági szolgálatokra, mivel egy ilyen alkalmazás megszerzése, visszafejtése, és/vagy az elfogott kommunikáció feltörése – már amennyiben ez egyáltalán lehetséges – aránytalanul nagy összegeket emészthet fel. Amennyiben a megfigyelt csoport tudomására jut kommunikációjuk kompromittálódása, úgy várhatóan – amennyiben nem a tudatos dezinformálás mellett döntenek – kommunikációs csatornát váltanak, melynek költsége az előző módszer megfigyelésére és a feltörésére a hatóságok részéről áldozott források töredéke lehet, és ezzel a körülménnyel a kommunikáció terén is megjelenik az aszimmetrikus hadviselés, melynek hatása akkor lehet erősebb, ha ezt a terrorcsoportok tudatosan alkalmazzák is.

A megoldás hátránya, hogy összetettebb, sok felhasználót kiszolgáló rendszereknél nagyobb, fejlettebb infrastruktúra szükségeltetik, amit célszerű az érintett ország joghatóságán kívül működtetni, melyet a következő pontban vázolt módon vesznek igénybe, vásárolnak meg.

Az informatikai szektorban működő vállalati körben számos szolgáltatónak van olyan portfóliója, mely hosszabb-rövidebb ideig tartó próbaidőszakot biztosít a felhasználók azonosítása nélkül – arra csak a megrendelést követően lenne szükség – ám a próbaidőszak lejáratát követően a terrorcsoportok tagjai ugyanannál a vállalkozásnál más azonosítókkal veszik igénybe ugyanazt a szolgáltatást, vagy másik cégnél keresnek hasonlót, így viszonylag gyorsan rotálódó, de biztos rendszert tudnak használni.

- Az illegális kommunikációra célszoftvereken kívül is számos lehetőség van. Ezek esetében az alapvető rendeltetés nem a kommunikáció biztosítása, az csak egy járulékos funkció, vagy épp a kérdéses szoftverbe „beleerőszakolt” képesség. Azonban e lehetőség használata esetén a kommunikáló felek előzetes egyeztetése, megállapodása mindenképpen szükséges, hiszen ennek hiányában nem is épülhetne fel a kapcsolat. Ilyen módszer lehet az internetes játékkonzolok, játékszoftverek chat

funkciói, de ide sorolhatóak a különböző társkeresőoldalak és webes áruházak beépített kapcsolat-felvételi lehetőségei is.

A szoftverekbe „beleerőszakolt" képességek tárháza széles, határt csak a fantázia szabhat, ilyenek lehetnek például a számítógépes játékokban, azok virtuális eszközeivel megrajzolt, jellemzően rövid ideig létező képek, megírt üzenetek, avatarok testre szabható ruháinak feliratai, stb.

E körbe tartozó módszerek egyik nagy előnye, hogy a biztonsági szolgálatok előtt a kommunikáció ténye rejtve maradhat. Egy illegális tevékenység gyanúja miatt megfigyelt személy életvitelébe könnyen, feltűnés nélkül beilleszthetők ezek az alternatív módszerek, mivel az érintett rendelhet különböző termékeket az interneten webes áruházakból, ismerkedhet az internetes társkeresőoldalakon, vagy épp szabadidejében különböző földrajzi területeken elhelyezkedő szervereken keresztül játszhat.

A játékok, illetve a játékkonzolok esetében további előny, hogy esetükben gyakorlatilag speciális operációs rendszereket futtató célhardverekről beszélünk, melyek – internetes játékok esetében – szervereikkel titkosított kapcsolatokon keresztül kommunikálnak, így mind a kapcsolat, mind pedig a hardver támadása rendkívüli kihívás.

III. 3. 2. Erőforrások gyűjtése, szolgáltatások igénybevétele

A terrorcselekmények végrehajtóinak bizonyos műveletek kivitelezéséhez szüksége lehet olyan erőforrások (infrastruktúraelemek, számítókapacitás, stb.) bevonására, melyek fölött fizikálisan nem rendelkeznek. Ez a rendelkezésre állási igény lehet folyamatosan fennálló szükséglet, de lehet csak ideiglenes jelentkező is, egy-egy művelet idejére. Ezekhez az erőforrásokhoz többféle módon is hozzájuthatnak:

- Megvásárolják a számukra szükséges erőforrásokat, szolgáltatásokat, melyhez a szükséges pénzforrásokat akár legálisan, akár illegálisan is megszerezhetik. Ez tűnik a legtriviálisabb módnak, és sok esetben az is, mivel a kérdéses erőforrások, szolgáltatások (például loggolást nem végző nagysebességű VPN kapcsolatok, tárhelyek, stb. bérlése) oly módon lesznek felhasználva, hogy nem indokolt a vásárló, vagy a megrendelő kilétének elrejtése. Azonban sok esetben indokolt lehet, hogy

legális vásárlás esetén is biztosítsák a nagyfokú anonimitást, mint például a hátrahagyandó/hátrahagyott eszközök esetében.

Anonimitást igényelnek továbbá az olyan illegális – akár fizikális, akár virtuális – eszközök vásárlásai is, melyeket egy támadásnál valamilyen módon (azonosító-, gyári szám, forgalmazó, gyártó, botnet hálózat neve, stb.) azonosítani lehet. Erre példa lehet egy botnet hálózat bérlése, amikor a megrendelőként megjelenő kiberterroristának célszerű ismeretlennek maradni annak érdekében, hogy a hálózatot üzemeltető személy ne legyen képes kilétének ismeretében ellene zsarolóként fellépni, illetve a bérlők valós kilétére akkor se derüljön fény, ha esetleg a hálózatot a hatóságok felszámolják és a vizsgálatok során a szolgáltatást bérlőkről részletes vagy részleges (technikai) adatok állnak rendelkezésre.

Az anonim vásárlások egyik bevett módszere az, amikor emelt díjas szolgáltatás keretében, a támadóhoz nem köthető, alkalmi jelleggel üzemelő, készpénzzel feltöltött, csak egyszer, vagy csak erre az egy célra használt prepaid kártyás mobilhívószám egyenlegére történik meg a vásárlás, mely a hatóságok számára gyakorlatilag visszakövethetetlen. Amennyiben pedig az emelt díjas szolgáltatás tárgya eleve törvénybe ütköző, úgy vélelmezhető, hogy a mind a két fél – az eladó is és a vásárló is – anonim módon próbál meg jelen lenni a kibertérben.
Speciális megoldása az identitás elrejtésének, amikor a kiberterroristák egy valós, létező személyt személyesítenek meg, vagy pedig egy teljesen fiktív személyt alakítanak ki. A darkweb megfelelő helyein mindkét módszer megvásárlására van lehetőség, akár a megfelelő dokumentumokkal együtt, melyek birtokában már a valós fizikai térben is lehet szolgáltatásokat igényelni (például számlanyitás, emelt díjas szolgáltatások indítása, stb.).

- A terrorcsoportok szimpatizánsaik támogatása révén jutnak hozzá a szükséges erőforrásokhoz, ez jellemzően oly módon valósul meg, hogy valamilyen szoftver futtatását vállalják saját gépeiken, melynek funkciójáról rendszerint azért rendelkeznek ismeretekkel, így tudatosan/tevőlegesen vesznek részt a terrorcselekményben. Az ilyen szoftvereknek funkciója lehet a túlterheléses támadásban való részvétel (például HOIC/LOIC), vagy épp a terrorcsoportok finanszírozását segítő kriptovaluták bányászata is.

A kis támogatást nyújtó nagyszámú tömeg jogi szempontból is kihívás elé állíthatja a bűnüldöző és igazságügyi szerveket, mivel a nagyszámú, ám csekély mértékben bevonódó bűnelkövető ellen nem lehet hatékonyan fellépni, mivel ha csak kismértékű szankciókkal élnek, akkor annak nem lesz érdemi visszatartó ereje, ha pedig „példát statuálnak", akkor akár több ezres felháborodott – a társaik hibáiból okult – szimpatizáns kíván majd retorziót venni az általuk méltánytalannak tartott ítéletért.

- Illegálisan, különböző rendszerekbe való behatolás útján is szerezhetnek erőforrásokhoz, szolgáltatásokhoz hozzáférését a támadók. Ennek a módszernek a megvalósítása, kivitelezése gyakorlatilag más módszerek (például célpontok kutatása, feltérképezése), támadások előzetes alkalmazását feltételezi, melynek eredője egy olyan újabb erőforrás feletti rendelkezés, melynek birtokában további képességek építhetők ki.

  E területen egyrészt valamilyen sebezhetőség kihasználása révén szereznek hozzáférést olyan rendszerek felett, melyek felépítésükből, rendeltetésükből adódóan nagy erőforrásokkal rendelkeznek. Másrészt pedig ezt megvalósíthatják oly módon is, hogy a szükséges erőforrásokat nem egy-két nagy rendszer kapacitásainak birtoklásával érik el, hanem számos kis erőforrással bíró eszközt vonnak irányításuk alá. Ezeknek a botnet hálózatoknak előnye, hogy a megfelelő tudás (például „0-day" sérülékenységekre vonatkozó ismeretek, mély szintű programozói képesség) birtokában viszonylag könnyen szervezhetők és könnyen konfigurálhatók, skálázhatók a különböző feladatokra. Hátrányuk, hogy könnyen el is lehet veszteni felettük az irányítást, mivel a hálózatba bevont gépek számának, illetve aktivitásuk növekedésével, együtt nő annak lehetősége, hogy észlelik a hálózat létét, az érintett számítógépek rendellenes működését.

III. 3. 3. Finanszírozási források megteremtése

Az információs térben végrehajtandó illegális műveletek döntő hányadához az értékes eszközök, erőforrások megvásárlása, valamint szaktudás megszerzése vagy elsajátítása érdekében pénzügyi forrásokat kell bevonni. Az információs rendszerek révén a kiberterroristák hatékonyan – olykor viszonylag könnyen – elő tudják teremteni a szükséges pénzt, akár szimpatizánsaik támogatásával, akár illegális módon, különböző csalásokkal (hoax), pénzügyi rendszerekbe való behatolásokkal, magán és üzleti adatok megszerzésével és

értékesítésével, stb.. A pénzszerzés e típusú módozataira mind a jog, mind pedig a közvélemény alapvetően számítógépes bűnözésként tekint. Robert Mandell csoportosítása szerint a számítógépes bűnözés valójában kétféle tevékenységtípust foglal magába:

1. „Számítógép felhasználása csalásra, lopásra vagy valaminek a titokban tartására pénzügyi, üzleti jellegű, vagyoni vagy szolgáltatási előny megszerzése érdekében,
2. Magának a számítógépnek a megtámadása, így különösen a hardver vagy a szoftver eltulajdonítása, ezek elleni szabotázs cselekmény elkövetésével való fenyegetés és váltságdíj követelése". [68]

Az anyagi források megszerzése az alábbi cselekmények végrehajtásával történhet:

- Csalások;

  Ebbe a kategóriába sorolhatjuk akár a kampányszerűen folytatott, akár az alkalomszerűen végrehajtott üzleti csalásokat, melyek rendkívül változatosak lehetnek. Tipikus példái lehetnek a „nigériai levelek" különböző – például üzleti, társkeresős – variánsai, a hamisított vagy illegális termékek forgalmazása, a – hiszékeny ügyfelek kártyaadatainak megszerzésére is alkalmas – „fake-webshopok", de a lista hosszan sorolható lenne.

- Bankkártya-csalások, banki rendszerek;

  A pénzügyi rendszerek mindig is vonzó célpontot jelentettek a bűnözők, terrorcsoportok számára, annak ellenére is, hogy ezek a rendszerek a legvédettebb infokommunikációs rendszerek körébe tartoznak, tekintettel arra, hogy e körben rendszerint rendelkezésre áll a védelem megfizetésének képessége.

  A nyilvánosságra került incidenseket elemezve megállapítható, hogy a sikeres támadások rendszerint „belső" munkatársak (saját munkavállaló, szerződéses partner, stb.) információira építettek, akiknek kellő mélységű ismeretük volt a bank védelmi megoldásairól, a vállalaton belüli visszaélések mind gyakoriságban, mind pedig értékben nagyobb veszélyt jelentenek, mint a kívülről elkövetett csalások. [69]

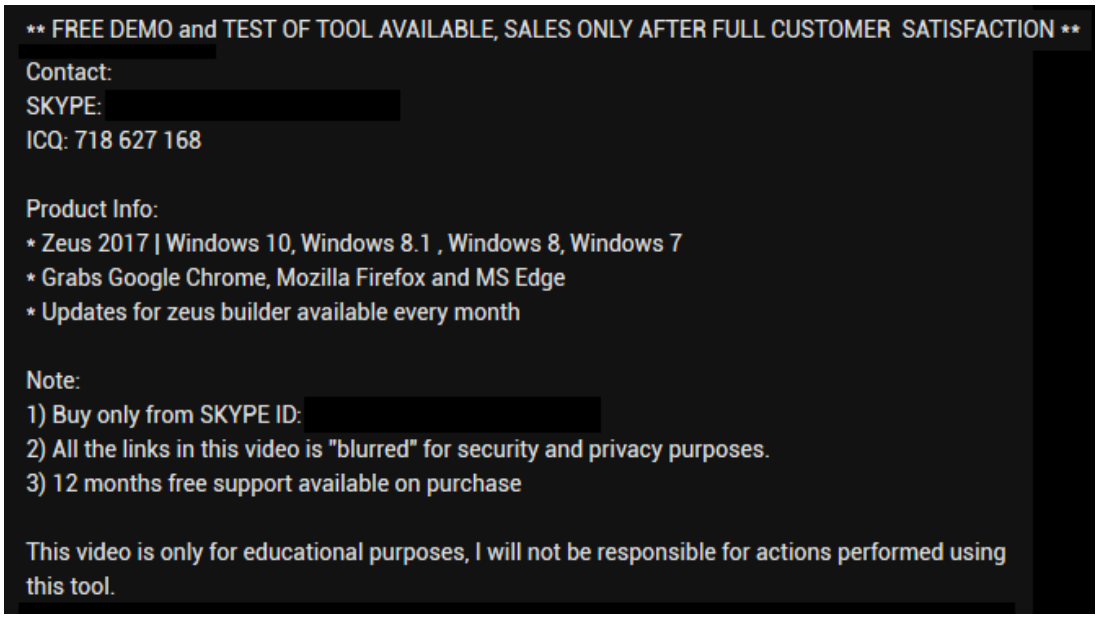
  Az esetek kisebb százalékában azonban a támadók az alkalmazott védelmi technológia nem ismert „0-day" hibáit használták ki, azonban ezen esetek jellemzője – köszönhetően a többszintű védelmi rendszereknek – hogy a bekövetkezett kár, az üzlet volumenéhez viszonyítva, nem volt jelentős.

  Fentiekből adódóan ezért a támadók inkább a banki ügyfelek, illetve a banki adatokhoz hozzáféréssel rendelkező adatkezelők (webshop-ok, kártyakibocsátók, stb.), illetve a felhasználók irányából kísérlik meg a támadást. Ennek fő oka, hogy a banki szolgáltatásokat igénybevevők körében sokkal nagyobb valószínűséggel találnak meg

olyan, kevésbé biztonságtudatos, figyelmetlen, hiszékeny és megtéveszthető, védelmi rendszert egyáltalán nem, vagy csak elavultat használó ügyfelet, akit sikeresen támadhatnak.

Ezen támadások az olyan banki azonosítók, jelszavak, kártyaadatok megszerzésére irányulnak, melyek birtokában az elkövetők vásárolhatnak, vagy hozzáférhetnek a számlákhoz, és ott tranzakciókat bonyolíthatnak le.

- Az előző pontban vázolt módon megszerzett valamilyen erőforrás felhasználásával teremtenek elő pénzt, mely alatt rendszerint valamilyen már kiépített botnetben rejlő képesség használatát, vagy épp erre épülő szolgáltatások értékesítését kell érteni. Nagy előnye, hogy a szolgáltatásokat anonim módon lehet hirdetni és ugyanilyen módon igénybe is lehet venni (például a TOR hálózaton). Ez a módszer olyannyira bejáratott, hogy a botnetek irányítói akár „próbaüzemre" is lehetőséget biztosítanak.



4. ábra Botnet hirdetés a TOR-hálózaton

Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

5. ábra DDOS szolgáltatások árai [70]

Ezek a módszerek viszonylag könnyen igényre szabhatóak és nagyon hatékonyan kiegészítik, pótolják a terrorcsoport meglévő, vagy hiányzó képességeit:

- Spamterjesztés

  Az ellenőrzés alá vont gépek ezreinek, olykor tízezreinek bevonásával a botnetek kéretlen reklám- és propagandalevelek millióit terjeszthetik az Interneten, így jelentős bevételi forrást jelentenek.
- Szolgáltatás-megtagadásos támadás

  A botnetek ilyen jellegű támadásokba történő bevonásával igen nagyfokú hatékonyságot lehet elérni, mivel alkalmasak végpontok, de akár komplett információs infrastruktúrák blokkolására is. Hatékonyságon túl további érv, hogy a nagy propaganda értékkel bíró hatás mellett a hatóságok kétséges kimenetelű elsődleges fizikai és jogi intézkedései elsősorban a botnet szervezőire, vezérlőire irányulhatnak, nem pedig annak megrendelőire.
- Nyers erőn alapuló támadás

  Ritkábban a botnet elemeinek erejét fel lehet használni nyers erőn alapuló támadások kivitelezésre is, jellemzően illegális módon megszerzett, ám titkosított állományok feltörésére, jelszavak kitalálására.
- Kriptovaluták bányászata

  Ezt a funkciót a támadók rendszerint saját jövedelmeik gyarapítása érdekében használják. Egy botnet létrehozásának lehet ez az elsődleges célja, azonban legtöbb esetben ez csak egyfajta „üresjárati" funkcióként működik, amikor nem az előbbiekben felsorolt, sokkal jövedelmezőbb feladat valamelyikét hajtja végre, akkor a valamilyen kriptovaluta bányászatát segíti (például a Dofoil nevű kártevő Electroneum-ot bányász).
- Kripto-zsarolás (Ransomware támadások)

  Az illegális pénzszerzés egyik legújabb formája a kripto-zsarolás, mely az utóbbi időszakban egy komoly pénztermelő ágazattá vált, melynek igen jó a „megtérülési aránya". Az FBI becslése szerint az egyes ransomware támadásokat végrehajtó csoportok havi bevétele elérheti akár az egymillió dollárt is. [71] [72]

  A ransomware programok titkosítják a megtámadott eszközökön található fájlokat, majd váltságdíjat követelnek a rendszer vagy a fájlok feloldásáért. A fertőzés az esetek többségében e-mailek csatolmányaként, mellékleteként,

valamint fertőzött weboldalak fertőzött reklámjaiként (malwertising) terjed, továbbá az ilyen kódok sűrűn felbukkannak a fájlcserélő programokban is, és sok esetben pedig a botnetek egyik priorált célja e fertőzések terjesztése. [73] Ma már egész iparág alakult ki az ilyen programok köré, olykor jelképes összegért, olykor igen borsos áron kínálnak ransomware-készítő, -terjesztő készleteket, melyekhez alkalmanként technikai háttértámogatást is nyújtanak a készítők, ami jelentős segítséget jelent a potenciális – de kezdő – támadóknak. A zsarolók változó összeget követelnek a titkosítás feloldásáért, és a váltságdíjat mindig valamilyen kriptovalutában kell fizetni. A lenyomozhatatlanságot segíti az is, hogy a károkozó távoli kommunikációs szervere (C&C) általában az anonimitást biztosító TOR hálózaton található, ami a hatóságok számára alaposan megnehezíti a felderítést.

- Szerzői jogokkal kapcsolatos visszaélések

  A megszerzett képességeik birtokában a terrorcsoportok viszonylag kis erőforrások bevonásával viszonylag nagy jövedelmezőségre tehetnek szert a szerzői jogok megsértésével, különböző – jellemzően filmek, zenék, szoftverek, ritkábban pornográf (pedofil, hírességekről szóló) – tartalmak megosztásával. Ez a tevékenység legtöbb esetben valamilyen fájlmegosztó technológián (például torrent, FTP) keresztül történik meg.

  E területen a bevételt a honlapok reklámfelületeinek, vagy ritkábban a hozzáférések értékesítésével is generálják. További, az üzemeltetők részéről nem publikált, vagy épp tagadott „járulékos” funkció, hogy a szolgáltatásokon keresztül támadókódokat telepíthetnek a tartalmat letöltők eszközeire.

  Ez a támadás történhet közvetlenül a honlapokon keresztül, de többnyire a honlapon, a kereskedelmi forgalomban pénzért árult, de megosztás előtt a támadókóddal bővített szoftvereken, illetve ezen szoftverek shareware verziónak feltörését, legalizálását végző úgynevezett crack és keygen – de szintén támadókódot telepítő – alkalmazásokon keresztül. Ezen támadások célja – felölelve a kibertámadások szinte teljes spektrumát – többféle lehet, például botnet hálózatok kiépítése, ezáltal spamek terjesztése, kriptovaluták bányászata, DDOS támadások kivitelezése, információk, jellemzően pénzügyi adatok lopása.

- Információk lopása, értékesítése

  Az információk eltulajdonításának képessége már feltételezi azt, hogy a támadók valamilyen sikeres támadás eredményeképpen már rendelkeznek olyan hozzáféréssel az érintett rendszerhez, hogy onnan le tudnak tölteni olyan információkat, melyek bizonyos körök (például üzleti, politikai életben a konkurencia, háborús helyzetben a szembenálló felek, bulvármédia) számára materializálható értékkel bírnak. Ilyen esetekben – a fizikai térben létező tárgyakkal ellentétben – nem jellemző, hogy a kompromittált rendszerek üzemeltetői a megszerzett információk visszavásárlásában érdekeltek lennének, hiszen az információra – ahogy már utaltunk rá a bevezető részben – nem érvényesek a megmaradási törvények, így az „egyedülisége" nem garantálható, tehát többszörösen is eladható.

- Pénzek mozgatása

  A terrorcsoportoknak biztonságuk érdekében elengedhetetlenül fontos, hogy akár az illegális módszerekkel megszerzett jövedelmeiket, akár a támogatóik részéről felajánlott pénzösszegeket elrejtsék, illetve oly módon legyenek képesek azok mozgatására, hogy az a hatóságok, biztonsági szolgálatok előtt rejtve maradjon. A kreativitásra szükségük is van, mivel az ilyen pénzügyi mozgásokat a hatóságok a pénzintézetek közreműködésével (például konkrét számlák, személyek és célországok figyelőztetése révén) viszonylag könnyen monitorozni tudják, így a kérdéses pénzösszegek közvetlenül számlák, személyek közötti mozgatása kizárt. Ugyanakkor nemzetközi szinten is megfigyelhető jelenség, hogy a terrorizmus és a pénzmosás ellen hozott jogszabályokból adódóan a bankoknak bizonyos összeghatár feletti tranzakciót automatikusan be kell jelenteniük. E körbe tartozó pénzmozgásokról a hatóságok erőfeszítések nélkül tudomást szereznek, ennek okán viszonylag kisebb összeg mozgatása történik csak a kibertérben, mivel a nagyobb összegek mozgatása érdekében már aránytalanul nagy mögöttes, szükség szerint nemzetközi infrastruktúrát (például fedőcégek hálóját) kell kiépíteni, és erre csak kevés terror- bűnözői csoport képes, bár értelemszerűen ezen infrastruktúrák más funkciókkal is bírhatnak.

  Fentiek okán vagy olyan anonim, hivatalos pénzügyi rendszeren kívüli módszert kell alkalmazni, amivel nem azonosíthatóak a tranzakcióban résztvevő felek, vagy olyan leplezett tevékenységhez szükséges kötni a pénzmozgást, mely illeszkedhet az érintett személyek tevékenységéhez, életviteléhez. Előbbi esetben névtelenséget garantáló kriptovaluták használatát kell érteni, mely megfelelő körültekintés mellett képesek

arra, hogy akár országhatárokon átívelve pénzt mozgassanak. E célra jellemzően a Bitcoin terjedt el, de az elmúlt időszakban annak köszönhetően, hogy az érdeklődés központjába került, illetve hogy árfolyam-ingadozásai hektikusak, más kriptovaluták (Electroneum, Ethereum) is megjelentek az illegális finanszírozási formák eszköztárában.

Második esetben viszont csak a terrorcsoportok kreativitásán múlik, hogy milyen módszert alkalmaznak. Az itt megjelenő módszerek többnyire valamilyen kereskedelmi tevékenységhez kapcsolódnak, melyek legálisnak tűnő felületet adnak a tranzakcióknak. Például alkalmasak e célra a már említett emelt díjas telefonszolgáltatások, de az olyan online felületek is, ahol különböző művészeti alkotásokat, régiségeket, egyéb gyűjteményi darabokat lehet megvásárolni, tehát ahol a valós – esetleg előállítási – objektív értéket nem lehet összehasonlítani azzal a szubjektív értékkel, amit a vásárló hajlandó megfizetni az adott áruért, így a hatóságok részéről rendkívül nehéz bizonyítani, de akár észlelni is a rosszhiszemű pénzmozgást. [74] További lehetőség lehet még a globális online játékplatformokon keresztül történő pénzmozgatás, amikor is az egyik országban lévő játékos az általa valós megvásárolt, de akár a játék folyamán megnyert virtuális játékeszközét a platform saját, e célra létrehozott online boltján keresztül egy másik országban lévő játékostársának értékesíti, aki aztán az ellenértéket saját országa valós pénzére visszaváltja. [75] Az ilyen jellegű pénzmozgások felderítését tovább nehezíti, ha azt úgynevezett harmadik országos tevékenységként végzik, tehát a tranzakcióban résztvevő felek, illetve a tranzakciót lebonyolító szerver más-más, eltérő jogrendű, a tevékenységét másként szabályozó országban vannak.

További tendencia, hogy a kereskedelmi szerverek üzemeltetői saját – nem pénzintézeti szintű – pénzügyi szolgáltatásokat (wallet-ek) indítanak, ahol lehetőség van pénzösszegeket tárolni, korlátozottan mozgatni.

III. 4. Támadó módszerek

A támadó módszerek körébe azok a terrorizmushoz kapcsolódó tevékenységkörök tartoznak, melyekkel a jogalkotó szerint megvalósítható „az információs rendszer vagy adat elleni erőszakos, közveszélyt okozó vagy fegyverrel kapcsolatos bűncselekmény”.

A kiberterrorizmus módszerei között a támadómódszerek azok, melyek bizonyos célpontok esetében a leglátványosabbak lehetnek, legtöbb érdeklődésre tarthatnak számot, így azonnal bekerülnek a média fő hírfolyamaiba és terítődnek az információs társadalomban. Ennek oka egyrészt az, hogy a társadalom tagjai esetleges saját érintettségük révén ekkor kerülnek közvetlen kapcsolatba a jelenséggel, vagy másrészt pedig ekkor tudatosul bennük, hogy körülményeik – kiberteret érintő szokásaik, földrajzi elhelyezkedésük, munkahelyük, infrastrukturális, pénzügyi, egészségügyi, stb. szolgáltatói kötődésük, hardver, szoftver környezetük, és a listát hosszasan lehetne folytatni – révén ők is potenciális célpontok, tehát akár ők is lehettek volna a támadás alanyai. A kibertérben végrehajtott terrorakciók is szimbolikus értékű agressziók, amelyek a közvetlen áldozatoknál nagyobb célpont ellen irányulnak: a támadások túlmutatnak az áldozatok közvetlen körén, és az egész társadalom számára küldenek üzenetet. [76]
A terrorcsoportok – működjenek azok teljesen, vagy csak néhány módszer tekintetében a kibertérben – értelemszerűen igyekeznek hitvallásukkal, céljaikkal összeegyeztethető, viszonylag körülhatárolható célpontokat kiválasztani, ám a kibertér sajátosságaiból adódóan ez olykor nehezen kivitelezhető, mivel a célpontok érintettsége és az áldozatok „bevonódása” – az áldozatok fentebb vázolt körülményeikből adódóan – az előzetesen tervezettől jelentősen eltérhet egymástól, így egy támadásnak olyan érintettjei is lehetnek, akik eredendően nem is voltak célpontok.

Ez a jelenség pedig a terrorcsoportok szemszögéből nézve is egyfajta kockázat, mivel a támadásban érintettek köre kiterjedhet a csoport irányába semleges, vagy épp a szimpatizánsi körre is, ami pedig a támadók ellen hangolhatja őket.

Összességében elmondható, hogy az információs rendszerek ellen indított támadások kiválóan alkalmasak arra, hogy azok révén a terroristák félelmet, nagyfokú bizonytalanságot keltsenek a társadalom széles köreiben, azonban a támadások eszkalálódása, illetve az interdependencia jelenségéből következő másodlagos hatások megjelenése esetén – a kibertér jellegzetességéből adódóan – az eredetileg támadni tervezett célpontokon messze túlmutathat annak eredménye, így a terrorcsoportok is jelentős veszteségeket (például eszközök, szimpatizánsok, erőforrások) szenvedhetnek el.

III. 4. 1. Célpontok keresése és azokról információk gyűjtése

A telekommunikáció XX. századi robbanása a terroristák akcióinak hatásmechanizmusát, célpontválasztási stratégiáját is alapvetően megváltoztatta. [77] A kiberterroristák az interneten nagyon könnyen hozzáférhető nyílt, vagy a kompromittált információs rendszerekből illegális módon – akár maguk, akár más támadók révén – megszerzett információk alapján olyan potenciális célpontokat azonosíthatnak, melyek támadásával érzékeny csapást mérhetnek a társadalomra.

A különböző információ-megosztó helyek és technológiák (például politikai, gazdasági, tudományos-ismeretterjesztő, stb. műsorszórás, közösségi oldalak, blogok, fórumok, stb.) használatával folyamatos, úgynevezett tippkutató tevékenységet folytathatnak, mely révén szűrhetnek földrajzi területre, ipari ágazatra, időszakra, eseményre, vagy akár konkrét személyre, illetve személyi körre, illetve a már kiválasztott célpontról szerezhetnek be további kiegészítő ismereteket. Nem kétséges, hogy a mai világ nagyon összetett, ami bizonyos mértékben előnyös helyzetet teremt a terrorista cselekmények, a célpontok kiválasztásában. A gyorsuló, táguló világ velejárói ezek, amelyek segítik a demokráciák fejlődését, kialakítják az emberi élet teljességét. A források tömény koncentrációja, az azokhoz való hozzáférés lehetősége az anyagi és a humán forrásokat is centralizálják a világban. Ez lehetővé teszi a terroristák számára a könnyű célpontválasztást. [78]

A kiválasztott célpontok döntő részéről számos közvetlen, vagy közvetett érzékeny adat elérhető az olyan információs rendszerekben, melyek lehetnek nyíltak, korlátozottan elérhetőek, vagy épp a nyilvánosságtól elzártak:

- Az információszerzés tekintetében a nyílt információs rendszerek spektruma – a számos általános, illetve specifikus keresőmotorok, ingyenes és fizetős információs szolgáltatások korában – szinte végtelen lehet. Sok esetben olyan helyről is szerezhetők be információk, melyek első hallásra meghökkentőek és nem is kapcsolhatók össze a tervezett jogellenes cselekménnyel. Ennek egyik ilyen példája lehet a *Strava* nevű népszerű fitneszalkalmazás, melynek szolgáltatásai segítségével sikeresen azonosítottak be Közel-Keleten több nyugati katonai objektumot, illetve az ott szolgálatot teljesítő katonák kocogó-útvonalait, illetve maguknak a katonáknak a személyazonosságát. [79] Ennek az incidensnek az eredményessége több részeredményből adódott össze, egyrészt a támadók sikeresen ismerték fel azt az életviteli „anomáliát”, hogy az adott veszélyes földrajzi területen a helyiek nem

engedhetik meg maguknak a fitnesz (úszás, kerékpározás, kocogás), illetve ennek online nyomon-követhetőségének luxusát, így ezek a személyek vélhetően nyugatiak, illetve nagy számban ott tartózkodó nyugati katonák. Másrészt az érintettek neve, nációja beszédes nickneveik alapján könnyen azonosítható volt, harmadrészt pedig a sportolási szokásaikból, helyelőzményeikből másik kontinensen található lakókörnyezetük, munkahelyük is azonosíthatóvá vált.

További, és egyre nagyobb információgyűjtő platformmá válhatnak a különböző közösségi honlapok, ahol a felhasználók a támadandó rendszer és személyek vonatkozásában felelőtlenül, sokszor tudtukon kívül osztanak meg olyan – a kívülállók számára indifferensnek tűnő – adatokat (például időpontokról, résztvevőkről, eszközökről, képzésekről, helyekről, de akár a megosztott fényképek meta adatai is ide sorolhatók, stb), melyek értékes segítséget nyújthatnak egy támadás kivitelezéséhez. A közösségi oldalakhoz kapcsolódó adatszivárgások száma is rendkívül magas, példaként azt a 2012. évi eset említhető, amikor az egyik iszlamista terrorcsoport több száz Irakban és Afganisztánban szolgáló amerikai katonát azonosított névvel, címmel saját, illetve kapcsolati körük Facebook profiljainak tanulmányozását követően.

Ugyanakkor a támadók sok esetben ennél tovább is mennek, és nem csak a megosztott tartalmakból próbálják meg a számukra hasznos információkat kiszűrni, hanem aktívan, célirányosan igyekszenek az érintett személyi kör irányába kapcsolatokat kiépíteni – legtöbb esetben álprofilokkal – és így tesznek kísérletet érdemi információk megszerzésére (például pletykák meghallgatásával, az érintettek „beszéltetésével").

Az információszerzésen túl kiemelt cél lehet még az érintett személyi kör befolyásolása is (például rémhírek terjesztésével, „véleményalkotók" megtévesztésével), mely napjainkban egyre hatékonyabb propaganda eszköznek tűnik. Az említett célok megvalósítására alkalmas profilok létrehozása, kapcsolatépítési irányok meghatározása, utána azok kiépítése, a kapcsolatok fenntartása, ápolása, a tartalmak elkészítése, a tájékozottság fenntartása, összességében a virtuális személy hitelességének megőrzése rendkívül idő-, pénz- és erőforrás igényes feladat, így ez rendszerint nem is egy ember munkája, hanem csoportban, feladat-specifikusan végzik a támadók. Az ebben a támadási módszerben rejlő potenciált jelezheti az a nem ellenőrzött tendencia, miszerint a híradások egyre több esetben számolnak be arról, hogy a különböző ilyen jellegű összetett, és összehangolt incidensek mögött államok állnak, mivel csak ők rendelkeznek az ehhez szükséges erőforrásokkal. Erre példa

lehet a 2016-os egyesült államokbeli választásokat követő belpolitikai botrány, melynek következményeként a Facebook több száz olyan személy – véleményformáló – profilját törölte, akik mögött azonosítottan az orosz hírszerző szolgálatok álltak. [80]

- Az előző ponthoz hasonlóan hatékonyan gyűjthetők adatok a korlátozottan elérhető adatbázisokból is, melyből valamilyen regisztráció mellett – jellemzően anyagi ellenszolgáltatás fejében – teljes körűen, vagy valamely mértékben szűrten érhetők el a nyilvánosság, vagy ritkább esetben egy meghatározott foglalkozási kör számára az információk (például cégadatbázisokból, földhivatali nyilvántartásokból, építészeti adatbázisokból, közmű-nyilvántartások, tudástárakból, stb).

  Ebbe a körbe sorolhatók továbbá az államigazgatás közérdekű adatai is, melyek közvetlenül nem találhatóak meg a világhálón, de az adatigénylést követően kiadásuk nem tagadható meg. Például egy támadás megtervezése során hasznos információ lehet az, hogy egy államigazgatási szerv milyen informatikai beruházásokat (hardver, szoftver), milyen értékben, milyen beszállítótól vásárolt meg, a munkatársak milyen és milyen szintű képzéseken vettek részt, milyen külső informatikai partnerekkel (szakértők, fejlesztők, internetszolgáltatók), milyen témában állnak üzleti kapcsolatban. Ennek okán a kiemelt rendszerekkel kapcsolatos adatokat jogszabályok révén ki is vonják a közérdekű adatok köréből.

  E lehetőségek tekintetében a támadónak már mérlegelnie kell, hogy az adatszerzést milyen módon, módszerrel kívánja végrehajtani, mivel ezen adatbázisok esetében már vélhetően szükséges lesz identitását/személyazonosságát – a hozzáférés jogossága, esetlegesen felmerülő díjak rendezése, vagy pusztán a lekérdezés tényének rögzítése érdekében – igazolni, ezért ezekben az esetekben a támadónak szükséges személyazonosságát valamilyen módon leplezni. Ez történhet ellopott elektronikus identitásokkal (például bankkártya-, szerződési, hozzáférési-belépési adatokkal, stb.), személyazonossági azonosítókkal (például hamis, hamisított személyazonossági igazolványokkal, jogosítványokkal), vagy akár támogatók, szimpatizánsok által felajánlott, biztosított hozzáférési módokkal, vagy épp közvetlenül általuk.

  Magyar sajátosság, hogy hazánkban az adatigénylő bármelyik államigazgatási, költségvetési szervtől akár álnéven, csak email-címes elérhetőséggel is kérhet – minősített adatoktól eltekintve – bármilyen, működési körét érintő információt, csak az információ előállításának esetlegesen felmerülő költségeit kell megtérítenie.

- A támadáshoz szükséges információk megszerzése történhet illegális módszerrel is, melynek spektruma szintén rendkívül széles lehet, de legtöbb esetben egy információs rendszerbe – már egy sikeres támadást követően – történő jogosulatlan behatolással kapcsolatos. Ez megvalósulhat oly módon, hogy a támadáshoz szükséges információ valamelyik, a megtámadni kívánt rendszerrel kapcsolatban álló másik rendszerből, vagy épp annak alrendszeréből származik. A megszerzett adatok lehetnek különböző műszaki, adminisztratív, gazdasági dokumentumok, üzemi beállítások, programrészletek, melyből aztán a támadók következtetni tudnak az érintett rendszer képességeire, működési sajátosságaira. A módszer gyakorlatilag ugyanaz, de a nézőpont merőben más abban az esetben, amikor egy megtámadott rendszerből kinyert adatokat a támadók különböző fórumokon kiposztolják, majd azokat más támadók tanulmányozva olyan ismeretek birtokába kerülnek, tulajdonképpen véletlenül, mely az általuk kiválasztott célpontra vonatkoznak. Illegális módszerek közé sorolhatók az olyan információ megszerzési módok is, amikor támadók az érintett információs rendszerből származó, de nem illegálisan birtokukba került, nem megfelelő módon selejtezett, karbantartott alkatrészek, adathordozók elemzése során kinyert adatokat használják fel a támadáshoz.

  Érdemi információk szerezhetők be egy információs infrastruktúráról különböző műszeres mérések révén is, melyek eredményeiből a rendszerelemek működési sajátosságaira, képességeire tudnak következtetni a kiberterroristák.

III. 4. 2. Célpontok támadása

Az információs rendszerekből származó adatokkal, illetve az információs rendszerek felhasználásával, különböző technikákkal, technológiákkal, illetve ezek kombinált alkalmazásával rendkívül hatékonyan lehet támadni is más információs infrastruktúrákat. Az információs térben végrehajtott illegális műveletek esetében előnyt jelent az, hogy számos olyan megoldás (pl.: proxy-szerverek, TOR, stb.) létezik, melyek viszonylag nagyfokú anonimitást képesek biztosítani az elkövetők számára.

Továbbá nem elhanyagolható körülmény a támadók és a célpontok fizikai elhelyezkedése sem, hiszen a terrorizmus e megjelenési formájánál a fizikai távolság nehezen értelmezhető. A támadónak a művelet végrehajtásakor az országhatárok érdemi akadályokat nem jelentenek, ugyanakkor a cselekmény akadályozása, ellenintézkedések foganatosítása, vagy esetleg az elkövetők felderítése során a megtámadott infrastruktúra, illetve az azt "védő" hatóságok

részéről az államhatárok már jelentős jogi és technikai akadályokat jelentenek. A témával foglalkozó szakirodalom szinte minden egyes publikációja megemlíti a támadásokkal kapcsolatos jogi problémákat, anomáliákat. Mivel viszonylag új jelenségről beszélünk ezeknek az incidenseknek a kezelése nemzetközi szinten elfogadott normák szintjén nincs még szabályozva. Míg a nemzeti jogszabályokban az információs rendszerek, valamint az azokban kezelt adatok elleni támadásokat rendszerint pontosan megkülönböztetik, körülírják, illetve szankcionálják is, addig a nemzetközi jogban – tekintettel a jelenség újszerűségére – nincs még kialakult gyakorlat arra, hogy a sok országot és sok különböző állampolgárságú elkövetőt, tettestársat, támogatót érintő jogellenes cselekményeket miként kezeljék.

Bizonyos államok egyenesen deklarálták is, hogy infrastruktúráik védelme érdekében a kibertérből ért támadások esetében is – mivel ezt is fegyveres támadásnak tekintik – jogot formálnak arra, hogy katonai megelőző, vagy megtorló csapásokat is hajtsanak végre vélt, vagy valós ellenséges államok ellen. Azonban ez a nemzetközi jog számos pontja tekintetében problémás lehet, mivel a fegyveres támadás alapvető ismertető jegye, hogy a támadásnak minden esetben egy másik állam által betudhatónak kell lennie, tehát fegyveres támadást csak állam tud elkövetni. Nyilvánvaló tény, ha egy állam reguláris csapatai követnek el meghatározott intenzitású támadást ebben az esetben az fegyveres támadásnak minősül. Kérdéses viszont magánszemélyek vagy csoportjaik által megvalósított támadás betudható-e az államnak, és ha igen, akkor milyen szintű kapcsolatnak kell fennállnia köztük. Az ENSZ 3314. számú közgyűlési határozat rögzítette, hogy irreguláris csapatok tevékenysége is tekinthető államok közötti agressziónak, ezt erősítette meg a Nemzetközi Bíróság, amely szerint ennek határozatba foglalása a nemzetközi szokásjogot tükrözi, ennek okán irreguláris csapatok tevékenysége is betudható egy államnak. Kérdéses viszont, hogy a kapcsolatnak milyen szintűnek kell lennie ahhoz, hogy az betudható legyen az államnak. Elfogadott nézet, hogy magánszemélyek és csoportjaik cselekményei kizárólag akkor tudhatók be egy állam cselekményének, ha azok az adott állam utasítására, irányítása alatt vagy ellenőrzése mellett tevékenykednek. Az ellenőrzés mértéke azonban szintén nincs meghatározva. [81]
Életszerűtlenül elbonyolított demonstratív példa lehet az, amikor az Iszlám Állam által ellenőrzött területen tartózkodó terrorista megbíz egy orosz állampolgárságú hackert, aki Londonban, az észak-koreai nagykövetség nyilvános wifi-hálózatán keresztül egy lengyel hackertől a darkweben bérelt, főként Norvégiában működő zombi hálózat bevonásával Japánban lévő, amerikai vállalatok érdekeltségébe tartozó atomerőművekre mér csapást és a kínai területeket érő sugárszennyezés következtében kínai állampolgárok halnak meg. A

fantázia szülte szürreális példa rávilágíthat arra, hogy egy kibertámadás végrehajtása során milyen sok tényezőből állhat, melynek gyors, hatékony kezelésére, kivizsgálására a nemzetközi jog – tekintettel az eltérő jogrendekre, ellenérdekelt szövetségi rendszerekre, gazdasági feszültségekre – még nincs felkészülve.

Kibertérben végrehajtott terrortámadások osztályozása többféle módon történhet:

- A legegyszerűbb eset, mely talán első olvasatban nem is kibertámadásként értelmezhető, az az, amikor a támadó valamilyen információs rendszeren keresztül olyan ismeretek birtokába kerül, mellyel képes terrorcselekményt végrehajtani. Ebben az esetben az információs infrastruktúra, illetve rendszer az információ megosztása révén a támadás egyfajta eszközeként értelmezhető. E körbe rendszerint az egyszerű, primitív, fizikai térben materializálódó támadási módok (például „hogyan csináljunk háztartási eszközökből otthon csőbombát", „hogyan vezessünk tömegbe járművet", hogyan siklassunk ki vonatot", stb.) tartoznak.

  Ez a típusú ismeretszerzési módszer lehet passzív, amikor a támadó valamilyen közösségi oldalon, vagy a darkweben elhelyezett, bárki számára elérhetővé tett statikus módszer leírását tanulmányozza, és önként dönt annak végrehajtásáról. Továbbá lehet aktív, amikor a terrorcsoport tagja anonim, személytelen módon – az előző pontokban már taglalt kapcsolatépítés valamelyik fázisában – az eszméivel szimpatizáló jelöltet rábírja a jogellenes cselekményre, és a kiválasztott módszer, a kiválasztott helyszín, vagy épp esemény sajátosságaira felkészítve hajtatja végre vele a támadást.

  Az ilyen jellegű terrorcselekményeknél első olvasatban nem is fedezhető fel az információs jelleg, azonban a cselekmények, illetve az elkövetők hátterének vizsgálata során sok esetben megállapítható, hogy az információs rendszerek által nyújtott szolgáltatások nagyban segítették, vagy alapozták meg a támadás sikerét.

  Az ilyen jellegű aktív információszerzésre lehet példa a 2016-ban Németországban történt, gépjárművel végrehajtott terrortámadás is, amikor a fiatal elkövetőket az Iszlám Állam képviselői az interneten keresztül bujtották fel és képezték ki a „tömegbehajtás" sajátosságaira, majd a cselekmény végrehajtása alatt telefonon keresztül tartották egymással a kapcsolatot. [82]

- Az információs infrastruktúrák rendszerelemei ellen intézett fizikai támadások elsődleges célja az, hogy az érintett rendszerelemek működését zavarják, vagy akár

fizikailag meg is semmisítsék, melyek révén a támadók – a jelentős anyagi káron túl – széles körben képesek akadályozni, vagy teljesen blokkolni az érintett infrastruktúrát használó rendszerek szolgáltatásait.

A rendszerelemek fizikai léte, integritása elleni támadások – az egyszerű kivitelezés és az egyszerű eszközpark miatt – szinte mindig valamilyen kinetikus energia alkalmazását jelentik, de ritkább esetben, speciális eszközrendszer birtokában ez a támadás megvalósulhat irányított energiák (például lézerek) alkalmazásával is. Egészen ritka esetben pedig akár logikai úton is, amikor a támadók az infrastruktúra informatikai rendszerébe valamilyen módon behatolva az eszközök szabályozó rendszereinek manipulálása révén érik el azok végleges károsodását.

A modern információs infrastruktúrákra jellemző, hogy – főleg a végponti elemek környezetében – intenzíven kihasználják az elektromágneses tér nyújtotta lehetőségeket, így az itt gerjesztett mesterséges zavarokkal hatékonyan lehet akadályozni a rendszer rendeltetésszerű működést. A zavarásnak az alapvető feladata, hogy az információs rendszerben kezelt információk tulajdonságainak (elérhetőség, rendelkezésre állás, gyakoriság, stb.) manipulálása révén érje el a támadó a célját. E módszer előnye, hogy bármikor beüzemelhető, a beüzemelés helyszíne, az eszköz teljesítménye változtatható, a fizikai térben nyomot nem hagy, ugyanakkor hátránya, hogy az érintett rendszerről alapos ismeretekkel kell bírni, bemérhető és az eszköz a támadónál megtalálható.

- Az információs infrastruktúrák elleni legkifinomultabb támadási módszerek azok az eljárások, amikor a rendszerben kezelt adatok, információk jelentik a célpontot, és ezek tartalmának, valamint a már tárgyalt tulajdonságainak manipulálása révén, vagy pusztán az információ megszerzése által érik el céljaikat a támadók.

  Amennyiben a támadás az információnak tulajdonságai ellen irányul, azt rendszerint viszonylag rövid időn belül érzékelik az infrastruktúra üzemeltetői, illetve a szolgáltatásokat igénybevevő felhasználók, még ha annak okát, a támadás tényét olykor nem is ismerik fel azonnal.

  Ezeknél a támadási módozatoknál jellemzően nem maga az információ kerül veszélybe, hanem az arra épülő társadalmi folyamatok, szolgáltatások folytonossága, hitelessége, megbízhatósága válik kérdésessé, így alapvetően nagy transzparenciát

mutató támadásokról beszélünk, melyek az információs társadalomban kiemelt érdeklődésre tarthatnak számot.

Az információ tartalma ellen irányuló támadások esetében jellemzően nem cél az, hogy a sikeres támadás tényét transzparens módon bárki előtt hirdessék, hiszen a támadónak elemi érdeke fűződhet ahhoz, hogy a kompromittált rendszer az általa megváltoztatott információkkal az üzemeltetőket, illetve más ellenérdekelt felet is megtévesztve tovább működjön, ezáltal biztosítva a támadónak az elérni kívánt előnyt, pozitív hatást, akár hosszabb időtávon keresztül is. A támadónak azonban alaposan ismernie kell a rendszer működését és a benne kezelt információk sajátosságait, hiszen ha a kelleténél nagyobb beavatkozást hajt végre, akkor a rendszerben működő – a támadó által nem befolyásolható – biztonsági automatizmusok jelezhetik az anomáliákat.

Az információ tartalma elleni – annak eltulajdonlása és módosítása révén – sikeres támadások tényének nyilvánosságra hozatalával azonban a támadónak alapvetően az lehet a fő célja, hogy az érintett rendszerbe, illetve annak szolgáltatásaiba vetett bizalmat megrendítse, annak használatától a felhasználókat elriassza. A kompromittált állami információs rendszerek esetében is hasonló a helyzet, itt a közbizalmat, a közhitelességet ássa alá egy sikeres támadás, ellenben ezeknek a rendszereknek – a kereskedelmi, ipari célú infrastruktúrákkal ellentétben – nincs alternatívájuk, így a társadalmat ért hatás is általában jóval súlyosabb.

Ugyanakkor szükséges megemlíteni, hogy egy ilyen jellegű támadás nem csak az információs rendszer fontossága, infrastrukturális jellege miatt következhet be, hanem fenn állhat annak veszélye is, hogy a szolgáltatásokat igénybevevő transzparens felhasználók köre miatt irányul rá a támadók permanens figyelme. Ennek példájaként megemlíthető az az incidens, amikor a hackerek az egyik nemzetközi szoftvervállalat felhőszolgáltatását sikeresen támadták meg, de csak a hírességek fiókjaiból töltöttek le intim felvételeket, majd azokat az interneten áruba bocsátották.

Megemlítendő, hogy az információs infrastruktúrák működésének egyik jellegzetességéből, az interdependenciából adódóan más, akár perifériálisan kapcsolódó szolgáltatók zavarai is kihathatnak egy adott információs rendszerre, így ha a támadók alapos ismeretekkel bírnak a célpontról, illetve annak működési körülményeiről (jogi, fizikai, gazdasági, szociológiai), akkor más rendszerek támadásával, ezeknek a működési körülményeinek a befolyásolásával is

tudnak zavart előidézni abban. Itt nem csak a műszaki berendezésekre lehet, s kell gondolni, hanem akár például az infrastruktúrát működtető személyzetre, hiszen ha az üzemeltetésben résztvevő személyzet akár – a közlekedési rendszer megzavarása miatt – nem jut el munkahelyére, akár – rémhír terjesztése miatt – sztrájkba lép, akár munkavégzésben – akusztikus fegyverekkel – zavarják, az kihat az érintett rendszerre is. Utóbbi esetre lehet példa, amikor felmerült annak gyanúja, hogy az Egyesült Államok havannai nagykövetségének személyzete, és így közvetve az általuk üzemeltetett információs rendszerek ellen ismeretlenek vélhetően akusztikus fegyvereket vetettek be, ami az érintetteknél kisebb mértékű, de maradandó agykárosodást okozott. [83] Bár a híradások sem az elkövetőket, sem azok célját nem nevezik meg, azonban könnyen belátható, hogy a cselekmény súlyos károkat okozott az ott működő információs infrastruktúrákban. Egyrészt a rendszerek korábbi, illetve a leendő üzemeltető személyzete, a diplomaták a történtek ismeretében, egészségkárosodástól való félelmükben vélhetően nem szívesen vállalnak ott újra munkát, másrészt az amerikai kormányzat minimálisra csökkentette a személyzet létszámát, ami kihatással van a politikai, gazdasági információk megszerzésére, áramlására, feldolgozására, illetve a kapcsolatépítésre.

III. 5. Összegzés, részkövetkeztetések

A kibertér tértől és időtől függetlenül köti össze az információs infrastruktúrák különböző szolgáltatásait, ez által biztosítva az információs társadalom funkcióinak folytonosságát, a társadalmat alkotó entitások szükségleteinek kielégítését, ezért ezek az információs infrastruktúrák a kiberterrorizmus kiemelt célpontjai és ugyanakkor eszközei lehetnek (például DDoS támadás esetében). A kibertér, illetve az azt alkotó információs infrastruktúrák összessége, az abban megjelenő funkciók és szolgáltatások sokrétűsége a kiberterrorizmus számára is rendkívül sok olyan lehetőséget kínál, melyekkel élve, közvetve vagy közvetlenül elérhetik céljukat, növelhetik jogellenes tevékenységük hatékonyságát, az elért személyek számát.

Ugyanakkor a kibertérben végrehajtott terrorcselekményeknél a specifikus cél- és módszerválasztásnak lehet egy olyan, a terrorizmus korábbi megjelenési formáinál sokkal veszélyesebb hatása, hogy a támadásban nem, vagy csak kevésbé érintett társadalmi körök – a valós veszélyt nem érzékelve – érdemben nem fognak reagálni, kívülállóként pedig sokkal nehezebben lesznek mozgósíthatók a jogellenes cselekmény felszámolása érdekében.

Mivel a kibertér polgári és katonai értelmezése némileg eltér egymástól, ezért más-más szempontból közelítik meg a kibertér létét, lényegét. A számos azonosságon túl a katonai értelmezés lényegesen komplexebb, mivel az itt alkalmazott rendszerek rendeltetésükből, működési környezetükből, illetve az irányukba támasztott követelményekből adódóan teljesen más szemléletmódot igényelnek. Ugyanakkor pedig mind a katonai, mind a polgári információs rendszerek képességeinek fenntartása az üzemeltető céljainak elérése érdekében kulcsfontosságú, ezért fel kell mérnie a kibertérből érkező, az adott rendszerre fenyegetést jelentő körülményeket, esetleges támadási módokat, relevanciával bíró terrorcsoportokat, és a kockázatelemzés eredményének ismeretében ki kell alakítani a rendszer megóvásának képességét. Katonai szervezetek és rendészeti szervek esetében, az előzőeken túl az ellenérdekelt felek rendszereinek irányába felderítési és támadási képességeket is meg kell szerezni. E képességek megszerzésének igénye azonban nem csak a polgári és katonai szervezeteké, hanem a kibertérben működő, vagy annak szolgáltatásaira nagyban építő terrorszervezetek célja is.

Mivel – mint ahogy arra már utaltunk – a kibertérben elérhető szolgáltatások nem csak közvetlenül, hanem közvetve is felhasználhatók a terror céljainak elérése érdekében, továbbá nem csak a szolgáltatások, illetve szolgáltatások akadályozása lehet a cél, hanem közvetlenül a szolgáltatást biztosító, fizikailag elérhető műszaki infrastruktúra is.

Az információs infrastruktúrák vonatkozásában, a kiberterrorizmus lehetséges közvetlen, közvetett céljait kutatva három olyan kategóriát találtam, melyek több alkategóriára is bonthatóak, melyekbe a különböző módszerek viszonylag könnyen csoportosíthatóak:

- támogató (ideológia terjesztése, támogatók toborzása),
- logisztikai (kommunikáció, információk-megosztása, erőforrások gyűjtése, szolgáltatások igénybevétele, finanszírozási források megteremtése),
- támadó (célpontok keresése és azokról információk gyűjtése, célpontok támadása).

A viszonylagosság azonban jelen van, mivel bizonyos módszerek a cél függvényében más-más kategóriába eshetnek. A kategóriák bevezetése segítheti a jogellenes cselekmények büntetőjogi besorolását, illetve az infrastruktúrák üzemeltetőinek segíthet annak felmérésében, hogy szolgáltatásaikat milyen jogellenes cselekményre használhatják fel.

Egy, a kibertérben előkészített, vagy onnan érkező támadás azonban jellemzően nem csak egy-egy módszer alkalmazását jelenti, hanem a különböző kategóriába tartozó módszerek

logikailag egymásra épülő, egymást követő, vagy olykor épp párhuzamos használatát feltételezi. Minden kibertámadásnak az érintett információs infrastruktúra egyedisége, a támadással elérni kívánt cél, illetve a kiber-terrorcsoport rendelkezésére álló képességek és eszközök együttese egyedi mintát adhat, melynek elemzéséhez, következtetések levonásához mélyreható háttérismeretekre van szükség.
Tekintettel a fenti körülményekre az értekezésben az elmúlt időszakban napra került, a kibertérben terrorcselekménynek aposztrofált támadások vizsgálatára a kiberterrorizmus vázolt módszereivel összefüggésben nem került sor, mivel az ehhez szükséges mélységi információk – például műszaki adatok, motivációk, képességek, sérülékenységek, személyzet felkészültsége, egyéb körülmények, stb. – a számomra elérhető forrásokból – például a szakirodalomból, média híradásaiból – azok bizalmas jellege miatt nem szerezhetők be.

A kibertérben működő terrorcsoportok az elérni kívánt cél függvényében, illetve az érintett információs infrastruktúráról megszerzett előzményismeretek (például interdependens kapcsolatok, műszaki háttér, stb.), valamint egyéb jellemzőkhöz (például földrajzi elhelyezkedés) igazodva állíthatják össze azt az „eszközparkot”, aminek birtokában nagy valószínűséggel célt érnek. Azonban ezeknek a fizikai hatáson alapuló és logikai eszközöknek egy része a közvetlen támadáson túl arra is alkalmas, hogy az érintett információs infrastruktúrák működési paramétereiről, sérülékenységeiről előzetes információt szolgáltassanak.

IV. A kiberterrorizmus eszközei

Az információs infrastruktúrák támadásakor a kiberterroristák alapvetően a fizikai hatáson alapuló, illetve a logikai eszközökre támaszkodhatnak, melyek alkalmazásának technikai, képesség- és képzettségbeli, finanszírozási feltételei merőben eltérnek egymástól, így vizsgálatukat is célszerű külön végezni.

IV. 1. Fizikai hatáson alapuló eszközök

Az információs infrastruktúrák szolgáltatásainak akadályozásának, illetve megszüntetésének legegyszerűbb, legkézenfekvőbb módja a rendszer kritikus elemeinek, illetve kommunikációs összeköttetéseinek kiiktatása, fizikai megsemmisítése. Ez a legkülönbözőbb eszközökkel megvalósítható, függvényében annak, hogy a kiberterroristák milyen eszközrendszerek állnak rendelkezésére, milyen messze van a céltól, illetve attól, hogy magát a kritikus információs infrastruktúrát milyen eszközökkel, módszerekkel igyekeznek megóvni az ilyen jellegű külső behatásoktól.

A katonai doktrínák alapján a fizikai támadás érkezhet földről, levegőből, vízfelszínről, vagy éppen víz alól indított eszközök révén, de ide sorolhatók a helyszínen bevetett különleges erők is. Az információs infrastruktúrák, illetve azok részelemeinek, alrendszereinek egyszeri, vagy folyamatos fizikai támadása, pusztítása nagymértékben csökkenti azok hatékonyságát, képességeit, tehát magát a használhatóságot. A fizikai támadások célpontjai a már fentebb tárgyalt infrastruktúrák, melyek ellen bevetett eszközök, eszközrendszerek kiválasztása az adott szituációtól, környezettől függ. Az információs infrastruktúrák ellen alkalmazott fizikai kinetikus, termikus eszközök lehetnek:

- repülőeszközök fedélzetéről indított, nagy pontosságú irányított rakétafegyverek;
- tüzérségi eszközök;
- légvédelmi tüzér- és rakétaeszközök;
- gépesített lövész- és harckocsi-csapatok;
- különleges erők. [15:216]

A fizikai hatásokon alapuló támadásoknak azonban a kinetikus erőnél lehetnek finomabb formái is, hiszen az infrastruktúrák működési zavarát, egyes elemeiknek ideiglenes lebénítását elő lehet idézni rombolás nélkül is. Ilyen megoldás lehet például az elektromos távvezetékekben rövidzárlatot okozó grafitbomba. Ezek a robbanóeszközök ugyanúgy

kerülnek alkalmazásra, mint a hagyományos eszközök, csak ebben az esetben nem a robbanás következtében fellépő kinetikus energia fejti ki a pusztító hatást, hanem a célpont fölött detonáló eszköz robbanása eredményeképpen szétszóródó grafitszálak rátelepedve a távvezetékekre rövidzárlatot okoznak az elektromos hálózatban. [84]

A terrorcsoportok szempontjából az alábbi eszközök nyilvánvalóan, ha nem is a „hagyományos", megszokott megjelenési formáikban, nem is katonai precizitással megalkotva, de szintén rendelkezésre állhatnak. Például Közel-Keleten rendszeresek a terrorcsoportok által végrehajtott rakétatámadások, mely eszközök ugyan precíziós támadás kivitelezésére nem használhatók, ám nagyobb infrastruktúraelemek esetében – akár tömegesen bevetve őket – már korlátozottan alkalmasak lehetnek azok rongálására.

6. ábra Házilag barkácsolt rakéta a Közel-Keleten [85]

Természetesen a nagyobb terrorcsoportok is rendelkeznek olyan – különleges erők körébe sorolható – alakulatokkal, melyek tagjai hatékonyan bevethetőek az információs infrastruktúrák ellen. Megerősített, páncélozott gépjárműveikkel viszonylag könnyen áttörhetik az infrastruktúrákat védő akadályokat és a helyszínen, más, közvetlen módon tesznek kárt az érintett rendszerben, illetve az esetlegesen járműveikre szerelt különböző fejlettségű tüzérségi eszközökkel viszonylag nagyobb távolságból, hirtelen lecsapva pusztíthatják az infrastruktúra elemeit.

7. ábra Házilag barkácsolt "rohamlöveg" a Közel-Keleten [86]

Fizikai jellegű támadások körébe tartoznak az elektromágneses energia-formák felhasználásával – különböző cél érdekében – végrehajtott tevékenységek is. A katonai szaknyelvben elektronikai hadviselésnek hívott eszköz- és eljárásrendszer a katonai tevékenység azon része, mely az elektromágneses tér energiáinak elemzése révén meghatározza, felderíti, csökkenti vagy akadályozza az elektromágneses spektrum ellenség által történő használatát. E tevékenység keretében megszerzett információk elősegítik az értékelő, döntéshozó folyamatokat, hozzájárulnak a szervezéshez és a szervezet hatékony irányításához.

Az elektronikai hadviselésnek három, egymást kiegészítő szakterülete van [15]:

– az elektronikai védelem;

  Az elektronikai védelem biztosítja az elektromágneses spektrum saját részről történő hatékony kihasználásának lehetőségét az ellenség, illetve az ellenérdekelt fél elektronikai támogató és ellentevékenysége, valamint a saját eszközeink, alakulataink nem szándékos elektromágneses interferenciái ellenére.

  Az elektronikai védelmi tevékenység napjainkban nincs jelen a kibertérben tényked terrorcsoportok repertoárjában, mivel önállóan, önerőből nem üzemeltetnek összefüggő, működésük szempontjából megvédendő infrastruktúrákat sem, hanem már meglévő, kereskedelmi vállalatok tulajdonában álló szolgáltatásokat vesznek igénybe. Ebből kifolyólag a rendszerekkel kapcsolatos védelmi tevékenységtől is mentesülnek, hiszen azok végrehajtása a

szolgáltatókat terheli. Fentiekből adódóan az elektronikai védelem a terrorcsoportok számára jelenleg szükségtelen képességnek tűnik.

– az elektronikai támogató tevékenység;

  Az elektronikai támogató tevékenység a különböző fenyegetések azonnali jelzése érdekében az elektromágneses kisugárzások felkutatására, elfogására, azonosítására és helyének meghatározására irányul.

  A kritikus információs infrastruktúrák elleni támadások eredményessége nagymértékben függ attól, hogy a támadást végrehajtó birtokában van-e azoknak az információknak, melyek a támadni kívánt rendszer fizikai (földrajzi) elhelyezkedésére, strukturális összetételére, hardver és szoftver összetevőire, a rajta zajló adatforgalom céljára, mennyiségére, esetleges gyenge pontjaira, és annak jellegére, valamint az adott információs rendszer üzemeltetőire és felhasználóira vonatkoznak. [84]

  Az elektronikai felderítés – mint az elektronikai támogató tevékenység egyik legfontosabb részterülete – az információszerző tevékenység szempontjából általában kettős céllal kerülhet végrehajtásra. Egyrészt az infokommunikációs rendszerekben tárolt és továbbított adatokhoz való hozzáférés és azok felhasználása céljából, másrészt pedig a hatékony, a kibertéren keresztül kivitelezett támadáshoz szükséges célinformációk megszerzése érdekében.

  Az illegális tevékenység tekintetében e részterületen már lényegesen nagyobb lehetőségei vannak a kibertérben működő terrorcsoportoknak. Megfelelő eszközök birtokában érdemi információkat szerezhetnek meg a megtámadni kívánt infrastruktúrában alkalmazott rendszerszervezési elvekről, az eszközök működési tartományairól (adatátviteli sebességek, átviteli távolság, stb.) üzemeltetési statisztikákról (üzemi csúcsidőkről, üzemszünetekről), illetve bizonyos esetekben (például a rendszerelemek fontosságának felmérése esetén) a reagáló erők megjelenésének szintidejéről, eszközparkjáról, útvonaláról.

  Fenti információkat elemezve pedig a támadók már tervezni tudják a támadáshoz szükséges eszközrendszer összetételét, azok képességeit, teljesítményét, a támadás időpontját, időtartamát és akár pontos helyét is.

Extrém esetben az adott információs infrastruktúra folyamatos „zaklatásával” – amennyiben az infrastruktúra üzemeltetője nem ismeri fel a támadást, vagy nem helyesen értékeli a kialakult helyzetet – az is elérhető, hogy a rendszer topológiáját, a rendszerelemek konfigurációját a hatékonyabb működés érdekében – a támadás szempontjából kedvező módon – átszervezzék, átalakítsák. Ez a lehetőség értelemszerűen nem tervezhető, illetve bekövetkezte esetén sem törvényszerű, hogy az infrastruktúrában a támadás szempontjából kedvező változtatás történik.

A terrorcsoportok biztonságának szempontjából is rendkívül hasznosak lehetnek azok az információk, melyeket elektronikai felderítési tevékenység során a kibertérből – jelen esetben saját környezetükből – szereznek be. A saját fizikai terüket jellemző elektromágneses környezetben hirtelen megjelenő markáns, szokatlan változásokat figyelemfelkeltő, biztonságukra veszélyt jelentő körülményként értékelhetik. Ilyen változások lehetnek a biztonsági szolgálatok, vagy rendvédelmi szervek kommunikációjának megjelenése, intenzitásának hirtelen változása környezetükben. Például egy terrorcsoport tagjának terepen történő mozgása során az őt esetlegesen ellenőrző (követő) biztonsági szolgálat által használt frekvenciában – már ha ez ismert az érintett előtt – történő forgalmazás megjelenése már ellenintézkedést (például a cselekmény befejezése, vagy épp meg sem kezdése) válthat ki.

- az elektronikai ellentevékenység;

  Az elektronikai ellentevékenység célja, hogy az elektromágneses és irányított energiák alkalmazásával csökkentse vagy akadályozza az elektromágneses spektrum hatékony használatát a szembenálló fél számára.

  Három fő szakterületre bontható:

  - elektronikai zavarás;
  - elektronikai megtévesztés;
  - elektronikai pusztítás; [87]

  E szakterület módszereit érintően lehet legkézzelfoghatóbban érezni a kiberterrorizmus megjelenését, hiszen ezek sikeres alkalmazása esetében már az

információs társadalom entitásai – a funkcionális információs infrastruktúrák zavarain keresztül – akár azonnal, saját érintettségük okán is érezhetik az érintett információs infrastruktúra működésében jelentkező zavarokat.

IV. 1. 1. Elektronikai zavarás

Az elektronikai zavarás az elektromágneses energia szándékos kisugárzását, visszasugárzását vagy visszaverését jelenti azzal a céllal, hogy ez által akadályozzuk a megtámadott infrastruktúra elektronikai eszközeinek vagy rendszereinek hatékony működését. Az elektronikai zavarok olyan elektromágneses sugárzások, melyek megnehezítik, vagy kizárják az elektronikai eszközök útján továbbított hasznos jelek vételét és az információk kiszűrését. Az infrastruktúrákba integrált vevőegységekre hatva az elektronikai zavarok torzítják a megfigyelt és a végberendezés által rögzített jeleket, információkat, megnehezítik, illetve kizárják az adatforgalmazás lehetőségét, a cél felderítését, csökkentik a felderítő eszközök megkívánt hatótávolságát, pontosságát. [88]

Az elektronikus eszközök működésük során az úgynevezett elektromágneses környezetben működnek, melynek vannak természetes és mesterséges összetevői, kisugárzásai is. A természetes kisugárzások lehetnek atmoszferikus, kozmikus, valamint a Föld körüli térség szporodikus elektromágneses sugárzásából adódó elektronikai zavarok. A mesterséges elektronikai zavarok az elektronikai hullámok energiáját visszaverő, illetve az elektromágneses rezgéseket kisugárzó berendezések által keltett zavarok, melyek akadályozzák az elektronikai eszköz rendeltetésszerű működését. A zavar előállításának szempontjából passzív és aktív eszközöket különböztetünk meg. A passzív elektronikai zavarok reflexió útján, valamely elektromágneses energiát visszaverő tárgy által hozhatók létre. Ez a módszer a teljes frekvencia spektrumon alkalmazható, azonban térben, időben, frekvenciánként hatása, jellege változó. Az aktív elektronikai zavarok az elektromágneses rezgéseket előállító berendezések működése, sugárzása révén alakulnak ki, tehát a szándék tükrében meg lehet különböztetni szándékos és nem szándékos zavarokat. A nem szándékos elektronikai zavarok a berendezések működéséből adódó természetes eredetűek, vagyis olyan elektromágneses sugárzások, melyek a berendezés rendeltetés szerinti normális működése, illetve technikai hiba következtében jönnek létre. [89:133]

A kiberterroristák ezzel a módszerrel azt kívánják elérni, hogy az információs infrastruktúrák elektromágneses spektrumban működő elektronikus rendszerelemeinek rendeltetésszerű működését ártó szándékkal, mesterségesen előállított, adott hatásmechanizmusú zavarás céljából létrehozott jelstruktúrákkal akadályozzák, megbontsák, vagy a berendezéseket speciális üzemmódba kényszerítsék. E tevékenység irányulhat közvetlenül az információs infrastruktúra ellen (például anyagi kár okozása a szolgáltatások kiesése (kötbér), újabb, fejlettebb és így költségesebb eszközök beszerzése, bizalomvesztés révén), vagy közvetve, a szolgáltatások kiesése által a felhasználók ellen (például adathozzáférések meghiúsítása, rendvédelmi erők kommunikációjának szabotálása, vagy vészhelyzetek bejelentésének akadályozása).

IV. 1. 2. Elektronikai megtévesztés

Az elektronikai megtévesztés olyan hamis jelek szándékos kisugárzását, visszasugárzását vagy visszaverését jelenti, amely megtéveszti, félrevezeti az információs infrastruktúrába integrált elektronikai alrendszerben működő humán, vagy gépi döntéshozatali folyamatok működését. E tevékenységnek az a célja, hogy az adott rendszerbe bejuttatott jelek, információk szintaktikailag és szemantikailag is egyaránt helytállóak legyenek, illeszkedjenek az adott szituációhoz, helyzethez, ugyanakkor hamis voltuk miatt olyan hibát okozzanak, melyek helytelen döntéseket eredményeznek a megtámadott információs infrastruktúrában.

A hatékony elektronikai megtévesztés feltétele egyrészt, hogy a másik félnek érzékelnie kell a megtévesztő jeleket, másrészt pedig e tevékenységeknek - hogy a félrevezetést ne lehessen felfedezni - valóságosnak is kell látszaniuk. Ennek érdekében az elektronikai megtévesztés részletes és alapos tervezést, előkészületet, koordinációt és végrehajtást igényel. [84]

E módszer lehetőségeivel a kiberterrorizmus viszonylag könnyen tud élni, céljait magáénak tekintheti, hiszen számos olyan infrastruktúra létezik, melyek a beérkező adatokra építkezve rendkívül fontos társadalmi igényeket szolgálnak ki. Például ilyen cél lehet egy repülőtér közelében elhelyezett, megfelelően konfigurált és ott működésbe hozott hamis jeladó, amely a valóságostól eltérő adataival veszélybe sodorja a körzetében repülő repülőgépeket, összezavarja a légiközlekedés rendjét, de ide sorolhatók a mobilhálózatok kapacitásait lefogó hamis eszközök is.

A kiberterrorizmus, a jellegéből adódóan azonban az e körbe tartozó lehetőségeknek csak a szűkebb halmazával, főleg a navigációs, kommunikációs és lokációs eszközök megtévesztésével tud élni. Ezeket a funkcionális információs infrastruktúrák által nyújtott szolgáltatásokat a társadalom széles köre (magánszemélyek, vállalkozások, vészhelyzeti szervezetek, kormányzati szervek) használja, zavaraik azonnali hatást (gazdasági kár, vészhelyzet, félelem és bizonytalanság) váltanak ki az információs társadalomban.

IV. 1. 3. Elektronikai pusztítás

Az elektronikai pusztítás az elektronikai ellentevékenység része, az elektronikai hadviselés támadó fegyvere, mely minden olyan technikát, módszert és eszközt felhasznál, ami az elektromágneses és más irányított energiák révén képes működésképtelenné tenni az ellenség elektronikai eszközeit, rendszereit. A haditechnológia jelentős fejlődésének eredményeképp az elektronikai hadszíntéren megjelent az irányított energiával operáló hadviselés, mely már pusztító fegyvereket is képes adni a hadviselő felek kezébe.

Az elektronikai pusztítás az elektromágneses és egyéb irányított energiák, vagy – sok tanulmány szerint – az önrávezetésű fegyverek bevetését jelenti, annak érdekében, hogy az ellenség elektronikai eszközeiben, ideiglenes vagy huzamosabb ideig tartó zavarokat, kárt okozzanak, a működtető személyzetet pedig harcképtelenné tegyék. Az irányított energiájú fegyverek körébe tartoznak a nagyenergiájú akusztikus és rádiófrekvenciás sugárforrások, az impulzusbombák, lézer- és részecskefegyverek. [89:39]

A technológiai fejlődés következtében az elektronikai eszközökben és a számítógépekben használt mikroprocesszorok méretének redukálása miatt a vezetőrétegek vastagsága már olyan rendkívüli mértékben lecsökkent, hogy kellő nagyságú sztatikus - külső vagy belső forrásból származó - túlfeszültség hatására villamos átütés jöhet létre a rétegek között, amely roncsolja, és így működésképtelenné teszi az alkatrészeket. E jelenséget használják ki az elektromágneses impulzus elvén működő fegyverek, melyek képesek a megfelelő nagyságú elektromágneses teret irányítottan létrehozni a mikroprocesszorok környezetében.
Ezek az eszközök alkalmazhatók bombaként (E-bomba), amely egy bizonyos magasságban felrobbantva, közel kör alakú területen az összes működő elektronikai berendezést képesek tönkre tenni. Másik alkalmazási mód, amikor az eszköz az adott célpont felé irányítva nagy energiájú impulzusok kibocsátásával rongálja a kiszemelt berendezéseket. Utóbbinak előnye,

hogy míg az E-bomba csak egyszer alkalmazható, addig a rádiófrekvenciás fegyver többször is bevethető egyéb nyom nélkül. [84]

Az elektronikai pusztítás eszközrendszerébe tartozó berendezések osztályozását többféle módon el lehet végezni, és lehet vizsgálni őket a használati terület (szárazföldön, levegőben, űrben használt eszközök), az okozott sérülés (halálos és nem halálos erejű, úgynevezett nem ölő fegyverek) szerint is:

- Nagyenergiájú rádiófrekvenciás fegyverek

  E fegyvertípusok esetében nagy energiájú rádióhullámot bocsát ki a szerkezet, és az impulzus károsítja a célban található elektronikát. E fegyvereket a magastól (100 MHz) az ultra magas frekvenciáig terjedő skálán lehet hangolni (5 GHz), s így az adott intervallumon belül minden frekvencián egyszerre tudnak hatni, ami maximalizálja a pusztító erőt.

  A mikrohullámú fegyverek hatalmas előnye, hogy területet is képesek lefogni, ugyanakkor a széles frekvencia tartománynak, valamint a pontosságnak köszönhetően akár egyes célpontok is támadhatóak, mely révén elkerülhető, hogy a célterületen tartózkodó saját eszközök is megsérüljenek. További előny, hogy az energiájukat kevésbé csökkentik a természeti jelenségek (például a köd), valamint a beállításoktól függően úgy lehet ezekkel az eszközökkel támadásokat, szabotázsakciókat végrehajtani, hogy magát a támadás forrását fel sem ismerik. Az alacsonyabb frekvencia tartományokban megzavarhatók az elektronikai eszközök működése, míg a magas frekvenciatartományban tönkre is tehetők.

  A mikrohullámú fegyverek elsősorban az elektronikai eszközök ellen hatásosak, mivel többnyire rövid és igen erős energiaimpulzust bocsátanak ki, és gyakorlatilag – megfelelő erősség esetén – szétégetik a mikrohullámú sugárzás ellen nem védett célpontot. Ugyanakkor ezek az eszközök a célpontot jelentő infrastruktúra rendszerelemeit működtető személyzet ellen is hatásosak, mivel olyan fiziológiai folyamatokat indíthatnak el bennük, melyek alkalmatlanná teszik őket munkavégzésre, de akár egészségüket is károsíthatják.

  Ezek a fegyverek terrorcselekményekben szinte bármilyen elektronikus berendezés ellen bevethetők, akár a főcsapásként (például valamely kritikus infrastruktúra vezérlését ellátó alrendszer ellen), akár hagyományos terrorcselekmény

kiegészítéseként, annak hatásának súlyosbítása érdekében (például robbantásos merényletet követően a rendészeti és vészhelyzeti erők kommunikációjának megszüntetésére).

- Lézerfegyverek

  A lézerben használt fényerősítés mechanizmusából és a folyamatból eredően a fényforrásból kilépő fény kis széttartású, az elemi hullámvonulatok a nyalábban nagymértékben szinkronizáltak, és nagymértékben egyszínűek. A lézerfény e jellemzői miatt nagy energiasűrűség érhető el a nyalábban, azaz kis keresztmetszeten viszonylag nagy elektromágneses energia halad át.

  A lézerek romboló ereje nemcsak a nyaláb energiasűrűségétől, hanem a teljesítménytől is függ, minél nagyobb az időegység alatt besugárzott energia, annál nagyobb a roncsoló hatás. A lézernyaláb roncsoló hatása szempontjából a céltárgy felületének tulajdonságai is szerepet játszanak, minél nagyobb a céltárgy felületének abszorpcióképessége a lézerfény hullámhosszán, annál nagyobb a roncsoló hatás. A lézerfény hullámhosszától függően a roncsolás mechanizmusa is más.

  Az infravörös tartományban a roncsolás termikus jellegű, azaz a céltárgy által elnyelt lézerfény a céltárgy atomjainak, molekuláinak rezgését gerjeszti, ami a hőmérséklet növekedését jelenti. Ennek hatása lehet a céltárgy felületének megolvadása, vagy hőre bekövetkező kémiai átalakulása. Az ultraibolya tartományban a lézerfény már nem az atomok, molekulák rezgéseit gerjeszti, hanem azok elektronburkával lép kapcsolatba, így a közöttük fennálló kapcsolatokra közvetlenül hat és közvetlen anyagszerkezeti változásokat okoz, amelyek a felület roncsolódását okozzák.

  A kiberterroristák a lézerfegyvereket az energiasűrűségtől és a teljesítménytől függően többféleképpen is felhasználhatják. Tipikus példa a kisebb energiasűrűségű alkalmazásokra az optikai tartományban működő berendezések érzékelőinek működésképtelenné tétele. Ilyenek a látható, vagy infravörös fényben működő kamerák képérzékelői, a mozgásérzékelő optikai szenzorok, vagy akár az optikai elven működő gázdetektorok, de az éjszaki célzó berendezések, éjjellátó eszközök ellen is alkalmazhatók. Mivel egyes kommunikációs eszközök fényhullámokat használnak

információhordozóként, ezek esetében a kommunikáció zavarása, megakadályozása lehet a cél.

Ugyanakkor a lézerek a kiberterrorizmus esetében célpontként is szolgálhatnak. A jelfeldolgozás, jeltovábbítás egy része ugyanis az optikai tartományba eső frekvenciákat használja, ezért pl. az optikai kábelekhez a vivő elektromágneses hullám (fény) előállítására szilárdtest lézereket használnak, melyek működését akár elektronikus, akár optikai módon is lehet befolyásolni, zavarni.

Humán erők elleni felhasználásra is folytak már kísérletek, melynek legegyszerűbb módja a látás ideiglenes blokkolása, vagyis a szemre irányított lézersugárral történő ideiglenes, vagy részleges, esetleg végleges látásvesztés előidézése. Ez a különböző fegyver-, vagy védelmi rendszerek kezelőinek zavarását, vagy munkaképtelenné tételét jelenti. Hátránya, hogy a nyalábot pontosan a szemre kell irányítani, egy nyaláb egyszerre csak egy ember ellen alkalmazható.

A lézerfény egyéb használatai közül legismertebb a célmegjelölés, amikor adott hullámhosszúságú, valamilyen modulációval ellátott és legtöbbször folytonos, kis energiájú lézernyalábot irányítanak az adott céltárgyra, és a visszaverődő, legtöbb esetben szórt lézerfényt a fegyverrendszer célzó berendezése detektálja, megállapítja a szóró tárgy helyzetét és a fegyvert ennek alapján vezérli. Ugyanakkor ezen elv alapján a kiberterroristák képesek lehetnek arra, hogy megfelelő technikai felszereltség mellett fixen telepített bombákat robbantsanak fel, ha például egy haladó járművet, vagy egy infrastruktúraelemet távolról, adott pillanatban lézermegjelöléssel akarnak megsemmisíteni.

Kiberterrorizmus esetében a lézerfegyverek alkalmazásának korlátait a méretek és az energiaellátás problémája jelenti, amennyiben nagyobb mértékű roncsoló hatás a cél, így e területeken történt technológiai áttörésig tömeges elterjedésükkel nem kell számolni.

- Részecskesugár fegyverek

  E fegyverek az atomok, ionok, vagy elektronok gyors, összehangolt, egy irányú mozgásából származó hatalmas energiát használják fel arra, hogy célpontjaikban kárt

okozzanak azáltal, hogy megbontják annak molekula-, atom-, vagy elektronszerkezetét. A részecskesugár fegyvereknek két típusa létezik: az egyik megoldásban töltött részecskéket használnak, míg a másikban alapállapotú, nem töltött részecskéket gyorsítanak fel.

A részecskesugár fegyverek lényegében a részecskegyorsítás elvén működnek, azonban a jelenleg elérhető technológia szintjén a részecskesugár fegyverek csak jelentős korlátokkal valósíthatóak meg. Ilyen fegyver harctéren bevethető konstrukcióját gyakorlatban még senki sem mutatta be, mivel hatalmas mennyiségű energiát, igen nagy mágneses mezőt és igen hosszú gyorsítási pályát – valamint legtöbbször vákuumot is – igényel.

Ezek a fegyverek a kiberterrorizmus eszközrendszerében belátható időn belül nem bukkannak fel, azonban egy technológiai ugrást követően nagy valószínűséggel valós fenyegetést fognak jelenteni az információs infrastruktúrákra.

IV. 2. 1. Professzionális, fizikai hatáson alapuló eszközök

Tekintettel arra, hogy az elektromágneses spektrum, illetve az itt zajló kommunikáció a katonai doktrínákban kiemelt jelentőségű szereppel bír, ezért nem meglepő, hogy e területen jelenik meg a legtöbb, illetve legnagyobb mértékű komplexitással megalkotott – más információs, fegyver-, fegyverirányítási alrendszerekkel együttműködő – professzionális eszközrendszer.

Az elektronikus hadviselés területén a szembenálló felek között folyó óriási verseny miatt folyamatosak az erőfeszítések a meglévő képességek tovább-, illetve az új képességek kifejlesztése, valamint ezen eszközöknek a megóvása területén. A fejlesztések magas költségei miatt ezeket az eszközrendszereket – egy-két országtól eltekintve (például Egyesült Államok, Oroszország) – jellemzően az alkalmazó országok nem is egyedül fejlesztik, hanem szövetségi rendszereken belül a költségeket, képességeket és tudásbázist megosztva közösen gyártják.

Az elektronikai hadviselés eszközrendszereinek képességeit, működési paramétereit az üzemeltetők a fegyvernem kialakulása óta igyekeznek eltitkolni, mivel ezek esetleges ismeretében a szembenálló fél hatékonyan képes akadályozni, kijátszani azokat.

Ugyanakkor a kiberterrorizmus eszközparkjába e körbe tartozó modern berendezések felbukkanása egyáltalán nem várható, mivel be- vagy megszerzésükre, karbantartásukra,

rejtésükre és üzemeltetésükre a törvényen kívül álló irreguláris szervezeteknek alapvetően nincs lehetőségük, illetve erre jellegükből adódóan nem is alkalmasak.

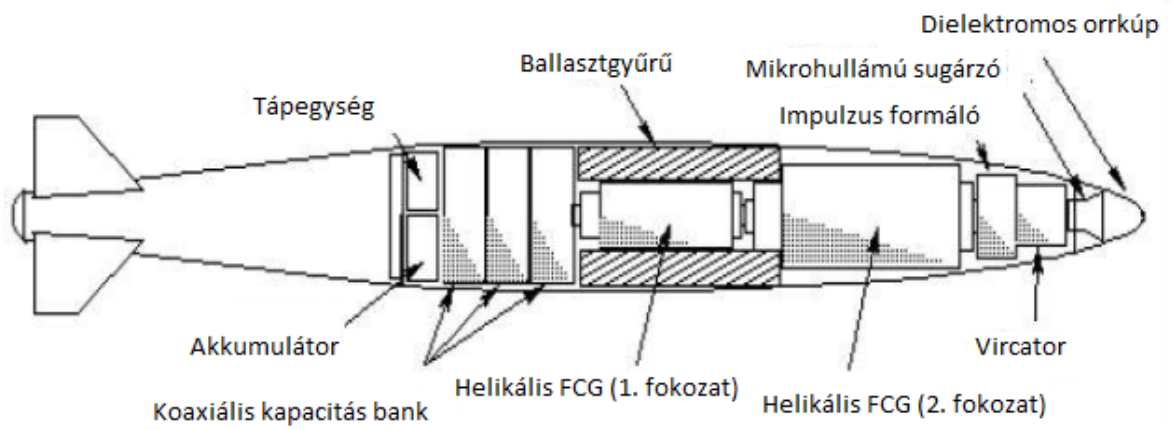
A professzionális fizikai hatáson alapuló eszközök közül a nagy energiájú rádiófrekvenciás fegyverek kiemelése azért lehet indokolt, mert a kiberterrorizmus számára ezeknek az eszközöknek a csökkentett képességű, kisebb alkalmazhatósági körrel rendelkező másolatai a vonzóak és elérhetőek, mind kezelhetőség, mind az üzemeltetéshez szükséges szaktudás, mind pedig a költségek tekintetében. A kibertérben a terroristák az infrastruktúra rendszerelemei ellen ezekkel az eszközökkel tudják elérni azt a pusztító hatást, amit a fizikai térben korábban a robbantásokkal tudtak csak kiváltani, ugyanakkor ezzel a módszerrel közvetlenül az emberi életekben sem tesznek kárt, ami megítélésüket akár javíthatja is.

A nagy energiájú rádiófrekvenciás fegyverek közül a leghatékonyabb az elektromágneses impulzusbomba (EMP), melynek vannak nukleáris (NEMP) és nem nukleáris (NNEMP) alapú implementációi is. A hidegháború elmúltával a nukleáris alapú elektromágneses impulzus fegyverek háttérbe szorultak, de a nem nukleáris alapú eszközök fejlesztését töretlenül folytatják.

A NNEMP fegyverek lényegesen szűkebb tartományban (kisebb hatóerővel, kisebb hatókörrel) működnek, azonban másodlagos hatásaik (például radioaktivitás) nincsenek, vagy el is hanyagolhatók, így kiválóan alkalmazhatók precíziós csapásokat igénylő műveletekben. A nem nukleáris elektromágneses impulzusfegyverek többféle megoldást használnak a nagy energiájú elektromágneses lökéshullám előállítására. A rádióhullámok fegyvertechnikai alkalmazása esetén meg lehet különböztetni:

- impulzusüzemű,
- periodikusan folytonos rádióhullámokat sugárzó rádiófrekvenciás fegyvereket.

Az ilyen fegyverek három részből állnak: egy energiaforrásból, melyek a mikrohullámok generálásához szükséges nagy mennyiségű energiát előállítják, tárolják, egy mikrohullámokat generáló eszközből, és egy antennából, mely a kívánt irányba sugározza a generált mikrohullámokat.



8. ábra Az E-bomba (NNEMP) elvi felépítése [90]

A fenti megoldás szintén nagyon egyszerű, hiszen a robbanóanyagok robbanási karakterisztikái és a kialakuló nyomáshullámok jól leírtak és tervezhetők. Az energiát előállító eszköz többféle lehet: Marx generátor vagy fluxus kompressziós generátor, de más eszközök is alkalmazhatók az újabb fejlesztéseknek köszönhetően. A csőben robbantással egy haladó lökéshullámot kell előidézni, amely az antennával ellentétes oldalról indul és megfelelő sebességgel halad végig a fémcsövön, hogy az tágulva a kívánt sebességgel zárja rövidre a tekercset. A rövidzárás sebessége fogja meghatározni azt, hogy a kialakuló elektromágneses impulzus spektrumának maximuma mely hullámhossztartományba esik. Ezt a fluxus kompressziós generátort használó NNEMP fegyverek esetében általában úgy állítják be, hogy a mikrohullámú tartományba essen. Mivel az impulzusbombában alkalmazott fluxus kompressziós generátort a robbanótöltet hozza működésbe, ennek következtében az eszköz megsemmisül. [91]

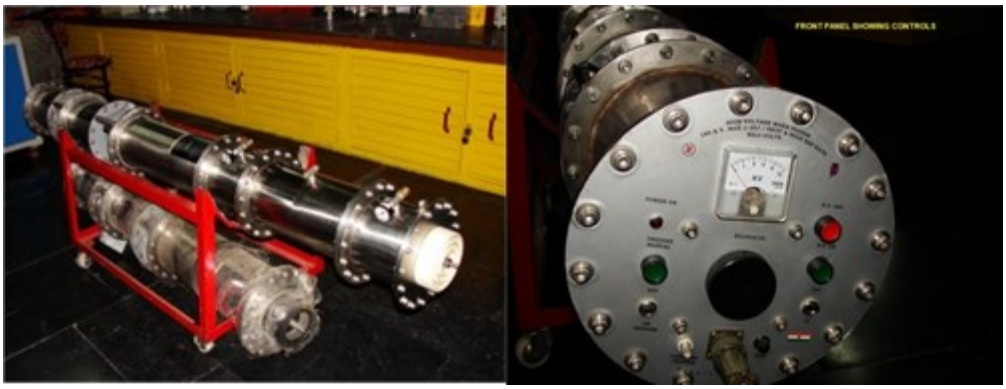
IV. 2. 2. Nem professzionális, fizikai hatáson alapuló eszközök

A kiberterrorizmus lehetőségeihez mérten próbál a professzionális fizikai hatáson alapuló eszközöknek, ha nem is birtokába kerülni, de azok képességeit alacsonyabb hatásfokkal ellátó berendezéseket beszerezni. Mivel az információs társadalom modern, „okos” nagyvárosaiban az információs infrastruktúrák rendszerelemei környezeti és működési paramétereikből adódóan nagy sűrűséggel vannak telepítve, így egy, az elektromágneses spektrumban végrehajtott kibertámadás – például a nagy energiájú rádiófrekvenciás sugarak alkalmazása, aminek célja a felvezetők károsítása, a mikro-áramkörök (processzorok, memóriák) túlterhelése, a villamos alkatrészek szigeteléseinek átütése és ezáltal az elektronikai eszközök

tönkretétele – nagyszámú eszközben kárt tehet, melyek helyreállítási költségei, illetve a szolgáltatás-kiesésből adódó károk jelentősek lehetnek, ezért csábító célpontot jelenthetnek a kiberterrorizmus számára. [92]

Azonban a fizikai pusztítás hagyományos eszközeivel a modern információs infrastruktúrák (például infokommunikációs hálózatok) technológiájának sajátosságaiból adódóan egy földrajzi területen egy időben elérhető, szétszórtan elhelyezkedő rendszerelemek (például mobilhálózatok bázisállomásai) lerombolása nehezen kivitelezhető. A kibertámadás végrehajtása szempontjából további nehézség, hogy az infrastruktúra használóinak eszközei (például a mobil kommunikációs eszközök esetében) nagy számuk, valamint a térben szétszórt és rejtettnek tekinthető elhelyezkedésük révén a fizikai pusztítás módszereivel közel egy időben nem iktathatóak ki.
Ugyanakkor egy kérdéses területen a kiberterroristák a mobil kommunikációs rendszerek elemeit nagy hatékonysággal tudják pusztítani elektromágneses fegyverekkel. A jelenség hasonló ahhoz, mint amikor egy madárrajra golyós, vagy sörétes puskával lőnek. Golyós puskával vagy sokáig tart és így lehetetlenné válik elegendő számú értékes madár elejtése, vagy egyszerre több helyről, több golyós puskával kell lőni. Míg sörétes puskával elég a madárraj közepére célozni. Lehet, hogy a rajban vannak olyan madarak is, amelyek nem érdekesek a vadász számára, viszont az eltalált nagyszámú madár között sokan lesznek olyanok, amelyek értékes vadászzsákmányt jelentenek.

Fentiek okán a nem professzionális fizikai hatáson alapuló eszközök alkalmazásának lehetősége egyre valószínűbb, mivel a megalkotásukhoz szükséges tervrajzok, használatukat, telepítésüket magyarázó leírások megtalálhatók az interneten, továbbá ezen eszközökhöz szükséges alkatrészek kereskedelmi forgalomban beszerezhetők és gyakorlattal házilag is megalkothatók, így pedig a potenciális kiberterroristák számára könnyen elérhetők.
A kevésbé elszánt, kisebb támadó potenciállal rendelkező kiberterroristák részéről nem az egyszer használható, robbanással működésbe hozható eszközök alkalmazására lehet elsősorban számítani, hanem a többször felhasználható – bár kisebb hatótávolságú és gyengébb – berendezések használata merülhet fel.
Ugyanakkor ilyen többször felhasználható berendezések már készre szerelt állapotban, pontosan paraméterezve, üzemeltetési utasításokkal is megtalálhatóak és megrendelhetők az különböző internetes oldalakon.

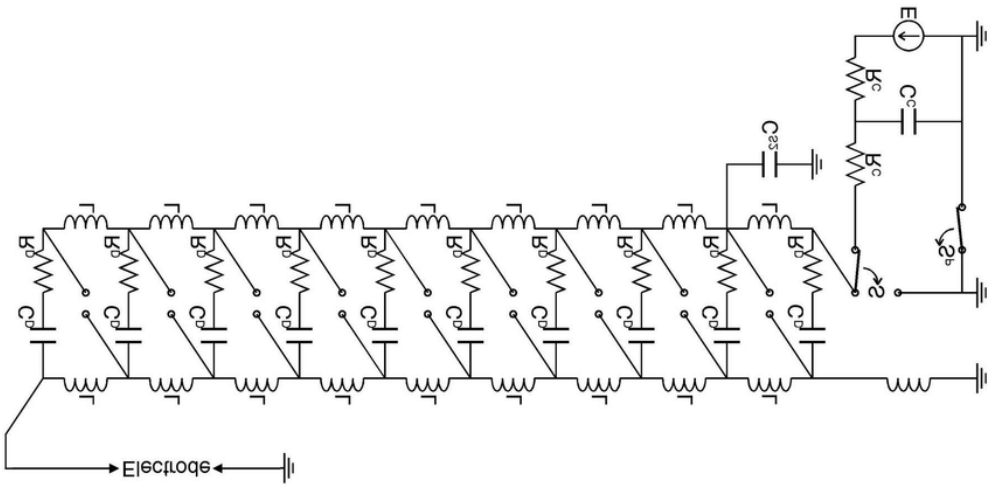


9. ábra Az Internetről rendelhető EMP eszközök [93]

Azonban az ilyen eszközök kereskedelemi forgalomban kapható alkatrészekből is összeállíthatók, melyeket a kiberterroristák könnyedén felhasználhatnak céljaik elérése érdekében. E körben felhasználható az egyszerű mikrohullámú sütő magnetronjától kezdve, régi televíziós készülékek képcsövéig, a fényképezőgépek nagyteljesítményű vakujáig minden, mely eszközök működési elve csaknem azonos. Feltölteni egy energiatárolót, ami akár egy egyszerű fényképezőgép vakujában található kondenzátor is lehet, és adott időben és helyen a lehető legrövidebb idő alatt kisütni. [92]

10. ábra EMP mikrohullámú sütőből [94]

A kiberterroristák talán legkönnyebben a Marx generátort építhetik meg. Ennek működési elve a párhuzamosan és sorosan kapcsolt feszültségforrások tulajdonságain alapul. Azonos feszültségforrásokat – például közönséges alkáli elemeket – párhuzamosan kapcsolva a kapcsolás közös pólusain mérhető feszültség megegyezik az egyes elemek kapocsfeszültségével. Ugyanakkor ugyanezen elemeket sorba kötve, a szabad kapcsokon mérhető feszültség az egyes elemek kapocsfeszültségének az elemek számával megegyező többszöröse lesz. Vagyis minél több elemet kapcsolunk sorba, annál nagyobb feszültséget kapunk.



11. ábra A Marx generátor elvi felépítése [95]

Egy rövid és nagy teljesítményű elektromágneses impulzus létrehozásához egy (általában tekercsből és antennából álló) rezonátorra nagyon rövid idő alatt nagy feszültséget és nagy áramerősséget kell kapcsolni. Ez alkáli elemekkel, akkumulátorokkal közvetlenül nem oldható meg, azok elektrokémiai működési mechanizmusai miatt. Ugyanakkor a kondenzátorok nagyon jó elektromos energiatárolók ebből a szempontból, mert a tárolt energiát nagyon gyorsan tudják leadni, nagyon gyorsan kisüthetők. Ráadásul párhuzamosan kötve elegendő számú azonos kondenzátort, egyszerű egyáramú forrásokkal viszonylag kis feszültségre könnyen feltölthetők.

Mivel a párhuzamosan kapcsolt kondenzátorok kapacitása nagyobb, mint az egyes kondenzátoroké, így lassú feltöltéssel is sok töltés, azaz nagy energia halmozható fel bennük. A töltőegységnek tehát nem kell különlegesnek lennie. Problémaként merülhet fel az, hogy miként lehet megfelelő módon, vagyis gyorsan és egyszerre a párhuzamos kapcsolásból soros kapcsolást létrehozni, vagyis az azonos feszültségre feltöltött kondenzátorokat sorba kapcsolni.

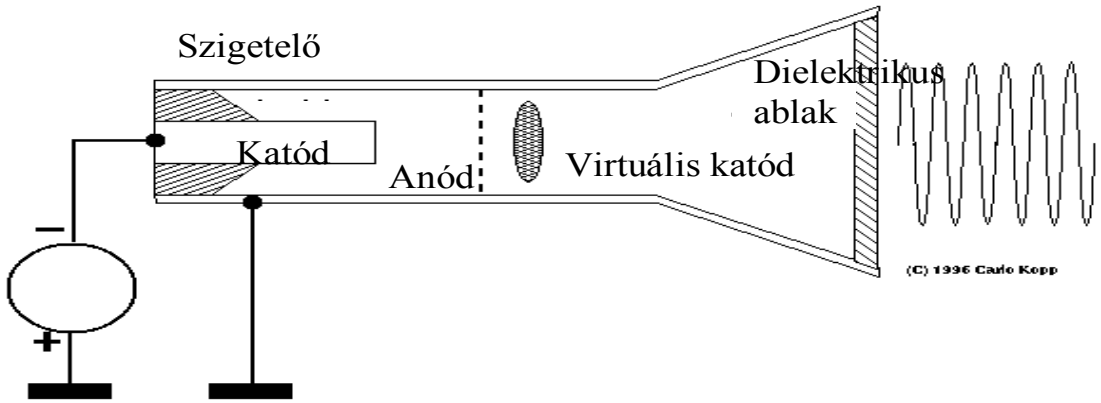
A Marx generátorban ehhez szikraközöket alkalmaznak. Minden kondenzátor ellentétes polaritású kapcsai közé egy-egy szikraköz van beiktatva, amelyek átütési feszültsége úgy van beállítva, hogy a párhuzamos kapcsolás feszültségén még ne keletkezzen áthúzás az elektródák között. Amikor az első szikraközt egy indító impulzus (trigger) segítségével kisütik, az első és a második kondenzátor ellentétes polaritású kapcsai a szikrán keresztül összekapcsolódnak.

Hogy mennyire is könnyű előállítani egy Marx generátort, a Szegedi Egyetem Kísérleti Fizikai Tanszékének kutatói is demonstrálták még az 1980-as években. A kutatók az embargós eszközök kiváltása érdekében megépítettek egy olyan excimer gázlézert, amelyben

kapcsolóelemként gépkocsi gyújtógyertyákból kialakított szikraközök, míg a kondenzátorok a televíziózásban használt kereskedelmi forgalomban használt nagyfeszültségű kondenzátorok voltak. A nagyfeszültségű, 220 V-ról működő töltő transzformátort házilag készítették, melynek feszültségét a mikrohullámú sütőkben is használt nagyfeszültségű diódákkal egyenirányították. A vezérlő elektronika tirisztoros gépkocsi-gyújtás volt. Gyakorlatilag minden eleme a lézer elektromos, elektronikai rendszerének házilag elkészített, vagy kereskedelmi forgalomban beszerezhető elem volt. A lézer működött, karakterisztikái hasonlók voltak a csúcstechnológia segítségével előállított lézerekéhez. [96]

A folytonos, periodikus jel előállítására alkalmas eszközök közül legelterjedtebb a virtuális katódú oszcillátor, amely a rádiófrekvenciás fegyverek abba a csoportjába tartozik, amely – a fluxus kompressziós generátort használó fegyverekkel ellentétben – többször is felhasználható [97].

12. ábra Különböző Vircatorok [98]



13. ábra A Vircator és elvi felépítése [99]

A Vircator a hagyományos televízió készülékekben is megtalálható katódsugárcsőhöz hasonló elven működik. A különbség itt az, hogy nem meleg katódos eljárással hoznak létre elektronnyalábot és azt nem vezetik egy fluoreszkáló ernyőre. A hidegkatód egy vezető fémcső végében helyezkedik el szigetelten. Az anód egy elektronok által könnyen áthatolható, például rozsdamentes rács formájában koaxilásan, a katódtól megfelelő távolságra van. A katód és az anód közé nagyfeszültségű, nagyteljesítményű impulzust kapcsolnak, amit például Marx generátorral állítanak elő. A katódból a nagy elektromos térerősség hatására kilépő elektronok egy része olyan sebességre gyorsul, hogy áthalad az anód síkján és a cső vége felé folytatja útját.
Mivel az elektron felhő töltése negatív, az anóddal szemben úgy viselkedik, mint egy katód, ezért hívjuk ezt virtuális katódnak. A feszültség impulzus időtartama alatt így az anód hatására az elektronok lelassulnak és megindulnak az anód felé. Megfelelő geometria elrendezés és feszültségviszonyok esetén az elektronok oszcilláló mozgásba kezdenek. A mozgó töltések maguk körül változó elektromágneses teret keltenek. A megfelelő geometriai kialakítás azt is jelenti, hogy a cső hullámvetőként működik, így a kilépő elektromágneses hullám jó irányítottsággal rendelkezik.
A létrejövő elektromágneses impulzus igen nagy teljesítményű is lehet, jól tervezett eszköz esetében akár Gigawattos impulzusok is elérhetők. A néhány 100 MHz tartományba eső impulzusokkal elsősorban az elektronikus kommunikáció zavarását lehet hatékonyan elérni, míg a GHz-es tartományba eső impulzusokkal az elektronikai eszközök tönkretételét.

Az ilyen fegyverek észlelése, felderítése nehéz, könnyű őket álcázni, üzemen kívül nem bocsátanak ki olyan jeleket, sugárzást, amivel azonosíthatók lennének. Mivel kereskedelmi forgalomban használt, mindennapi eszközökből is fel lehet építeni őket, ezért az alkatrészek vásárlása nem kelt gyanút, ugyanakkor a fegyverek antennái akár egy mikrohullámú internet kapcsolat létrehozására szolgáló digitális antennának is álcázhatók – például egy épület homlokzatán.

Az NNEMP fegyverek talán legveszélyesebb tulajdonsága az, hogy viszonylag távolról is alkalmazhatóak, a támadásra való felkészülés nehezen észlelhető, a támadásnak pedig külső jele nincs. A sikertelen támadásnak nyoma nem marad, egy sikeres támadásnál pedig a megtámadott kommunikációs rendszerek üzemeltetői és felhasználói csak a hatást, azaz eszközeik tönkremenetelét érzékelik.

Az elektromágneses impulzusok elleni védekezésnek csupán gazdasági korlátai vannak, a berendezések gyártóinak – elsődlegesen a megrendelők gazdaságossági szempontjainak tükrében – kell azt eldönteniük, hogy mit és mi ellen védjenek. Az elektromágneses romboló impulzusok elleni védekezés hatékony eszköze az elektromágneses árnyékolás, ami azonban bizonyos esetekben – például antennák, detektorok esetében – nem vitelezhető ki megfelelő módon. Az árnyékolás a mobileszközök esetében is korlátokat jelent.

Prognosztizálható, hogy az információs infrastruktúrák üzemeltetőinek, illetve az ő hálózatukon kiemelt jelentőségű szolgáltatásokat nyújtó felhasználóknak a fontosabb elektronikus eszközeik védelmének szintjének emelésére az elkövetkezendő időszakban fokozott figyelmet kell fordítaniuk.

IV. 2. Logikai eszközök

Az információs infrastruktúrák elleni támadások eszköztárában egyre nagyobb súlyt kapnak az olyan megoldások, melyek az infrastruktúra rendszerelemeinek fizikai zavarása, pusztítása helyett inkább az érintett rendszer „virtuális határain" belül működnek, ott fejtik ki hatásukat. Ezek az új támadási módszerek, eszközök az informatika minden társadalmi területet érintő robbanásszerű fejlődésének velejárói, melyet a katonai doktrínában számítógép-hálózati hadviselésként aposztrofálnak. Ez kiemelkedik más támadási módozatok közül, mivel eszközrendszere és módszerei megvalósíthatóvá teszik azt, hogy kibertéren keresztül úgy érjen el hatást, hogy a megtámadott információs infrastruktúrát annak fizikai megközelítése nélkül – akár kontinensnyi távolságból – akadályozza, rombolja, ellentétben az elektronikai hadviselés eszközeivel, melyek a célpontok viszonylagos – a támadóeszköz hatótávolságán belüli – közelségét feltételezik.

A számítógép-hálózati hadviselés (CNE-CNA-CND) eszközeinek és módszereinek alkalmazása esetében az elérendő célok gyakorlatilag megegyeznek a fizikai hatáson alapuló eszközök esetében is megfogalmazott célokkal. Itt is megjelenik:

- a célpontok felderítésének, azokról történő információgyűjtés (CNE),
- illetve az infrastruktúra rendszerelemeinek – működésük zavarásának, fizikai pusztításának – valamint a kezelt információk – tartalmának és tulajdonságainak – támadása (CNA),
- valamint az előző tevékenységek elhárításának (CND)

igénye. [99]

A logikai eszközök alatt a különböző célból létrehozott szoftvereket, támadókódokat, illetve ezek előállítására, generálásra alkalmas eszközkészleteket kell érteni. Mint ahogy utaltunk már rá, a kiberterroristák szemszögéből e megoldásoknak számos vonzó előnye van:

- Nem kell az érintett információs infrastruktúrát fizikálisan megközelíteni, a földrajzi távolság – e támadási módozatok végrehajtása során – nem értelmezhető a kibertérben, így ez a kockázatcsökkentő tényező egyfajta indikátorként hathat. Bár a támadás bizonyos szakaszaiban (például információgyűjtés, előkészítés) előfordulhatnak olyan mozzanatok, amikor a célpont megközelítése mégis indokolt lehet, ám ekkor (jogi) szempontból még nem történt meg a támadás.
- Megfelelő körülmények között a kibertér nagyfokú anonimitást képes biztosítani a kiberterroristáknak, akik így, a minimális kockázat mellett merészebben, agresszívebben, akár folyamatosan, módszereikkel kísérletezgetve, azokat finomítgatva támadhatják a kiszemelt információs infrastruktúrák körét.
- A logikai eszközök gyakorlatilag megtöbbszörözhetők, párhuzamosan működtethetők, illetve bármilyen ok miatt meghiúsult, sikertelen támadás esetén pedig korlátlanul újra felhasználhatók, továbbá megfelelő szakismeret birtokában átalakíthatók.

  A korlátlan újrahasznosíthatóságnak azonban korlátja lehet a módszer (támadókód) napvilágra kerülése, dekonspirációja, amikor az érintett infrastruktúrák, vagy a velük kapcsolatban álló egyéb támogató infrastruktúrák (például vírusvédelmi vállalatok) erről tudomást szereznek és kidolgozzák a védelem eszközeit.

A kibertér által biztosított körülmények, illetve az azokban rejlő lehetőségek (információs támadások, információszerzés illetve ezek módozati) természetesen nem csak a terrorcsoportok számára jelentenek csábítást, azt egyre erőteljesebben igyekeznek maguk az államok is kihasználni. A kibertér nyújtotta lehetőségeket egyre jobban kihasználó terrorcsoportokon túl, egyre több ország nyilvánítja ki, hogy szükségesnek tartja, hogy a kibertámadások elleni védelmi képességeit kiépítse, fejlessze, ugyanakkor a kevésbé „szemérmes”, vagy épp harcias államok egyenesen deklarálják is, hogy céljuk olyan támadó jellegű képességek fejlesztése, kapacitások kialakítása, melyek akár megelőző csapások végrehajtására is alkalmasak vélt, vagy valós ellenségeik ellen.

A színfalak mögötti fejlődést jelezheti az a körülmény, hogy egyre több incidens kapcsán történik meg az, hogy az érintett nagyhatalom megvádol egy másikat a támadással, miszerint

a másik fél kiberegysége áll a logikai eszközökkel végrehajtott támadás mögött, amit a másik fél rendre meg is cáfol. Az incidensek visszhangjaként a sajtóban, a szakirodalomban rendre visszatér az az elképzelés – amire eddig egyértelmű bizonyíték nem merült fel – hogy bizonyos ismert hackercsoportok – akik egyes országokban kiberterroristának minősülnek – és bizonyos országok reguláris kiberegységei közé egyenlőségjelet lehet tenni (például Equation Group = NSA (USA) gyanúja).

A támadóképességekről – titkos voltuk miatt értelemszerűen – pontos információkat lehetetlen beszerezni, sőt megközelítőleg becsülni sem lehet. Egyrészt, például a kifejezetten az elektronikai hadviselési rendszerek számáról, képességeiről – történetiségük okán – részleges információk fellelhetők, ugyanakkor a „virtuális térben állomásozó erők" kötelékébe tartozó személyi állomány mérete, képzettsége, eszközök fejlettsége, száma, szervezési és alkalmazási elvei, illetve ezek összképessége, hatékonysága szinte megismerhetetlen, hiszen az eszköz- és személyi állomány, valamint a mögöttük álló infrastruktúrarendszer jellegéből adódóan könnyen elrejthető, bővíthető, leépíthető, átstrukturálható, áttelepíthető. Másrészt itt az információk szerepe jelentősen felértékelődik, mivel egy lényegesen kisebb létszámmal és eszközszámmal rendelkező kiberegység – akár kibertérben működő terrorcsoport – bizonyos, a támadásban érintett infrastruktúra sérülékenységekre vonatkozó információk birtokában – melyekről a másik, akár az erőforrások többszörösével rendelkező fél nem is tud – könnyen felülkerekedhet a kibertérben és annulálhatja a szemben álló fél fölényét.

Az információs társadalom jelenlegi fejlettségi fokán mindenképpen szükségszerű, hogy egy ország intenzíven fejlessze a kibertérhez kapcsolódó védelmi képességeit, még ha a támadó képességeinek kiépítésére nem is marad erőforrása. E műszaki, gazdasági és virtuális térben folyó versengésben bizonyos országok – ipari fejlettségük, gazdasági, politikai és katonai szemléletük okán – oly mértékű előnyre tettek szert más országokkal szemben, mely kapcsán prognosztizálható, hogy ezt a lemaradást behozni már nem lehet.

A kiberfölény az érintett országoknak olyan folyamatosan rendelkezésre álló és folyamatosan fejlődő, szélesedő információgyűjtési, műveleti képességeket biztosít már, amelyekkel szemben az ellenérdekelt felek lehetőségei eltörpülnek. A megszerzett kiberfölény kényelmében szinte már ezen előnyök megóvására, fenntartására és fejlesztésére kell csak erőforrásaikat fordítaniuk.

E kiberfölény eklatáns példája az Egyesült Államok, ahol a globális kibertérhez kapcsolódó funkcionális és támogató infrastruktúrák, hardver- (például Cisco, Intel, Qualcomm stb.), szoftvervállalatok (például Google, Apple, Microsoft, stb.), szolgáltatások (Amazon, Ebay, Facebook, Linkedin (Microsoft) stb.) olyan koncentrációban találhatók meg, melyek megteremtik ezt az információs és képességbeli túlsúlyt. Az adott jogszabályi környezetben e vállalatok tudásbázisának, képességeinek birtokában olyan lehetőségek nyílnak az állami szereplők (rendvédelmi szervek, hírszerzőszolgálatok) előtt, mely képességeket más országoknak kialakítani szinte fölösleges is elkezdeni.
Például a kiberfölény kényelméből egy látókörbe került, megfigyelt e-mail cím esetében nem csak a postafiók és a kapcsolódó szolgáltatások (felhő-tárhelyek, keresések, (böngészési, vásárlási, videó, hang) előzmények, kapcsolati háló) tartalmát, aktivitását lehet azonnal megismerni, elemezni, de azonnal be lehet azonosítani az adott számítógépnek az IP címét és az alkalmazott operációs rendszert, valamint ezek birtokában a telepített vírusvédelmi és egyéb biztonsági eszközöket, továbbá a telepített programokat. Gazdasági szereplők, külföldi politikai szervezetek esetében lehetőségeket teremt gazdasági, politikai hírszerzésre (például hazánkban az Országgyűlés tagjai Apple eszközöket kaptak iCloud felhőszolgáltatással).
Az adott hardver- és szoftverkörnyezet ismeretében a fenti támadópotenciál nem csak a támadó által felderített, vagy más módon (például vásárlás révén) birtokába került, napvilágot még nem látott sérülékenységek kihasználására alkalmas, hanem célirányosan olyan szoftverkörnyezetet teremthet, melyben a támadás garantáltan sikeres. Ilyen támadás keretében az együttműködő, vagy jogszabályilag együttműködésre kényszerített hardver-, szoftvergyártóval, szolgáltatóval olyan kiskapukat építtetnek be a termékébe, mely lehetőséget biztosít az állami szervek számára egy támadás kivitelezésére (például csak és kizárólag a célpont számítógép (mobileszköz) számára készített szoftverfrissítés által).

A kiberfölény alkalmas továbbá a célpont által használt szolgáltatások (például felnőtt tartalmat szolgáltató, vagy speciális társkereső oldalak) felderítésére is, és az ott tanúsított aktivitás pedig – például biztonsági szolgálatok esetében – felhasználható az érintett identitás tanulmányozására, kompromittálására, zsarolására. Bizonyos feltételek esetében pedig technikailag meg is valósítható a technikai eszközökön, vagy a szolgáltatóknál elhelyezett tárolt tartalmak módosítása, a célpont tevékenységének szimulálása.

A fentieket az érintett felek, gyártók, szolgáltatók – piaci pozícióik megőrzése érdekében – kategorikusan tagadják, de ahogy utaltunk is már rá, a Snowden-botrány napvilágot látott

dokumentumai között számos olyan állítás van, mely alátámasztani látszik az általam kiberfölény kényelmeként aposztrofált jelenséget.

A fenti ismeretek birtokában könnyebben értelmezhető az a jelenség, hogy bizonyos, a kibertérben hátrányban lévő országok (például Oroszország, Kína, illetve maga az Európai Unió is) főleg adminisztratív eszközökkel (például adatvédelem jogcímén jogszabály-alkotással, (műszaki) cenzúrával) igyekeznek korlátozni, illetve visszaszorítani országhatáraikon belül az USA cégeinek további térnyerését. Ezzel egy időben pedig igyekeznek az érintett szolgáltatások, termékek kiváltásaként saját felügyeletük alá tartozó közösségi, üzleti megoldások felé terelni saját vállalataikat, állampolgáraikat, illetve próbálnak idegen identitásokat is megnyerni maguknak. Természetesen adottak a piaci törvényszerűségek, de részben e jelenségnek tudható be, hogy a nagyhatalmak tekintetében számos azonos funkciót betöltő – olykor állami pénzekkel támogatott – megoldás létezik (például Facebook = Tencent = VKontakte; Twitter = Weibo; Amazon = Alibaba, Google = Baidu = Yandex).

Figyelemre méltó körülmény, hogy minden érintett ország e képességének meglétét, illetve kiépítési szándékát tagadja, ugyanakkor más országot ezzel rendszerint megvádol. Erre példa, hogy az Egyesült Államok több nagy kínai elektronikai gyártót kitiltott piacairól, mivel felmerült annak gyanúja, hogy azok eszközei a kínai hírszerző szolgálatok számára hozzáférést biztosítanak az azokon kezelt adatokhoz, amit az érintett gyártók tagadnak. Ugyanakkor pedig a kínai és orosz hatóságok az amerikai vállalatok tevékenységét korlátozzák, blokkolják, mivel azok gyanújuk szerint nem garantálják állampolgáraik adatainak biztonságát. Erre szembenállásra már történt utalás, amikor a terrorcsoportok más érdekszférában történő működéséről volt szó, hiszen saját rendszereikből nem szívesen szolgáltatnak adatokat (esetleg kompromittálva azok képességét), illetve sok esetben az érintett nagyhatalom sem hozza szívesen a másik fél tudtára a látkörébe került személyek listáját.
Tekintettel a terület speciális jellegére, ezekre az értesülésekre hitelt érdemlő forrásokat, tudományos publikációkat, politikusi nyilatkozatok nem lehet találni.

Természetesen a terrorcsoportok a fenti, a kiberfölény biztosította lehetőségekkel nem tudnak élni, mivel nem képesek a kibertérben ilyen komplex hírszerző- és támadórendszereket kifejleszteni, fenntartani, finanszírozni és tevékenységüket koordinálni, így esetükben csak

egy-egy információs infrastruktúra, illetve közvetlen interdependens rendszer célirányos, ám kevésbé hatékony támadása várható. Ugyanakkor egy kibertérben működő terrorcsoport támadásának hatékonysága bizonyos esetekben – például egy csak általuk ismert sérülékenység kihasználása során – felérhet akár egy professzionális állami kiberegység hatékonyságával is.

Kiemelendő körülmény, hogy a kibertámadások eszköze maga a számítógép, mely az információs társadalom „alapeszközeként" olcsón, bárhol és bárki által könnyen beszerezhető. A kiberterrorista, vagy egy reguláris katonai szervezet tagja (információs harcosa) a megfelelő tudás birtokában ugyanazzal az eszközzel – az elérni kívánt cél függvényében – több típusú támadás kivitelezésére is képes lehet. Utóbbi a mögötte lévő állami képességek birtokában természetesen lényegesen nagyobb hatékonysággal, gyorsabban érheti el a kitűzött célt.

Tehát a professzionális és a nem professzionális logikai eszközök között technológiailag alapvetően nincs különbség, azonban a professzionális eszközök mögötti támogatás (jogi háttér, műszaki információk, finanszírozási lehetőségek, több dimenziós előkészítés és „rásegítés") olyan nagyfokú hatékonyságbeli különbséget okoz, mely mögött a nem professzionálisan fejlesztett és alkalmazott eszközök eltörpülnek. Ennek tükrében pedig egy nagyobb fokú kibertámadásról szóló információk, híradások (például egy zsarolóvírus terjedése) akár ijesztőek is lehetnek, mivel rámutathatnak arra, hogy ha egy kis támogatással rendelkező terror-, illetve bűnözői csoportok ilyen nagymértékű zavar okozására képesek az információs társadalomban, akkor egy dedikáltan erre a célra létrehozott állami szervezet a birtokában lévő, informatikai támadófegyvereknek titulálható eszközökkel milyen rombolásra képes egy másik ország információs infrastruktúráiban.

A kiberterrorizmus elleni hatékony védekezés érdekében azonban szükséges feltárni és megismerni azokat a logikai eszközök körébe sorolható módszereket, eljárásokat, melyeket a kiberterroristák potenciálisan felhasználhatnak az érintett információs infrastruktúrák ellen, és ki kell dolgozni azokat a protokollokat, melyek alkalmassá teszik a rendszereket az ellenük történő védekezésre.

A logikai eszközök a különböző felhasználói mulasztásokra, technológiai anomáliákra, műszaki, technikai gyengeségekre, konfigurálási hibákra, illetve ezek kombinációira építenek.

[100] Ezek köréből a viszonylagos egyszerűségük és így a kiberterroristák számára vonzó lehetőségeik okán – nem teljes körűen – az alábbiakban felsorolt és bemutatott módszerek ragadhatóak ki.

IV. 2. 1. Felhasználók megszemélyesítése, jogosultságaik megszerzése

A támadások egyik legkézenfekvőbb, legegyszerűbb módszere a hamis megszemélyesítés. Az információs rendszerek szolgáltatásait igénybevevők (személyek és szoftverek) legtöbb esetben csak bizonyos jogosultságok birtokában képesek hozzáférni a különböző szolgáltatásokhoz, erőforrásokhoz, az adott infrastruktúrának ezért valamilyen módon hitelesítenie kell a szolgáltatásait igénybe venni kívánó felet annak érdekében, hogy az érintett csak és kizárólag az ő számára kiosztott jogosultságokat kaphassa meg. A kapcsolat felépítésekor a kezdeményező fél elküldi azonosítóját a rendszernek, ezt követően pedig az ellenőrzi a kezdeményező felet, a kapott azonosítót összehasonlítja az adatbázisában tárolt azonosítókkal, és amennyiben egyezést talál, a kezdeményezőnek engedélyezi a rendszer használatát a talált azonosítóhoz rendelt hozzáférési jogokkal. [101]

E körbe tartozó módszerek lehetnek:

- Jelszavak kifigyelése;

  A jelszó kifürkészése a legegyszerűbb módszer, amikor is a kiberterrorista az érintett felhasználó környezetében tartózkodva kifigyeli, hogy az mit gépel be a billentyűzeten, vagy ha a felhasználó nem jegyzi meg a jelszót, hanem egy hozzáférhető helyre felírja, amihez mások is hozzáférhetnek.
- Jelszavak kicsalása;

  E módszer esetében a felhasználót a kiberterroristák félrevezetik és ráveszik, hogy hozzáférési adatait önként adja át.
- Jelszavak visszafejtése;

  Elvi síkon a jelszavak megszerzésének a legegyszerűbb módja az, hogy a támadó addig próbálkozik, amíg ki nem találja a helyes kombinációt.
- Jelszavak lehallgatása;

  Még napjainkban is léteznek olyan szolgáltatások, ahol az azonosítók és a jelszavak nyílt szövegként továbbítódnak a hálózaton, nincsenek titkosítva. Egy információs infrastruktúrába történő bejelentkezés folyamán a jelszavak a kibertér olyan részein haladhatnak át, ahol a kiberterroristák hozzáférhetnek.

IV. 2. 2. Hosztazonosítók hamisítása

Az információs infrastruktúrák elemei mindig rendelkeznek valamilyen formátumú saját azonosítóval, amit a felhasználóknak, más rendszerelemeknek ismernie szükséges. A különböző formátumú azonosítók közötti kölcsönös megfeleltetést különböző protokollok segítségével dedikált hálózati elemek végzik. E támadástípusnál a kiberterroristák célja az, hogy a kommunikáció során a másik féllel elhitessék, hogy az eredetileg kapcsolatba lépni kívánt féllel történik a kommunikáció. A kiberterrorista mind a kiszolgáló, mind pedig kliens oldaláról – azt megszemélyesítve – kezdeményezheti a támadást.

Ez a típusú támadási módszer megvalósítható:

- IP címek hamisításával;

  E módszerrel történő támadás esetén a megtámadott oldalon nem lehet azonosítani a csomagok valódi feladóját, továbbá ha a kiberterroristák a hamisított címet folyamatosan változtatják, akkor a megtámadott oldalon nem lehet letiltani a kiberterroristától érkező adatcsomagokat. A vázolt módszerrel pedig többféle támadást is meg lehet valósítani. Például hamis megszemélyesítést, de a forráscímek hamisítása jellemző kísérője a szolgáltatásbénító támadásoknak is, de feltétele a számítógépek közötti bizalmi viszonyba támadó számítógéppel történő belépésnek, hamis megszemélyesítésnek is. [102]

- DNS válaszok hamisításával;

  A felhasználók domain-névvel adják meg a keresett kiszolgálót, a számítógép pedig ilyenkor a konfigurációban megadott domain-név szerverhez (DNS) fordul, hogy megkapja a domain-névhez tartozó IP címet. Ha ennek a lokális névszervernek nincs a birtokában a keresett cím, akkor elindul felfelé a domain-név fán és megkeresi azt a szervert, amelyik ismeri a kérdéses IP címet. [103] A domain-név szerverek rendszerét azonban a kiberterrorista több ponton is támadhatja, ha egy kiberterrorista hatalmába tud keríteni egy ilyen lokális szervert, akkor a hálózat számítógépeinek lekérdezéseire az általa meghatározott IP címeket adhatja válaszul. A kérdéses IP cím mögött a kiberterrorista beállíthat egy olyan kiszolgálót, amely kapcsolatfelvétel során a felhasználó irányába úgy viselkedik, mint az eredeti szerver, ezért a felhasználó nem észleli, hogy nem az általa kívánt kiszolgálóval lépett kapcsolatba. Ebben a helyzetben azután a kiberterrorista többféle visszaélést követhet el, például adathalászattal (hamisított honlapok révén) bejelentkezési adatokat szerezhet meg.

- Közbeékelődéses támadás (Man in the Middle)

  A közbeékelődéses támadás esetében a kiberterrorista úgy hallgatja le a két fél között zajló kommunikációt, hogy a kommunikációs csatornát megszakítja, majd a két kommunikáló fél közé „beállva" mindkettőjük számára a másik félnek adja ki magát. A kapcsolat ezáltal mindkét fél számára zavartalannak tűnik, valójában azonban a teljes forgalom „átfolyik" a támadó eszközén, amellyel az itt zajló kommunikációt lehallgathatja, ahhoz teljes mértékben hozzáfér. [104] A támadás célja azonban nem csak az lehet, hogy a megtámadott nevében hozzáférjen valamilyen szolgáltatáshoz, hanem az is, hogy a megtámadott számítógépet valótlan információval megtévessze (dezinformálja), amiről a célpont azt hiszi, hogy vele kommunikáló féltől származik, holott az adatokat a kiberterrorista határozza meg. A támadás ellen leghatékonyabban itt is a titkosított kommunikáció alkalmazásával lehet védekezni.

IV. 2. 3. Kártékony programok

Kártékony támadókódról, vagy kárt okozó programról akkor van szó, amikor a számítógépre, azok hálózatára olyan programok kerülnek, melyek valamilyen módszer révén az üzemeltetőnek, vagy a felhasználónak közvetlenül, vagy közvetve kárt okoznak, vagy ennek veszélye fennáll. A kiberterroristák célja az információ megszerzése, manipulálása, részleges vagy teljes elérhetetlenné, vagy épp nyilvánossá tétele, de cél lehet a fizikai károk, vagy infrastruktúrák esetében az üzleti bizalom elvesztése. [105] [106] [107]

Típusai:

- Vírusok

  A vírus definíciójára többfajta meghatározás is létezik a szakirodalomban. A vírus általában egy olyan kisméretű támadókód, amely rejtett működése során más programokat fertőz meg oly módon, hogy a saját kódját beilleszti a megtámadott alkalmazásba, a vírusgazdába, ami ezután vírusként viselkedik, és további programokban helyezi el a kérdéses kódot, ami a fertőzés mértékét folyamatosan növeli. A vírus tehát képes önmaga reprodukciójára, ugyanakkor bizonyos típusai képesek arra, hogy módosított formában készítsenek másolatot az őket alkotó kódrészletről.

  Fontos ismérve, hogy önmagában terjedni nem képes, minden esetben szüksége van egy másik programra, mely a vírust alkotó kódrészt lefuttatja. Csak olyan fájl válhat vírusgazdává, melynek futtatásra alkalmas formátuma van.

- Trójai programok

  A trójai program rendszerint ártalmatlan, hasznos alkalmazásnak tűnik, de eközben támadókódot tartalmaz. Mivel ezek a programok a felhasználó számára vonzó funkciókat mutatnak, azonban e funkció mellett a háttérben rejtve, a kiberterroristák szándékaitól vezérelten kártékony műveleteket végeznek a kiszemelt számítógépen. [108]

  Miután a gyanútlan felhasználó tevőleges közreműködése mellett a trójai program sikeresen elindul, rendszerint átnevezi magát és el is rejtőzik. Néhány trójai program – a beépített számos funkció miatt – túlzottan nagyméretű, így ezeknek bejuttatását egy kisméretű, speciálisan erre a feladatra optimalizált program (dropper) végzi, ami majd egy webhelyhez kapcsolódik, és onnan tölti le a nagyméretű fájlokat.

- Férgek

  A vírusokhoz hasonló, reprodukcióra képes programok, de a vírusokkal ellentétben nem szükséges hordozóközeg (vírusgazda) a terjedésükhöz, önálló futtatható fájlban helyezkednek el, melyek képesek önmagukat a hálózaton különböző módszerekkel továbbterjeszteni. Sokféle károkozásra képesek, azonban sok esetben már önmagában a terjedésük is olyan forgalmat generálhat, amely leterheli a hálózatot, elvonva az erőforrásokat a hasznos szolgáltatásoktól. A férgek alapvetően három funkcióval rendelkeznek, a keresés, a terjedés és a támadókód futtatása.

  Abban az esetben, ha a féreg megfelelő célpontot talál, kísérletet tesz arra, hogy másolatát arra a helyre továbbítsa. A legjellemzőbb és a legkézenfekvőbb módszer az elektronikus levélen keresztül – érdekes, figyelemfelkeltő mellékletként – történő terjedés, amikor túlnyomó részben szintén a felhasználóra bízzák annak indítását. Legtöbb esetben a kérdéses levelet a féreg saját beépített levéltovábbító protokollal küldi tovább, ami a hálózati levéltovábbító szervertől függetlenül képes működni. [109]

- Egyéb kártékony programok

  Léteznek olyan kártékony programok is, amelyek kiberterroristák számára nem biztosítanak teljes körű távoli hozzáférést a megtámadott információs infrastruktúrához, hanem csak egy-egy speciális célra lettek kifejlesztve:

- Jelszókeresők

  Ezeknek a programoknak csak egyetlen célja van, megszerezni a számítógépeken tárolt jelszavakat. A fertőzést követően átvizsgálják a fájlokat és speciális formátumú karakterláncokat (például bankkártya- és bankszámlaszámok), jelszavakat keresve, majd a potenciális találatokat valamilyen kommunikációs csatornán keresztül visszaküldik a kiberterroristáknak. A fejlett jelszókeresők képesek az adatokat kiolvasni a számítógépre telepített alkalmazások (például a böngészők) védett táraiból is.

- Billentyűzetfigyelők

  A billentyűzetfigyelők a háttérben, a felhasználó előtt rejtve végzik adatgyűjtő tevékenységüket. A feladatuk az, hogy minden billentyűleütést – írásos kommunikációt, és bizonyos esetekben képernyőképet is – eltároljanak, majd azt egy kommunikációs csatornán továbbítsák a kiberterroristák számára. A megszerzett adatokat kielemezve pedig a támadó érzékeny információk birtokába juthat (jelszavak, levéltartalmak, stb.).

  Bizonyos billentyűzetfigyelők – felderítésük megnehezítése érdekében – csak a számítógép elindításától kezdve bizonyos ideig (például 10 percig) futnak, majd eljuttatják az összegyűjtött billentyűleütéseket a kiberterroristáknak, ezután pedig megsemmisítik magukat, ezáltal eltüntetve minden nyomot a támadásról.

- SQL Injection

  Ez a támadási módszer alapvetően fertőz, hanem célponton futatott szoftver hibája révén támadja az információs infrastruktúrában kezelt adatokat. E webes alkalmazásokat érintő sérülékenység esetében a kiberterrorista képes az alkalmazás által lefuttatott SQL utasításba olyan módon karaktereket, karakterláncokat beinjektálni, hogy azok egy része ne adatként, hanem SQL utasításként kerüljön feldolgozásra. A bejuttatott kódrészlet révén a kiberterrorista képes lehet új adatokat beszúrni, meglévőket módosítani, de akár magát az adatbázist is letölteni. [110]

IV. 2. 4. Szolgáltatásbénító támadások

Szolgáltatásbénító támadásnak (DoS: Denial of Service) azokat a támadásfajtákat nevezik, amelyek vagy a közvetítő infrastruktúrának rontják le az áteresztőképességét, akadályozzák vagy teszik lehetetlenné a hasznos üzenetcsomagok áthaladását, vagy pedig a célpontokat terhelik le oly mértékben, hogy azok alig vagy egyáltalán nem lesznek képesek hasznos hálózati kapcsolatok felépítésére. A nagy terhelést okozó támadások egyik fajtája azon alapul, hogy az infrastruktúrában nagy – maximális kapacitáshoz közeli – adatforgalmat indukál, ezáltal mintegy forgalmi dugókat hoz létre az infrastruktúra bizonyos szakaszain. A nagy terhelés megbénítja a rendszerelemeket, ugyanakkor betelítheti a közöttük lévő adatátviteli kapcsolatokat is.

A támadások másik típusa a végpontot célozza meg. A kiberterroristák a végpontot a hálózatról érkező nagy mennyiségű, rendszerint speciális adatcsomaggal, üzenettel árasztják el, aminek a feldolgozása annyira leterheli a célpontot, oly mértékben leköti az erőforrásait (CPU idő, memória), hogy hasznos működésre már képtelenné válik. Bizonyos speciális üzenetek akár önmagukban, vagy kis számban is alkalmasak arra, hogy a számítógépet olyan állapotba juttassák, hogy erőforrásait teljesen elhasználja, esetleg puffer túlcsordulás következzen be, a gép leálljon. [111]

A szolgáltatásbénító támadások között a legelterjedtebb típus az elosztott szolgáltatásbénító (DDoS: Distributed Denial of Service) támadás. Itt a támadási láncban kiberterroristák által vezérelt, úgynevezett multiplikátorok vannak, a támadásban nagyon sok számítógép vesz részt. A támadott hosztot, illetve annak hálózatát a támadást felügyelő számítógép irányítása alatt lévő számítógépek (ágensek) árasztják el adatcsomagokkal, így a támadásban részt vevő számítógépek és hálózatok egyenkénti teljesítményének nem kell kimagaslónak lennie ahhoz, hogy összességükben a legnagyobb teljesítményű hálózatok vagy hosztok megbénítására is képesek legyenek. [112]

Egyes esetekben azonban a kiberterroristák más támadások leplezése vagy kivitelezése érdekében gátolják valamelyik hoszt, vagy hálózatrész működését, és így másodlagosan a szolgáltatásbénítás is szerepet játszik adatok ellen irányuló más jellegű támadás sikerre vitelében. A szolgáltatásban történő fennakadás ugyanakkor bizonyos szolgáltatás típusoknál természetesen önmagában is hatalmas károkhoz vagy veszélyekhez vezethet (például banküzem, felügyeleti, vagy irányító-rendszerek).

A szolgáltatásbénító támadások közvetlenül nem jelentenek veszélyt az adatokra, nem történik adatvesztés, adathamisítás, adatszerzés, ugyanakkor a kiberterroristák az információs társadalom információs folyamataiban transzparens módon zavart és közveszélyt okozhatnak.

Ilyen támadási módszerek lehetnek:

- SYN elárasztás;
- ICMP elárasztás;
- Halálos ping;
- Land-támadás;
- IP szegmentációs támadás.

IV. 2. 5. A végponti számítógép gyengeségeit kihasználó támadások

Az információs infrastruktúrák végpontjait jelentő számítógépek, illetve azok védelme sok esetben elkülönül a számítógépeket, illetve a hálózatokat összekötő infrastruktúrák védelmétől. Ennek oka egyrészt az lehet, hogy az üzemeltetők, így védelmi elgondolásaik sem azonosak, más technológiákat alkalmaznak, mások a finanszírozási lehetőségeik. Ezekből a különbözőségekből adódik, hogy a végpontokon lévő (kiszolgáló) számítógépek gyengeségeit egy kiberterroristának külön kell megvizsgálnia egy támadás előkészítésekor.

Ez a módszer lehet a nyitott portok felderítése. Az információs infrastruktúrákban lévő eszközök nyitva lévő portjai pontosan elárulják a rajtuk futó hálózati szolgáltatásokat, a hálózatban betöltött szerepüket, így a kiberterroristák is ezeket a portokat vizsgálják át ahhoz, hogy az infrastruktúra védelmének réseit, gyenge pontjait távolról kifürkészhessék.

A portszkennelés ugyan még nem tekinthető támadásnak, de mindenképpen támadási kísérletet megelőző tevékenységként azonosítható. A kiberterroristák számára nagy hátrány, hogy ez a fajta szkennelés randomscan, slowscan, proxyscanning, stb. módszerek alkalmazása nélkül viszonylag könnyen felismerhető és kiszűrhető, mivel a célgép naplóállománya a sok különböző kapcsolódási kísérletet kimutatja.

Az esetlegesen meglévő biztonsági rések, sebezhetőségek feltérképezésére irányuló eljárás a nyitott portok felderítésén túlmenően azt is vizsgálja, hogy az eddig ismert sebezhetőségek közül nincs-e már valamelyik jelen a támadott gépen. E tevékenységhez a kiberterrorista egy naprakész adatbázist használ, mely az ismert sebezhetőségek meglétére utaló jeleket tartalmazza. A különböző operációs rendszerek, valamint az egyes portok és az azokat kezelő alkalmazások vonatkozásában szinte naponta kerülnek nyilvánosságra olyan hibák, sebezhetőségek, melyek megfelelő eljárással távolról is kihasználhatók. A kiberterrorista ezért a célpont távolról történő feltérképezésével első lépésben megállapítja, hogy milyen sebezhetőségekre számíthat az adott számítógépen, majd a második lépésben azokkal a

támadási eljárásokkal próbálkozik, amelyek a potenciális sebezhetőségeket használják ki. Erre a célra különböző technikák léteznek, melyeknek gyorsasága és megbízhatósága eltérő:

- TCP Connect Scan
- TCP SYN Scan
- TCP FIN Scan
- UDP „ICMP" port elérhetetlen" Scan. [113]

A fenti módszer fejlettebb megoldása az, amikor az információs rendszerek különböző biztonsági réseit, sebezhetőségeit feltérképező alkalmazások – az úgynevezett vulnerability scannerek – derítik fel az adott számítógép sebezhető pontjait. Az alkalmazások alapja egy jól felépített és naprakész biztonsági réseket tartalmazó adatbázis (vulnerability database). [114] Működésük részben hasonló a fenti portszkennelési technikákhoz, csak ez kiegészül azzal, hogy a vizsgált gépen kiderített portokon futó szolgáltatások vonatkozásában automatikusan megvizsgálják az ismert biztonsági hibák meglétét, illetve a meglétére utaló jeleket, így a kiberterrorista azonnal képet is kaphat a célszámítógép sebezhetőségének mértékéről. Az így azonosított gyengeségekre a kiberterroristáknak már csak egy megfelelő támadókódot kell alkalmazni az eszköztárukból, hogy eredményesen támadni tudják a kiszemelt számítógépet.

IV. 2. 6. Hálózati elemek gyengeségeit kihasználó támadások

Az információs társadalomban a számítógépek hálózatokba történő integrálása általánossá vált, így bármely szervezet információs rendszere számítógépek százait szervezi egységbe az információ hatékonyabb megosztása, feldolgozása érdekében. A hálózati infrastruktúra tükrözi a szervezet topológiáját is: néhány gépből álló lokális hálózatokat hub-ok és útválasztók csatolnak magasabb egységbe, amelyeket útválasztók, átjárók, tűzfalak kapcsolnak már általában a nagyterületű hálózatokat jelentő még magasabb egységekbe.
A hálózat rendszerelemeinek gyengeségei alatt olyan sebezhetőségeket kell érteni, melyek a hálózati architektúra kialakításából, vagy a hálózati protokollok tervezési elveiből, megvalósítási gyakorlatából, vagy a hálózat belső működéséhez szükséges berendezések sebezhetőségeiből adódhatnak

- ARP tábla meghamisítása

  ARP tábla meghamisítása, vagy mérgezése az egyik legveszélyesebb támadási módszer, melyet szolgáltatásbénító, illetve hamis megszemélyesítéses támadások során alkalmaznak. Üzenetszórásos lokális hálózatok egyik kritikus pontja a fizikai és

IP címek közötti összerendelés mechanizmusa. Ahhoz, hogy egy hálózatban a feladó IP csomagot juttathasson el valamelyik címzetthez, előbb meg kell tudnia a címzett IP címének ismeretében annak Ethernet címét, aminek megoldására az ARP mechanizmust alkalmazzák. A lokális hálózatokban a forgalom a számítógépekről közvetlenül nem hallgatható le, de az ARP mechanizmus megtévesztésével, tehát az ARP gyorsítótár meghamisításával, a forgalom átirányításával erre van lehetőség. [131]

- Forrásvezérelt útválasztás

  Az útválasztók egymás közötti útvonal-hirdetések, vagy a rendszergazdák által rögzített útvonal-táblák alapján döntik el, hogy merre irányítják az adatcsomagokat. Az IP forráscím hamisítás esetében a kiberterrorista a hamis forráscímmel érkező csomagokat el tudja ugyan fogadtatni a célszámítógéppel, azonban a válaszokat az útválasztók nem az eredeti címre küldik meg, hanem a forráscímben megjelölt számítógépnek. A kiberterrorista nagyobb károkozásra is képes, ha a válaszcsomagok is eljutnak hozzá. A forrás vezérelt útválasztás – főleg az úgynevezett laza irányítás – hatékony eszköz lehet egy olyan támadó kezében, aki a hálózatban akar IP forráscím-hamisítás alapú támadást megvalósítani. [100]

- Kapcsolat eltérítése

  A kapcsolat eltérítése olyan támadási módszer, amikor a kiberterrorista már egy felépült és hitelesített aktív kapcsolatot akar az egyik szereplő nevében átvenni, illetve más nevében is kezdeményezhető kapcsolat felvétel ezzel a módszerrel, például ha a támadott célpont kizárólag forrás IP cím alapján hitelesít. A kiberterrorista célja, hogy a hitelesítési folyamatot megkerülje, és a megszemélyesített felhasználó jogosultságát megszerezze a kiszemelt célponton. Ez a támadási eljárás főleg az erős hitelesítést alkalmazó kapcsolatoknál lehet eredményes, mivel az erős hitelesítés e támadási metódus ellen nem véd. A kapcsolat eltérítése lehet passzív vagy aktív, attól függően, hogy a támadó csak megfigyeli az eltérített kapcsolatban folyó adatokat, vagy aktívan manipulálni is akarja azokat.

- Routerek elleni támadások

  Egy útválasztó üzembeállításakor a környezetének megfelelően fel kell tölteni routing tábláját. A routing tábla feltöltése, az útválasztó konfigurálása az adminisztrátor

feladata, melyet megfelelő jogosultság birtokában lehet csak végrehajtani. A támadás célja az adminisztrátori felügyelet megszerzése, a routing információk cseréjének manipulálása, így az IP csomagok eltérítése.

IV. 3. Összegzés, részkövetkeztetések

A kiberterroristák számára az a legegyszerűbb metódus, ha egy meglévő, előttük ismertté vált (technológiai, fizikai, humán, stb.) hibára, sérülékenységre lehet felépíteni a támadást, melyből azonban következtetni lehet a támadás módszerére, illetve magára a célra is. Ugyanakkor a legtöbb esetben ez nem elég, ezért a kiberterroristáknak a kitűzött célok elérésére alkalmas sérülékenységeket fel kell kutatniuk, vagy azokat egyéb műveletek keretében előzetesen meg kell teremteniük, például az infrastruktúra egy alkalmazottjának megnyerése, és az általa kialakított sérülékenység révén. Már ezek az előkészítő fázisok is mély szakismereteket igényelnek, melyet a támadások kivitelezése tovább mélyít, így egy, a kibertérben végrehajtott terrortámadás humánerőforrások tekintetében fokozott kihívást jelent egy terrorcsoportnak, mely ugyanakkor nem minden esetben áll rendelkezésükre.

A terrorizmus lényegéből következik, hogy a kiberterroristák ideológiája – akár funkcionalitása, akár a felhasználók köre, akár a tulajdonosok összetétele által – kijelöli a veszélyeztetett infrastruktúrák körét, míg a kitűzött célok determinálják azt, hogy az infrastruktúrában kezelt információ mely tulajdonságait fogja érinteni a támadás, tehát a cél a támadás végrehajtásának potenciális eszközeit is előrevetíti.

Míg a katonai szervezetek esetében a célpontok köre viszonylag állandó, addig a kiberterrorizmus által veszélyeztetett infrastruktúrák csoportja számos tényezőből (például politikai, gazdasági helyzet, stb.) adódóan dinamikusan változhat, ami megnehezíti a védelemre való felkészülést. A katonai, illetve az állami szervek a kiberteret érintő műveleteiket legtöbb esetben az adott célfeladatra tervezett, optimalizált professzionális, fizikai hatáson alapuló-, illetve logikai eszközökkel hajtják végre, melyek azonban a kiberterroristák számára nem elérhetőek. Ez okból kifolyólag ők az illegális műveleteik lebonyolítása érdekében kénytelenek a professzionális eszközöket az általuk is elérhető megoldásokkal kiváltani, melyek hatékonyság tekintetében azonban értelemszerűen elmaradnak a céleszközöktől. Bár a különböző eszközök és módszerek mögött álló elvek, sérülékenységek, fizikai törvényszerűségek azonosak, azonban a megvalósítás minősége a

professzionális megoldások esetében nagyságrendileg magasabb szinten áll, ellenben – főleg a logikai eszközök esetében – a kiberterroristáknak is tudomására juthatnak olyan sérülékenységekre vonatkozó információk, melyek birtokában előnyre tehetnek szert az infrastruktúrákkal, illetve a rendészeti erőkkel szemben, ám ezek kiaknázása csak magasan képzett humánerőforrások rendelkezésre állása esetén van esélyük.

Az eszközök fejlettségi szintjében megjelenő különbözőséget azonban a kiberterroristák az esetleges anomáliák más dimenzióiban képesek lehetnek kiegyensúlyozni, amennyiben a műveleteikhez, illetve az érintett információs infrastruktúrákhoz kapcsolódóan azonosítanak számukra olyan előnyöket biztosító lehetőségeket, melyek lecsökkentik a védelmi, az elhárító és a rendészeti tevékenység hatásfokát. Ez okok miatt az üzemeltetőinek célszerű már előzetesen felmérni az információs infrastruktúrán belül és interdependens kapcsolataiban azokat a körülményeket, munkafolyamatokat, jogszabályi és szabályozási kereteket, technikai és technológiai gyengeségeket, sérülékenységeket, melyek gyengíthetik, akadályozhatják egy kibertámadás érzékelését, megszakítását, vizsgálatát.

Mivel a fizikai hatáson alapuló eszközök alkalmazása számos nehézséggel (speciális, nehezen megszerezhető szakismeret az alkalmazás, a megalkotás terén) és kockázatnövelő tényezővel (birtoklás, beszerzés, az alkalmazás során viszonylagos fizikai közelség) jár együtt, így már most is érezhető az a tendencia, hogy a több előnnyel bíró logikai eszközök alkalmazását részesítik előnyben a kiberterroristák az információs infrastruktúrák támadása során.

A fenti logikai eszközök, módszerek bizonyos típusaira kész toolkit-ek is beszerezhetők, melyekkel akár laikus támadók is képesek különböző támadókódokat legenerálni, azonban ezek hatékonysága viszonylag csekély. Egyes „elhanyagolt” rendszerekkel szemben, vagy frissen nyilvánosságra került, még nem kezelt sérülékenységek esetében lehet eredményes támadást lebonyolítani használatukkal. Ennek fő oka az, hogy ezekbe az alkalmazásokba már ismert, nyilvánosságra került sérülékenységeket használnak fel, melyekre az infrastruktúrák üzemeltetői jó esetben – például a vírusvédelmi cégek közreműködése révén – már felkészítették rendszereiket.
A „0-day” sérülékenységek azonosítása, kihasználása rendkívül mélyreható ismereteket igényel, mely a hackerek, kiberterroristák felsőkasztjára jellemző csak, akik ezeket az információkat inkább felhasználják saját támadásaik során, minthogy toolkit-ek formájában megosszák. Meg kell jegyezni, hogy a kibertérben a „0-day” sérülékenységek adás-vétele is

megjelent már, mind legális formában államok, vállalatok számára (például Zerodium (Vupen)) [132], mind pedig illegális formában a darkweben, akár kiberterroristák számára is.

A kiberterrorizmus eszközeinek vizsgálatából leszűrhető az a konklúzió, hogy az információs infrastruktúrák támadásához, illetve ennek előkészítéséhez sok esetben valamilyen módon más információs infrastruktúrák által biztosított szolgáltatások szükségesek (például DDoS támadások esetében más infrastruktúrák kapacitása).

A terrorizmus fogalmának és a fenti következtetésnek az egyesítéséből megalkotható a kiberterrorizmus általam javasolt definíciója:
A kiberterrorizmus a terrorizmus azon megjelenési formája, amikor a terrorcselekmény célpontjai az információs infrastruktúrák, illetve ezek rendszerelemei, a bennük kezelt információk, funkciók és meglévő képességek, és/vagy a terrorcselekmény előkészítése, támogatása, végrehajtása más információs infrastruktúrák szolgáltatásai nélkül nem valósulhatott volna meg.

A kiberterrorizmus jelentette összetett fenyegetés létéből következik, hogy az információs infrastruktúrák üzemeltetőinek olyan védelmi megoldásokat szükséges kidolgozniuk, melyek egyrészt tükrözik saját rendszereik sajátosságait, másrészt kezelik a kibertérben megjelenő potenciális fenyegetések dinamikus változásait is. Az alkalmazott védelmi rendszernek a biztonság minden területére komplexen ki kell terjednie, hogy szavatolni tudja az adott információs infrastruktúra biztonságos és rendeltetésszerű működését.

V. A kiberterrorizmus elleni védekezés megoldásai

Mint ahogy már többször is kijelentettük a XXI. században, az információs társadalom korában élő embereknek mindennapjait behálózó, az információs folyamatok alapját jelentő kritikus információs infrastruktúrák védelme a társadalom hatékony működésének szempontjából elengedhetetlen.

Ugyanakkor a társadalom szűkebb szegmensét alkotó entitások (magánszemélyek, gazdasági társaságok, társadalmi és állami szervezetek) is működtethetnek olyan információs rendszereket, melyeket maguk szemszögéből nézve – saját tevékenységük, biztonságuk vonatkozásában – kritikusnak ítélhetnek meg, azonban ezek köréből – össztársadalmi szempontból – csak néhány emelhető ki. [115]

Ezek az entitások céljaik elérése érdekében használják az információs rendszereket, ugyanakkor minden ilyen rendszernek meg van az a kritikus pontja, melynek zavara súlyosan veszélyezteti az adott cél elérését. Amikor egy zavar, vagy egy támadás olyan komponenst, alrendszert ér, ami bár sérülékeny, de az alapfeladatok ellátása szempontjából nem kritikus, az bizonyos kárt, presztízsvesztést okozhat, de az alapfeladatok ellátását nem veszélyezteti. Ám az infrastruktúra folyamatos és biztonságos működése érdekében célszerű azokat a kritikus funkciókat, illetve az ezeket biztosító szoftver és hardver komponenseket meghatározni, amelyek védelme kiemelten fontos.

Amennyiben pedig ezek a kritikus funkciók részben, vagy teljes egészében más infrastruktúrák szolgáltatásaihoz kapcsolódnak, gondoskodni kell az üzemeltetőnek arról, hogy ezeknek bármi okból bekövetkezett zavarai esetén azonnal kiválthatóak legyenek más szolgáltatóval, vagy más megoldásokkal. Ezért a biztonságos működés érdekében az információs rendszerekben – függetlenül rendeltetésüktől és méretüktől – azonosítani kell azokat a folyamatokat, rendszerelemeket és interdependencia kapcsolatokat, melyek a kritikusságra vonatkozóan meghatározó szereppel bírnak, illetve, hogy a védelem mely dimenziói befolyásolhatják az információs szolgáltatások megfelelő szintű színvonalát.

Az információs infrastruktúrákat veszélyeztető kritikus tényezők alapvetően négy csoportra sorolhatók:

- adatbiztonság, bizalmasság sérülése;

  Az információs rendszerben gyűjtött, tárolt, feldolgozott, továbbított információk megváltoztatása, hozzáférhetetlenné tétele, nyilvánosságra hozatala, elvesztése, illetéktelen hozzáférés megvalósulása valamilyen rosszindulatú zavar vagy cselekmény következtében. [116]

- rendelkezésre állás csökkenése;

  A felhasználók számára az információkhoz vagy szolgáltatásokhoz való hozzáférés idejének jelentős megnövekedése, valamint részleges vagy teljes elérhetetlenné válása valamilyen külső vagy belső behatás következtében. A rendelkezésre állás az annak a biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek. [116]

- teljesítmény romlása;

  Az infrastruktúra összetevőinek, szolgáltatásainak, funkcióinak részleges vagy teljes egészének számottevő teljesítmény-, hatékonyságromlása, költségek jelentős növekedése.

- jogi szabályzóktól eltérő működés;

  Az információs rendszer az üzemeltetése során nem tud megfelelni a működését szabályozó külső és belső előírásoknak, szabványoknak, jogszabályi normáknak.

Az információs rendszerek tervezése, fejlesztése során figyelembe kell venni az adott ágazatra jellemző fenyegetettségeket (például terrorizmus, bűnözés), kritikusságot meghatározó tényezőket, gazdasági és jogszabályi környezetet. A megvalósítás során létrejövő infrastruktúra paraméterei nagyban függnek a felhasznált eszközök színvonalától, az igénybe venni kívánt ötös szolgáltatáskör (adatgyűjtés, továbbítás, tárolás, feldolgozás és szolgáltatás) rendelkezésre álló és elérhető paramétereitől, a felhasznált szaktudás minőségétől, illetve az entitás speciális igényeitől, mely szinte minden esetben egyedi, csak az adott információs rendszerre jellemző.

Fentiek tükrében az információs infrastruktúrát támadni szándékozó kiberterroristának – ideológiájához igazodva – el kell döntenie, hogy milyen szolgáltatást, funkciót, vagy kritikus tényezőt (például adatbiztonság, rendelkezésre állás, teljesítmény, szabályzóknak való megfelelés) kíván támadni, majd ezt követően meg kell határoznia, hogy melyek azok a komponensek, melyek sebezhetőségét kihasználva elérheti célját. A támadás sikere nagyban függ attól, hogy a támadó motivációja, támadási potenciálja, illetve a kérdéses infrastruktúra paraméterei milyen viszonyban állnak egymással. Tehát a támadó az infrastruktúra tekintetében rendelkezik-e azokkal a műszaki, adminisztratív, humán erőforrásokra vonatkozó ismeretekkel, felderítési és támadó képességekkel, logisztikai és finanszírozási

lehetőségekkel, valamint felderítő- és támadóeszközökkel – és meg tudja ezek alkalmazásának lehetőségeit is teremteni – melyek birtokában támadni tudja a rendszer azon paramétereit, aminek következményeként fellépő zavar, vagy kár kiváltja az elérni kívánt célt. A hatékony védelem szempontjából pedig az üzemeltetőnek ismerni kell azokat a hatásokat, interdependens következményeket, melyek egy kritikus rendszerelemet ért támadás, egyéb hatás a rendszerének egészében kivált.

Az infrastruktúra üzemeltetőjének szempontjából nézve a rendszerek védelme jóval összetettebb feladat. Különböző kockázatelemző módszerek állnak az információs rendszerek védelmével foglalkozó szakemberek rendelkezésére, amelyek segítségével védelmi stratégiákat dolgozhatnak ki, azonban az elméleti rendszertervek és a védelem gyakorlati megvalósítása között nagy lehet az eltérés. Alapvető célként arra kell törekedni, hogy egyenszilárdságú védelmi rendszer kerüljön megalkotásra, mert így a foganatosított intézkedések hatékonysága nagyban növelhető. Olyan átfogó, komplex védelmi stratégiát kell alkalmazni, melyek révén kiküszöbölhetők a biztonsági rések, valamint az ezekből indukálódó további fenyegetések.

V. 1. Komplex információbiztonság

A védelmi alrendszerekkel szemben támasztott egyik legfontosabb követelmény, hogy folyamatos készenlétet és magas szintű védelmet biztosítsanak az adott információs infrastruktúra számára bárminemű fenyegetés ellen. Elengedhetetlen, hogy a védelmi alrendszer komponensei az elérhető legmagasabb technológia színvonalát tükrözzék, mind fizikális eszközök, mind hardverek, mind szoftverek tekintetében, mivel számos veszélyforrást indukálhat az, ha a kiberterroristák magasabb technológiai szinten állnak, mert ezzel jelentős mértékben növelni tudják a támadási potenciáljukat.

Az információs infrastruktúra, illetve az általa nyújtott szolgáltatás-portfólió folyamatosságát, valamint a kezelt adatok hozzáférhetőségét, bizalmasságát óvó kritikus rendszerelemek zavarainak, kiesésének elkerülése érdekében célszerű védelmi prioritásokat felállítani, hogy a rendelkezésre állási mutatók minél magasabb szinten maradjanak, illetve, hogy rendkívüli események bekövetkezésekor a kárt minimalizálják. A rendszerek védelmi protokolljainak kialakítása során az adatgyűjtés, az információ-továbbítás, a tárolás, a feldolgozás és a szolgáltatás ciklusának megfelelő, a kritikusságot befolyásoló elemeire kell kiterjednie.

A fenyegetést jelentő tényezők sokrétűsége miatt szükséges azokat csoportosítani, azonban az egyes csoportok hatása az interdependencia jelensége miatt összeadódhat, illetve erősíthetik egymást, így az egyes csoportok hatását, hatásmechanizmusát külön-külön elemezni félrevezető lehet. Az információs infrastruktúrák fenyegetései lehetnek humán, fizikai, logikai vagy épp a rendszer életciklusa során jelentkező kockázatok:

- Humán tényezők

  E körbe sorolt veszélyforrások során a hibák, vagy káresemények nem szándékos vagy tudatos emberi cselekményekre vezethetők vissza. A nem szándékos cselekmények motivációi sokrétűek lehetnek, állhat mögötte személyi alkalmatlanság, képzetlenség, gondatlanság, felelőtlenség, monotónia, stb..

  A tudatos, rosszindulatú emberi tevékenységre az angol nyelvű szakirodalom 7-E csoportként hivatkozik:

  1. Ego (személyiség);
  2. Eavesdropping (lehallgatás);
  3. Enimity (ellenségeskedés);
  4. Espionage (kémkedés);
  5. Embezzlement (sikkasztás);
  6. Extortion (zsarolás);
  7. Error (hiba);

  Fentiek mögött szintén számos ok húzódhat meg: sértettség, bosszú, vandalizmus, anyagi haszonszerzés, stb..

- Fizikai tényezők

  A fizikai tényezők általában az infrastruktúra hardverelemeinek, átviteli közegeinek, az üzemeltető személyzet, kiegészítő szolgáltatások elhelyezésével, elhelyezési körleteivel kapcsolatosak. Az információs infrastruktúra rendelkezésre állási mutatói sérülhetnek, ha a fizikai védelmi rendszer (épületek, nyílászárók, beléptető-rendszer, stb.) nem biztosít kellő mértékű ellenálló-képességet egy támadás vagy környezeti hatás (villámlás, árvíz, csapadék, por, földrengés, stb.) ellen.

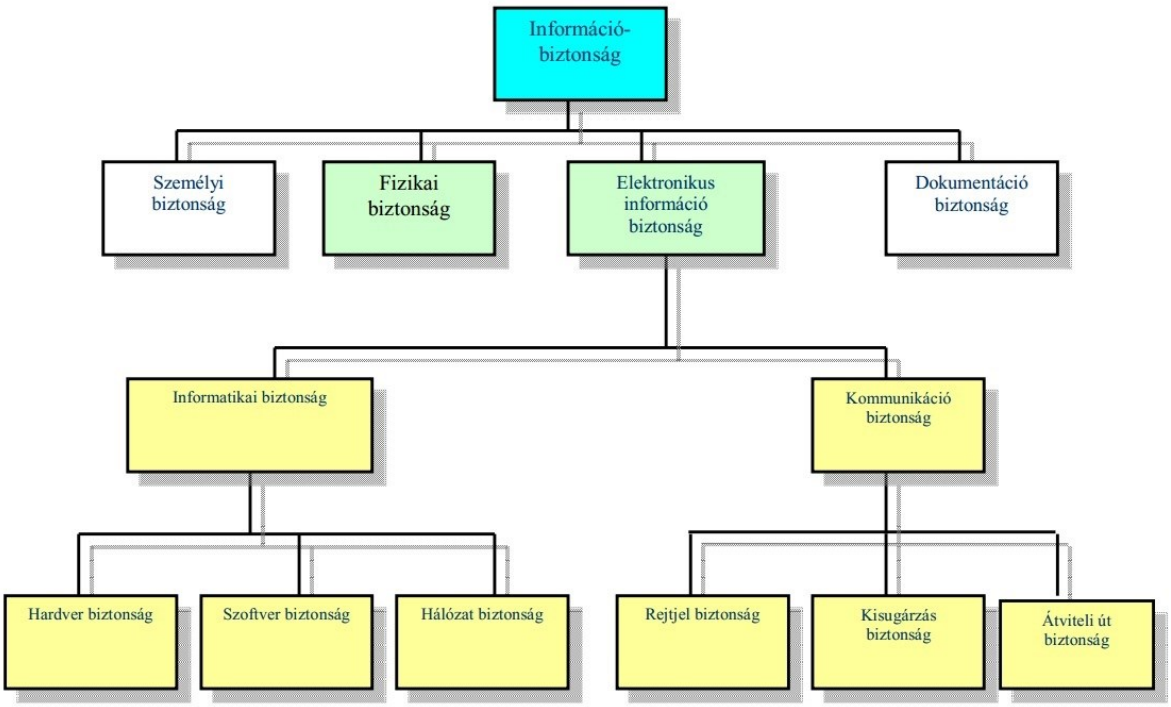
- Logikai tényezők

  Ezek a tényezők is nagyban képesek veszélyeztetni egy információs infrastruktúra rendelkezésre állási szintjét, illetve az abban kezelt adatok bizalmasságát, sérthetetlenségét. A logikai tényezőkből adódó veszélyek révén a kezelt

információk jogosulatlanok előtt megismerhetővé, módosíthatóvá vagy akár elérhetetlenné válhatnak, de el is veszhetnek. A logikai hibákat használhatják ki a rosszindulatú programok (például vírusok, trójai programok, stb.), de ide sorolhatók a hibás hardver- és szoftverbeállítások, valamint a rendszer átgondolatlan tervezéséből adódó tényezők is. [117]

Az információvédelem során lehetőség szerint törekedni kell az egyenszilárdságú védelmi rendszerek megalkotására, azonban a gondos tervezés és kiválasztás nélkül nincs garancia arra, hogy a legmodernebb és legdrágább technológia valóban képes lesz megfelelni az adott infrastruktúra igényeinek. Kijelenthető, hogy az információ megfelelő védelmét biztosító megoldások csak a technológiai síktól elvonatkoztatott, komplexebb szemléletmóddal valósíthatóak csak meg. [118]

A fentiek értelmében a védelemi stratégia kialakítása folyamán célszerű a különböző szakterületeket elkülönítetten kezelni [119]:



14. ábra A komplex információbiztonság elemei

V. 1. 1. Személyi biztonság

Tekintettel arra, hogy az információs infrastruktúrák tervezésében, kiépítésében, üzemeltetésében és fejlesztésében az emberi tényező kiemelt szerepet kap, ezért biztonsági

szempontból mindenképpen indokolt az, hogy a védelem során is kiemelt fontosságúként legyen kezelve.

Az információs infrastruktúrák üzemeltetését végző személyekre kiemelt figyelmet fordíthatnak a kiberterroristák. Egyrészt részükről olyan információk megszerzését remélhetik, melyek felhasználhatók egy támadás során. Ez az információszerzés lehet tudatos, az érintett személy megnyerésével, illetve lehet figyelmetlenség is, amikor felelőtlen „fecsegés" révén kompromittálódnak az érzékeny információk. Másrészt pedig célpontként is tekinthetnek rájuk kiberterroristák, mivel az üzemeltető személyzet munkaképességének befolyásolása révén sikeresen akadályozható a rendeltetésszerű működést.

Az infrastruktúrák tekintetében a személyi biztonságnak több dimenziója is értelmezhető:

- A személyi biztonság az információhoz való hozzáférés szempontjából is értelmezhető, vagyis, a minősített információ csak olyan személyeknek juthat a birtokába, akik a megfelelő szintű személyi biztonsági követelményeknek igazoltan megfelelnek, illetve az adott minősítésű információ megismerése munkakörük eredményes ellátása céljából szükséges. Állami hátterű infrastruktúrák esetében a személyi biztonság megteremtésének egyik legfontosabb eljárása a nemzetbiztonsági ellenőrzés lehet, melyen minden bizalmas munkakört betöltő személynek át kell esnie. [120]
- Tágabb dimenzióban értelmezve a személyi biztonság azonban már kiegészülhet a munkavállalóval kapcsolatos egyéb személyi és foglalkoztatási körülmények vizsgálatára is.

  Az üzemeltetés biztonsága érdekében elengedhetetlen, hogy a munkavállalók rendelkezzenek megfelelő szaktudással, ismerjék, illetve felismerjék az infrastruktúrát esetlegesen veszélyeztető jelenségeket, körülményeket, ezért az üzemeltető felelőssége, hogy a munkatársakkal az infrastruktúrára vonatkozó specifikus ismereteket elsajátíttassa, készségüket kialakítsa, és azt szinten is tartsa.

  Fontos továbbá, hogy a munkáltatók biztosítsák azokat a foglalkoztatási körülményeket (megfelelő eszközök, munkakörnyezet, munka- és pihenőidő betartása, stb.), melyek lehetővé teszik azt, hogy a munkavállalók külön erőfeszítések nélkül be is tudják tartani a biztonsági előírásokat.

- Kiemelt szempont, hogy a bizalmas információk megismerésére feljogosított személyek megfelelő javadalmazásban részesüljenek, ami nagyban hozzájárul a megfelelő munkamorál és lojalitás fenntartásában.

A magas színvonalú személyi biztonság érdekében elengedhetetlen a megfelelő ellenőrzési folyamatok, rutinok kidolgozás és azok konzekvens alkalmazása. Ennek keretében folyamatosan monitorozni kell a munkatársak tevékenységét, ismereteik naprakészségét, valamint azt, hogy az infrastruktúra biztonságos működése érdekében foganatosított rezsimintézkedéseket milyen szinten tartják be. Ugyanakkor figyelemmel kell kísérni azt is, hogy a rezsimintézkedések alkalmasak-e a biztonság szavatolására.

V. 1. 2. Fizikai biztonság

A biztonságos üzemeltetés érdekében az infrastruktúra elemeinek fizikai biztonságára kiemelt figyelmet kell fordítani. A rendszerelemeket és sok esetben magát az üzemeltető személyzetet is szükséges – a szándékos vagy a véletlenszerű rongálás, információszerzés, illetve egyéb káros, ártó tevékenység elkerülése érdekében – illetéktelen személyek elöl elzárni, és a védett területekre pedig csak a jogosultsággal rendelkező személyeket beengedni.
A fizikai biztonság a tényleges akadályok – falak, kerítések, épületek, beléptető rendszerek, biztonsági személyzet – összessége, amelyek képesek megakadályozni a terroristákat abban, hogy az információs infrastruktúra elemeihez, munkatársaihoz, a szervezet dokumentumaihoz, illetve egyéb védendő eszközeihez hozzáférjenek.

A fizikai biztonsági rendszer tervezésekor figyelembe kell venni az infrastruktúrában kezelt, vagy tárolt adatoknak a minősítési szintjét, mennyiségét és megjelenési formáit (technikai eszközök, eljárások) az érintett rendszerelemeknek a specifikumait, valamint a helyszín más dimenzióban értelmezhető veszélyeztetettségi szintjét (például nemzet-, vagy közbiztonsági körülmények). A biztonsági rendszert úgy célszerű kiépíteni, hogy az fizikailag és logikailag több egymásra épülő elemből álljon, mélységében tagolt legyen, valamint fokozódó erősségű védelmet biztosítson, és képes legyen ellenállni az illetéktelen hozzáférésnek, az erőszakos behatolásnak a reagáló erők beérkezéséig. [121]

A fizikai biztonság tervezésekor fel kell készülni az esetleges természeti fenyegetettségekre (tűz, földrengés, áradás, stb.) is, és a védelmi eszközöket a várható fenyegetések

összességéhez kell méretezni, továbbá ki kell alakítani az üzemeltetéshez szükséges rendszabályokat is, amelyeknél törekedni kell az életszerűségre és a betarthatóságra. A fizikai biztonsági alrendszerek hatékonyságára ugyanakkor hatással van az is, ha a védendő és kritikus rendszerelemek földrajzilag nagy területen szóródnak szét, ami a költségek növekedése mellett a támadók lehetőségeit is növelik.

A biztonság e dimenziójában a kiberterroristák által igénybe vehető eszközök és módszerek megegyeznek a terrorizmus hagyományos megjelenési formáival, azonban mivel a célpontok elsődlegesen az információs infrastruktúra elemei, tehát a kibertérben kiváltott hatáson van a hangsúly, így a támadás helyszínén látványos, félelemkeltő akciók kivitelezésének nincs prioritása.

V. 1. 3. Dokumentumbiztonság

Mind az üzleti, mind pedig a kormányzati, államigazgatási ügyvitelben még napjainkban is domináns szerep jut a papíralapú dokumentumoknak. Míg a kibertérben az információbiztonság kiforrott eszközökkel rendelkezik, addig a fizikai térbe kikerülő információ védelme nincs minden esetben teljes körűen megoldva. Fontos kiemelni, hogy az információk védelme nem csak magukban az elektronikus rendszerekben tárolt információk esetében szükséges, hanem azoknak az összes – az adott információs infrastruktúra esetében értelmezett – megjelenési formájánál, így a kinyomtatott dokumentumoknál, kézzel írt jegyzeteknél, hanganyagoknál, filmeknél is.

Az összes dokumentumot minősítésének megfelelően kell védeni. Az érzékeny adatokat tartalmazó dokumentumokhoz való hozzáférés – a személyi biztonsági elvekben deklarált módon – azon körre kell, hogy korlátozódjon, akik számára feltétlenül szükséges az, hogy munkájuk eredményes elvégzése érdekében annak tartalmát megismerjék. A dokumentumbiztonság megvalósítása ugyanakkor szervesen kapcsolódik az infrastruktúra fizikai biztonságához, illetve iratforgalmának kialakításához. A szervezeten belüli és kívüli irattovábbítás során is ki kell dolgozni azokat a protokollokat, melyek garantálják azt, hogy a dokumentumok tartalma csak az arra jogosultak előtt váljanak ismertté (például a közös, mindenki számára elérhető nyomtatóra érkező bizalmas iratok problémája).

A dokumentumbiztonság közvetlen módon kapcsolódik az elektronikus információ biztonsághoz, hiszen valamennyi elektronikus adathordozó egyben dokumentumnak is minősül [15:286]. Egy tipikus irodai környezetben a dokumentum biztonság alapvetően három kérdéskör köré csoportosul. Egyrészt ki kell alakítani az elektronikus dokumentumok tárolására, hozzáférésére (hálózati tárolóeszközök, verziókövetés, titkosítás, hozzáférési jogok adminisztrációja) vonatkozó szabályrendszert. Másrészt elengedhetetlen az elektronikus dokumentumok áramlásának nyomon követése, a ki- és beviteli csatornák (elektronikus adathordozók, e-mail, Internet, nyomtatók, fax, stb.) forgalmának adminisztrálása. Harmadrészt pedig az elektronikus dokumentumok fizikai térbe kikerülése (kinyomtatása) után is szükséges a papíralapú dokumentumok figyelemmel kísérése, tárolóhelyeik megfelelő fizikai védelme, valamint szállításuk biztonságos megszervezése. Mindhárom témakör kezelése egyfelől technológiai, másfelől belső szabályozási kérdés.

Mivel a dokumentumbiztonság szervesen kapcsolódik a személyi és a fizikai biztonság dimenzióihoz, így e területen az interdependencia feltérképezése kiemelt jelentőséggel bír.

V. 1. 4. Elektronikus információbiztonság

Az elektronikus információbiztonság az információs infrastruktúrákban, valamint azok támogató infrastruktúráiban alkalmazott azon rendszabályok összessége, amelyek védelmet nyújtanak az előállított, a feldolgozott, a tárolt, a továbbított és a megjelenített információk bizalmasságának, sértetlenségének és rendelkezésre állásának véletlen, vagy szándékos csökkenése ellen. [15:200] A logikai és a fizikai hatáson alapuló eszközök alkalmazása esetén a kiberterroristák a biztonságnak e dimenziójában kívánnak eredményeket elérni az információs infrastruktúrák támadása során.

Az információs infrastruktúrák elektronikus információbiztonságának kiépítése a fizikai biztonság megteremtéséhez hasonlóan folyik, tehát fel kell mérni, hogy a rendszer elemei milyen elektromágneses környezetben működnek, milyen természetes és szándékos veszélyeknek lehetnek kitéve. E területen megkülönböztetünk átviteli biztonságot, kompromittáló kisugárzások elleni védelmet, rejtjelezést és rejtjelbiztonságot, valamint számítógép és hálózati biztonságot.
Az információs infrastruktúrák infokommunikációs folyamatainak védelme során figyelmet kell fordítani a végpontokon az információk hozzáférésének szabályaira, a tárolás

biztonságára és a rejtjelezés (kulcsok és algoritmusok) védelmére. A továbbítás során, az átviteli utaknak a védelme szintén kiemelt figyelmet kell, hogy kapjon, célszerű kis valószínűséggel felderíthető adásmódokat a minimálisan elegendő teljesítménnyel alkalmazni, valamint a nem kívánt irányokat irányított antennák használatával kizárni. Annak érdekében, hogy az infrastruktúrába idegen elemeket nem tudjanak beépíteni, az egymással kommunikáló rendszerelemek közötti kapcsolatot a megfelelő protokollok alkalmazásával kell felépíteni.

Az elektronikus rendszerek biztonságát negatívan befolyásolhatja a kompromittáló kisugárzás is, mely az elektronikai eszközök használata során jelentkező elektromágneses háttérsugárzás, ami a laikusok számára zavarjelnek tűnhet, de egy kiberterrorista számára értékes információkat tartalmazhat. Ez az elektronikai eszközök létét és működését felfedheti, funkcióikat kompromittálhatja, így a terroristák birtokába értékes adatok kerülhetnek az információs infrastruktúra rendszerének, alrendszereinek, illetve elemeinek összetételéről, paramétereiről, funkcióiról, melyek alapján ki lehet dolgozni egy esetleges támadást, valamint következtetéseket is le lehet vonni annak várható eredményességéről. A kompromittáló kisugárzás elleni védelem megvalósítása során fontos a megfelelő konstrukciós megoldással rendelkező eszközök szervezetre szabott – az illetéktelenek távoltartása érdekében elkülönített, fizikailag védett objektumba történő – beépítése, valamint a telepítési és javítási, karbantartási ajánlások, előírások és utasítások betartása, továbbá a felderíthetőségi zónahatárok kimérése és esetlegesen elfedő, zavaró jelek kisugárzása.

Az elektronikus információbiztonság főbb szakterületei az alábbiak:

- Átviteli biztonság

  Mindazon védelmi rendszabályok összességének az eredménye, amelyek végrehajtásával biztosítják a kommunikációs adatátviteli utakon, csatornákon az információk sértetlenségének, rendelkezésre állásának és bizalmasságának meglétét, valamint adott esetekben az átvitel hitelességét illetve annak letagadhatatlanságát. [122] Az informatikai és a kommunikációs rendszerek fokozatos egybeolvadása révén ezt a szakterületet egyre inkább hálózatbiztonság keretein belül kezelik.

- Hálózati biztonság

  A hálózatba kötött számítógépek, illetve összekapcsolt számítógép-hálózatok közötti adatkapcsolatok, illetve azok szolgáltatásainak védelmét jelenti a

szolgáltatások színvonalának csökkenése, kapacitások lekötése, a rendszerben kezelt információk illetéktelen megismerése, módosítása és megsemmisítése ellen. Az információs infrastruktúrák védelmi rendszereinek nagyfokú rugalmasságot kell, hogy biztosítsanak az összetett fenyegetések, rosszindulatú támadókódok, DoS és DDoS támadások, IP-forráscím meghamisítások, levélszemetek, adatszivárgások, stb. ellen. A hálózati biztonság hatékonyságát nagyban lehet növelni azzal, ha törekszünk a védelmi rendszerek homogenitására, azaz a különböző helyszíneken és a különböző funkciókra nem különböző gyártók különböző fejlettségű technológiát próbáljuk meg együttműködésre bírni, hanem olyan megoldást alkalmazunk, mely már a tervezés kezdetétől fogva fel van készítve az integrációra.

- Számítógép-biztonság

  Számítógép-biztonság az az állapot, amelyben az informatikai rendszerek a bizalmasság, sértetlenség, rendelkezésre állás elvesztésével szemben védettek. A számítógépes biztonság a hardver-, szoftver- és firmware-biztonságot foglalja magába. [123] Tehát a számítógép-biztonság területe alatt rendszerint a szoftver- és a hardverbiztonság – ide értve a szoftverek és a hardverek megfelelő konfigurálásának, beállításának – együttesét értjük. A számítógépekbe beépítésre kerülő hardverelemek összességének tekintetében elvárás, hogy együttesen képesek legyenek biztosítani az adott szolgáltatás megfelelő színvonalú végrehajtásához szükséges teljesítményt az elvárt biztonsági paraméterek mellett. A szoftvereszközökkel szemben is elvárás, hogy képesek legyenek a funkcióikat maradéktalanul és biztonságosan betölteni. A biztonság tovább növelhető, ha az üzemeltetők az adott feladatra célirányosan készített szoftvereszközöket használnak, ami a hatékonyság mellett a biztonságot is növelik, mivel a támadók nem tudnak a kereskedelmi forgalomban elérhető verziókból felkészülve támadást indítani, bár ennek a megoldásnak költségvonzatai aránytalanul nagyok is lehetnek.

- Rejtjelezés

  A rejtjelbiztonság biztonsági intézkedések és eszközök alkalmazása abból a célból, hogy megvédjék a tárolás és az átvitel alatt az információt az illetéktelen felhasználás (megismerés) ellen, vagyis a rejtjelező eszközök és módszerek

alkalmazásával megvalósított rendszabályoknak az összessége. [124] Tehát minden olyan tevékenység, eljárás, megoldás, amely során a védendő információt abból a célból alakítják át, hogy eredeti állapota az illetéktelen támadó előtt – annak hozzáférése esetén is – rejtve maradjon. A folyamat részét képezi a rejtjelezett adatok eredetivé való visszaállítása is. [125] A rejtjelezés a másik olyan szakterület, mely rendkívül nagymértékben összefügg más szakterületek (személyi, fizikai, dokumentumbiztonság) hatékonyságával.

- Kompromittáló kisugárzás elleni védelem
  Ez a szakterület olyan aktív és passzív eszközök, rendszabályok alkalmazását jelenti, melynek célja, hogy az információs infrastruktúra elektronikai rendszerelemeinek másodlagos sugárzása alapján kialakuló vezetett és sugárzott elektromágneses energia analizálása révén kinyerhető információszerzést megakadályozzák. Megvalósítása során figyelembe kell venni az információs infrastruktúrák érintett rendszerelemeinek, valamint azok elhelyezésére szolgáló épületek sajátosságait (például fizikai elhelyezkedés a városban, megközelíthetőség), és adott esetben az objektum árnyékolásával, tempest eszközök és zavaró-berendezések alkalmazásával kell elzárni az információtól a támadókat. [126]

V. 1. 5. Információs infrastruktúrák nemzetbiztonsági védelme

A kritikus információs infrastruktúrák komplex információbiztonsággal kapcsolatos vázlatokon sok esetben nem tüntetik fel az elhárítást, azonban az előzőekben tárgyalt szakterületek fontos kiegészítője lehet, mely alapfeladatán túl gyakorlatilag értelmezhető azok egyfajta ellenőrzési funkciójaként is.

Az elhárítás azon eljárások és módszerek összessége, melynek alapvető célja az, hogy azonosítsa a kiberterroristáknak, illetve minden ártó szándékú entitásnak az információs infrastruktúra ellen irányuló felderítő jellegű adatgyűjtő tevékenységét (prevenció), illetve magát a támadást (detektálás). További cél, hogy az infrastruktúra belső és külső környezetéből olyan információkat szerezzen be, melyek rávilágítanak a részterületek esetleges gyengeségeire, sebezhetőségeire, a fenyegetésekre, a kockázatokra és a fejlesztési

igényeire (korrekció), valamint azonosítsa a potenciális támadókat, azok motivációit, illetve felbecsülje azok támadási potenciálját.
Tehát az elhárítási szakterület feladata – a szervezeti politika és a jogi környezet függvényében – a rendszert fenyegető veszélyek elemzése, és a kockázatok kezelésére történő protokollok, védelmi intézkedések kidolgozása, a veszélyforrások megszüntetése, illetve a bekövetkezési valószínűség, valamint az okozott kár csökkentése.

A fenti definícióból adódó feladatok végrehajthatósága nagyban összefügg a kérdéses infrastruktúrának egy ország életében betöltött szerepével, mivel egy kiemelt fontosságú – akár magántulajdonú – rendszer esetében rendvédelmi, titkosszolgálati eszközök is igénybe vehetők, addig egy kisebb súlyú információs rendszer üzemeltetőinek többnyire csak saját erőforrásaira hagyatkozhatnak, és információgyűjtő, prevenciós lehetőségeiknek a jogszabályi környezeten túl financiális helyzetük is gátat szabhat.

V. 1. 6. Aszimmetriák azonosítása

A komplex információbiztonság korábban felsorolt szakterületeinek működési folyamatainak hatékonysága vizsgálható az alábbiakban bemutatásra kerülő, esetlegesen létező aszimmetriák azonosítása által is, melyek rávilágíthatnak a védelem, a kárenyhítés és megelőzés gyengeségeire. Az aszimmetriák természetesen nem csak a biztonsági helyzetet érintő folyamatokkal kapcsolatosak, de e terület különösen érzékeny lehet létezésükre.

A modern kor fegyveres incidenseinek egyik jellemzője, hogy a felek között úgynevezett aszimmetrikus hadviselés folyik, ami a fegyveres konfliktusok megvívásának új formája, melynek alapja az, hogy a hadszíntéren jelenlevő fegyveres erők jelentősen különböznek egymástól méreteikben, felszereltségükben és képességeikben. [127] Tehát az egyik fél jelentős (például technológiai, létszám, finanszírozási, stb.) fölényben van a másik féllel szemben, és ennek leküzdése érdekében a hátrányban lévő fél igyekszik az ellenség gyengeségeit kihasználva olyan körülményeket, helyzetet teremteni, melyben eredményesen tud tevékenykedni.
Mint ahogy erre már utaltunk ez a taktika a terrorista szervezetek repertoárjában is megjelenik. Például a kiberterroristák olcsón beszerezhető eszközökkel bizonyos infrastruktúrák szakaszos „zaklatásával” igyekeznek azok működését akadályozni, valamint a

lakosságban veszély- vagy fenyegetettség-érzetet kialakítani, de az állandó, stabil védelem kialakítása az üzemeltetők részéről aránytalanul nagy befektetést igényelne.

A kiberterrorizmus vonatkozásában az aszimmetrikus hadviselésnek, illetve magának az aszimmetriának több „dimenziója" is megjelenhet. Ez az aszimmetria megjelenik az alkalmazott eszközök számának, fejlettségének, minőségének, a bevonható pénzügyi és humánerőforrások fölényében, jellemzően – ám nem minden esetben – az állam vagy a szolgáltató javára, ugyanakkor a terrorcsoportok is tudnak élni olyan lehetőségekkel bizonyos részterületeken, melyek révén kiválóan ellensúlyozni tudják az állam dominanciáját, még akkor is, ha e lehetőségek hátteréről kifejezetten nem is tudnak. Ezek a részterületek az alábbiak lehetnek:

Jogkövetési aszimmetria

Az egyik ilyen triviális terület – mely más részterületekre is hatással van – a jog. Míg a biztonsági és rendvédelmi szervek működésének határozott keretet szabnak a különböző jogszabályok, addig a terrorcsoportokat – sem céljaikban, sem működésükben – értelemszerűen ezek nem korlátozzák, így bármilyen helyzetre rendkívül rugalmasan, akár órák alatt tudnak reagálni. Kreatívan tudnak élni a jog által még nem szabályozott innovatív lehetőségekkel, a technológiai fejlődés révén megnyíló új támadási módokkal.

Ezzel szemben az állami szervek sok esetben elavult technológiai szintet reprezentáló jogszabályi környezetben kell, hogy működjenek, és az érintett jogszabályok megváltoztatásának bürokratikus rendszere (a probléma megismerése, megfogalmazása, egyeztetés, jogszabályok megszövegezése, társadalmi, parlamenti vita) nem is alkalmas a probléma hatékony kezelésére. Tehát hiába ismert egy fenyegetés, arra jogszabályok hiányában, vagy épp kifejezett tiltása miatt reagálni nem lehet.

A jogkövetési aszimmetria részeként fogható fel az a jelenség is, amikor a kibertérben jogellenes cselekményt végrehajtó személyek, csoportok a különböző országok különböző jogrendjeinek „kiskapuit" kihasználva, azok között lavírozva teremtik meg a támadás lehetőségét, vagy visszaélnek a jogsegélyegyezmények anomáliával. Előbbire lehet példa, hogy egyes országokban – bizonyos teljesítmény szintig – nem tiltott a mobilhálózatok blokkolását lehetővé tevő eszközök gyártása, kereskedelme, így innen ezek magánúton, vagy

futárral történő behozatala – megfelelő körülmények fennállása esetén akár törvényesen is – megvalósítható.

Bürokratikus aszimmetria

A szervezeten belüli jogi környezetből eredeztethető, de mindenképpen különálló körülményként említendő, mert még a fejlett technológiai szinthez igazított jogi környezet esetében is megjelenik a bürokratikus aszimmetria, mely nagymértékben képes visszafogni egy szervezet reagáló képességét.

Ez a jelenség alapvetően a szervezet belső munkafolyamataihoz kapcsolódik, amikor a különböző protokollok akadályozzák a szervezet hatékony működését. Ilyenek a különböző szervezeti egységek határidő-kezelésével, engedélyezési folyamatok bonyolultságával, vezetők helyettesítésével kapcsolatos anomáliák. Például az egyik szervezeti egységnek egy adott feladatra – melyben egy másik szervezeti egység is érintett – a szervezeti és működési szabályzat (SZMSZ) szerint egy napja van, ám a másik szervezetnek bármi nemű megkeresésre az SZMSZ öt napot ad válaszolni, így a megkeresés várhatóan nem fog időben megválaszolásra kerülni. A jelenség bizonyos tényezők, mint például a biztonság sérülése esetében kritikus jelenségként értékelhető.

Ez az aszimmetria az üzemeltetővel együttműködő külső partnerek esetében is megnyilvánulhat. A kibertérben zajló incidensben érintett biztonsági és rendvédelmi szervek működése során olyan – jogszabályokból (például Rtv, Nbtv) következő, de akár belső szabályzatokból, utasításokból levezethető – adminisztratív teendőik (engedélyek beszerzése, javaslatok elkészítése, egyeztetések, stb.) keletkeznek, melyek valós időben jelentősen korlátozzák, vagy épp ki is zárják az érdemi beavatkozás, későbbi nyomozati cselekmények, bizonyítási eljárások lehetőségét.

Például egy incidens, vagy egy jogellenes cselekmény bekövetkezésekor az érintett szervnek várnia kell, hogy a támadás tényét hivatalosan megerősítsék (feljelentés), intézkedési tervet kell készítenie, külső engedélyeket kell beszereznie, más szervekkel kell összehangolnia tevékenységét, holott a támadásban érintett szolgáltatónál a későbbi bizonyításhoz szükséges naplózási adatok akár percek alatt felülíródhatnak.

Protokolláris aszimmetria

Ez az anomália a szervezeti kultúra egy jelensége, mely akár a bürokratikus aszimmetria speciális eseteként értelmezhető, és amit rendszerint a belső szabályzók sem képesek kezelni. A döntési és engedélyezési szintekhez kapcsolódó visszásságok tartoznak ebbe a körbe. Például amikor a sűrűn jelentkező, ám alacsony prioritású helyzetben a döntéshozói pont a szervezetben túl magas szintre pozícionált, és az illetékes, jellemzően felsővezető nem a szükséges pillanatban hozza meg a döntését, hanem ezeket kérdéseket összegyűjtve – akár heti, havi bontásban vagy kellő darabszám esetén – tömegesen terjesztik fel számára, ami az adott folyamatokban huzamosabb ideig tartó fennakadásokat és egyéb károkat, érdeksérelmeket okozhat.

Finanszírozási aszimmetria

A költségek dimenziójában szintén nagy aszimmetria jelentkezhet. Egyrészt az egyre fejlettebb és így egyre drágább eszközökből álló rendszerek kialakítása, valamint a technológiai fejlődésből adódó avulás okán a viszonylag sűrű termék- vagy eszközváltási ciklusok már önmagukban, a piaci versenyből adódóan terheket rónak az infrastruktúrák üzemeltetőire, ugyanakkor a támadók repertoárjában megjelenő minden új módszer, új technológia lépéskényszerbe is hozza őket, hiszen ezek elhárítása érdekében – a korábban kalkulált üzleti tervektől eltérően – reagálniuk kell. Ez jelentheti az alkalmazott szoftver- vagy eszközpark részleges, de akár teljes cseréjét, vagy azok jelentős szám- vagy képességbeli bővítését, de jelenthet humánerőforrás terén történő fejlesztést (létszámbővítést, képzést) is, melyet egyébként a normál piaci működés nem tenne indokolttá.

Tehát amíg a támadók egy módszer, eszköz birtokában, vagy sérülékenység ismeretében az adott infrastruktúra bármelyik részelemét támadhatják, addig az üzemeltetőnek az összes infrastruktúra elem védelméről gondoskodnia kell, így a védelem költségei nagyságrendileg nagyobbak lehetnek, mint a támadók anyagi ráfordításai, mely jelenség alkalmas az üzemeltetők anyagi kifárasztására, mely további negatív hatásokat indukál.

A költségbeli aszimmetriának egy vetülete megnyilvánulhat egy sikeres támadást követően is, amikor az érintett infrastruktúrát ügyfelei a bizalomvesztés miatt tömegesen hagynak el, mely ügyfelek visszaszerzése, esetleges kártalanítása, illetve általában a szolgáltatásokba vetett bizalom visszaállítása nagyságrendileg nagyobb lehet, mint a kiberterroristák anyagi ráfordítása.

Kapacitásbeli aszimmetriák

A kapacitásokhoz kapcsolódó aszimmetria mutatkozhat például a rendvédelmi szektor irányából. Az egyre fejlettebb eszközöket és egyre kifinomultabb módszereket használó támadások – melyek száma évről-évre nő – kivédése és elhárítása, illetve a megtörtént incidensek, bűncselekmények és terrortámadások körülményeinek, valamint a gyanús tevékenységek vizsgálata egyre költségigényesebb, mind az alkalmazott eszközök, mind pedig a bevont humánerőforrások tekintetében. Továbbá a rendelkezésre álló, e feladatra felkészített személyi állomány véges létszáma is korlátot szab a vizsgálható, lereagálható incidensek számának.

Technológiai aszimmetria

A technikai, technológiai aszimmetria jelensége megjelenik egyrészt a költségek dimenziójában már vázolt módon, amikor is kiberterroristák olyan új technológiákkal, új módszerekkel hajtanak végre támadást, melyek az információs infrastruktúrák üzemeltetői előtt eddig „ismeretlenek” voltak, illetve nem alkalmazták őket, nem védekeztek ellenük. Másrészt az aszimmetriának e dimenzióját elő lehet idézni oly módon is, hogy a különböző rendszerelemek konfigurációs környezetében lévő gyengeségekre alapozva aránytalanságokra építik fel a támadást.

Ez utóbbi – nem kibertámadás gyanánt megjelenő – aszimmetriára lehet példa az a 2009-es eset, amikor az egyik magyar mobilszolgáltató rendszerében használt „jailbreakelt” iPhone készülékek hibás kapcsolatteremtési kísérletek révén a jelzésátviteli rendszerben hálózati szintű problémát okoztak. A megközelítőleg százötven készülék megállás nélkül, rendkívül sűrűn próbálkozott felvenni a kapcsolatot az adatátviteli rendszerrel, előfordult, hogy egy-egy bázisállomás néhány száz sikeres kapcsolatfelvétel mellett több tízezer sikertelent is regisztrált, ami jelentősen csökkentette azok kapacitását. A hibajelenség azonosítása érdekében – humán, technikai, pénzügyi – erőforrásokat kellett felszabadítani, azonosítani kellett a készülékeket, azok előfizetőit, felvenni velük a kapcsolatot, PR megfontolásokból a hibás szoftver cseréjére fel kellett készülni, azt le kellett bonyolítani, mely időtartam alatt a készülékek a rendszerben folyamatos hibákat indukáltak. [128]

A fentebb kiemelt aszimmetriák természetesen nem fedik le ezt a „jelenséget” teljes körűen, mivel minden szervezetnek saját munkafolyamatai, saját szervezeti kultúrája és belső szabályzói vannak, illetve más ügyfélkörrel, más piaci és jogszabályi környezetben

működnek, így szervezetenként jelentősen eltérő lehet azon aszimmetriák köre, melyek fennakadást okozhatnak a szervezet életében.

A fentiekre reagálva, javaslatom szerint a különböző aszimmetriák elkerülése érdekében az üzemeltetőknek szükséges egy – a saját szervezetükre, de legalább kritikus munkafolyamataikra illeszkedő módszertan alapján – aszimmetria vizsgálatot végezniük.

E vizsgálat keretében fel kell deríteni azokat a pontokat a szervezet belső munkafolyamatiban (például belső engedélyezési metódusok bonyolultsága, döntéshozói vagy beavatkozási szintek pozicionálása), illetve egyéb állapotjelzőkben (például financiális helyzet, szolgáltatások kieséséből adódó kötbérfizetési kötelezettség, földrajzi kitettség, alkalmazott technológia, műszaki berendezések, külső megállapodások, vagy épp az ügyfélkör összetétele), melyek egy rendkívüli esemény bekövetkezésekor aránytalanul megnehezítenék, vagy költségessé tennék az adott információs infrastruktúrák további, rendeltetés szerinti működését, vagy visszaállítását, illetve a károk felszámolását. A kritikus pontok azonosítását követően pedig – a kockázatok mértéke, az ésszerű gazdaságossági határok és jogi keretek között – intézkedni kell a kérdéses gyengeséget okozó körülmények kiküszöbölésére (például a szervezeti és működési szabályzat módosítására).

Ugyanakkor ezt az aszimmetria vizsgálatot a kibertér szabályozására hivatott, vagy az információs infrastruktúrákat ért esetleges rendkívüli események kivizsgálásába bevont állami szereplőknek is célszerű végrehajtani. A tapasztalatok tükrében pedig olyan jogszabályi és műszaki, technológiai környezetet kell alkotni – összhangban az üzemeltetők és a társadalmi entitások érdekeivel – melyben az érintettek érdemi idő alatt reagálni tudnak az infokommunikációs szféra gyorsütemű fejlődésére, és hatékonyan választ tudnak adni a kiberteret érintő jogellenes cselekmények jelentette kihívásokra és konkrét incidensekre.

Az aszimmetria bizonyos dimenziói ugyanakkor kombinálhatóak is egymással, mely a védelem szempontjából fokozottan hátrányos helyzetet okoz. Az 1. számú melléklet a rendvédelmi szektor vonatkozásában mutat be egy példát. A kiberterroristák az általuk használt kommunikációs eszközöket, hívószámokat, felhasználóneveket hetente lecserélik. A tevékenységüket ellenőrizni próbáló rendészeti szerv külső és belső jogi környezettel harmonizáló információs ciklusa (humán felderítés, technikai adatgyűjtés, adatellenőrzés, engedélyezés, problémaazonosítás) ennek többszöröse, és mire a folyamat lezárulna, addigra a

megfigyelt személyek újabb eszközcserét hajtanak végre, és ennek az aszimmetriának az a következménye, hogy a rendészeti szerv vezetési ciklusa nem képes lépést tartani a kiberterroristák által generált környezeti változásokkal.
Ennek a folyamatnak az indoka és magyarázata az információ elérhetőség és időperiódus tulajdonságához és a döntéshozói folyamatok körciklusához kapcsolódik, tehát amikorra az információ elérhetővé válik és a döntéshozói cikluson végig ér, addig már nem a valóságot tükrözi és nem a valós helyzetre reagálnak az illetékesek, így az általuk hozott intézkedések hatástalanok.

Az aszimmetria vizsgálatot a működés és a biztonság szempontjából kritikus folyamatok, munkafázisok vonatkozásában szükséges végrehajtani, melynek kivitelezője lehet egy adott szervezeti egység saját folyamatainak tekintetében, illetve a szervezet általános felügyeleti szerve. A vizsgálat módja lehet:

- A folyamatokat szabályozó külső és belső jogi normák áttekintése.
  Ez vonatkozhat a külső és belső jogszabályok harmonizációjára, illetve a folyamatokban érintett szervezeti egységek tevékenységét szabályozó belső normák összhangjára. Amennyiben szervezeten kívüli együttműködés is megjelenik a folyamatban, akkor erre is célszerű kiterjeszteni a vizsgálatot.
- A folyamatokban résztvevő munkatársak tapasztalatainak összegyűjtése.
  Az adott szakterületeken foglalkozatott munkatársak végrehajtva a folyamatokkal kapcsolatos teendőket alapos ismeretekkel rendelkezhetnek azokról az körülményekről (például technológiai hátrány, eszközök hiánya, humán kapacitások hiánya, kezelhetetlen határidők, engedélyezi szintekkel kapcsolatos anomáliák, helyettesítés, stb.), melyek aránytalanságokat okozhatnak.
- Időszakosan célszerű a folyamatok hatékonyságát stressz-tesztek alkalmazásával is felmérni, amikor is előzetes bejelentés nélkül (ne legyen idő rákészülni), akár extrém feltételek mellett (például szűk határidőkkel, rendelkezésre álló létszámú és képzettségű személyi állománnyal, eszközökkel) kell a folyamatokat, munkafázisokat végrehajtani.

Ideális esetben a szervezetek a napi rutin során feltárt anomáliákat haladéktalanul korrigálják, azonban ez pont a bürokratikus aszimmetria kapcsán akadályokba ütközhet, amikor a belső szabályzók kötöttsége, ehhez kapcsolódó protokollok nem teszik lehetővé a gyors reagálást.

V. 1. 7. Működési és biztonsági interdependencia térkép

Az információs infrastruktúrák üzemeltetése során számos belső, szervezeti egységek közötti, illetve külső, infrastruktúra és külső partnerek közötti kapcsolat alakul ki, melyek folyamatos, zökkenőmentes megléte biztosítja az adott információs infrastruktúra rendeltetésszerű működését. E kapcsolatok tartalma sokrétű lehet, azonban minden esetben valamilyen cél, igény kielégítése érdekében, és általában valamilyen feltételrendszer mellett alakulnak ki. A kapcsolatok minőségükben lehet például szolgáltató-megrendelő, állam-jogalkalmazó szolgáltató, tartalmában adatszolgáltató, adatigénylő, pénzügyi, feltételrendszerében pedig szerződésen alapuló.

Amikor a kapcsolatok megszakadnak, minőségükben változnak, az a szervezet működésére értelemszerűen mindenesetben kihatással van, tehát a szervezet valamely funkciója, képessége, állapotjelzője sérül. A hatásnak nagysága a kapcsolat fontosságával rendszerint összefüggésben van, és a következmények nagy valószínűséggel a szervezet más folyamataira, állapotjelzőire is kihatással lesznek. Tehát a zavartalan működés, illetve az esetleges kockázatok feltárása céljából szükséges a szervezet kapcsolatainak, függőségeinek feltárása, illetve ezzel egy időben azoknak a külső és belső körülményeknek az azonosítása, melyek a kapcsolatokra és azok minőségére kihatással vannak.

Az információs infrastruktúrák biztonságos, stabil üzemeltetésének és komplex védelmének érdekében indokoltnak tartom a működési és biztonsági interdependencia térkép bevezetését.

A térkép működési dimenziója – egyfajta folyamatindikátorként – egyértelműen feltárja egy adott infrastruktúrának saját alrendszerei, más külső rendszerek, szolgáltatók irányába meglévő direkt (szerződésen alapuló) és indirekt (például más közszolgáltatások, úgymint közlekedés, egészségügy) kapcsolatait. Azonosítja továbbá az ezekre a kapcsolatokra veszélyt jelentő körülményeket (politikai, gazdasági, rendészeti, stb.), valamint az esetlegesen bekövetkező rendkívüli események (például sztrájkok, kibertámadások, természeti katasztrófák, stb.) saját infrastruktúra működésére gyakorolt negatív hatásait, és azok elhárításának, a kieső funkciók kiváltásának és a kárenyhítés lehetőségeit.

Megjegyzendő, hogy a veszélyt jelentő körülmények folyamatos és mélyreható monitorozásával – bizonyos esetekben – a működési interdependencia elemzésének magasabb fokára is lehet lépni, amikor már nem az adott infrastruktúrával kapcsolatban álló rendszer interdependenciáját vizsgálják, hanem a kapcsolódó rendszerek más rendszerekkel való – és

az elemzők előtt ismerté vált – függőségi és hatásviszonyait, amelynek esetleges zavarai a saját infrastruktúrába is begyűrűzhetnek.

A térkép biztonsági dimenziója pedig – szintén egyfajta jelzőként – mutatja az információs infrastruktúra biztonsági szakterületeinek sajátságos, csak rá jellemző egyedi elegyének állapotát, kölcsönös függéseit, összefüggéseit. Feltárja, hogy bizonyos biztonsági szakterületek vonatkozásában megjelenő kapcsolatok, körülmények milyen hatással lehetnek az adott szakterület hatékonyságára, illetve, hogy ez milyen módon gyűrűzik át más biztonsági szakterületek helyzetére, illetve a teljes infrastruktúra működésére.

Hasonlóan a működési dimenzióhoz, a biztonsági vonatkozású körülményekben bekövetkező változásokat is folyamatosan figyelemmel kell kísérni, mivel egy technológiai ugrás, az alkalmazott védelmi rendszerek kapcsán napvilágra kerülő, eddig nem ismert sérülékenység, vagy szerződésen alapuló kapcsolatban történt változás a biztonsági interdependencia térképet is átrendezheti, ami azonnal beavatkozásokat indukálhat a védelmi stratégiában.

Természetesen a működési és biztonsági dimenzió akár több ponton is kapcsolódhat és hatást gyakorolhatnak egymásra. A 2. számú Mellékletben vázolt, egy munkafolyamatra vonatkozó térképelem ezt a kapcsolódást mutatja be. A pénzügyi rendszerben bármi okból bekövetkező zavar miatt az adott információs infrastruktúra által bérelt szolgáltatás díja nem érkezik meg időben az IT szolgáltatóhoz, ezért az csökkenti az általa nyújtott informatikai szolgáltatások minőségét, tartalmát, vagyis szűkíti az általa biztosított védelmi portfólió összetételét. Ez a minőségromlás pedig kihatással van az adott információs infrastruktúra szolgáltatásainak és védelmének színvonalára, és az ekkor esetlegesen bekövetkező kibertámadás miatt bizonyos, más rendszerek számára nyújtott szolgáltatásai is akadozhatnak, ami más infrastruktúrákban okozhat továbbgyűrűző hatásokat.

A működési és biztonsági interdependencia térkép elkészítése azonban szervezetszintű feladat, azt – megítélésem szerint – szűk alkalmazotti réteg nem képes összeállítani, mivel egy-egy személy nem ismerheti a szervezet működésének minden, biztonsági, gazdasági, műszaki, jogi, humán, stb. aspektusát. A kapcsolatok, függőségek összeállítása csapatmunka, melyben minden szakterületnek részt kell venni és a különböző munkafolyamatokat vázolva közösen kell keresni kritikus kapcsolatokat, és azok megszakadásának következményeit, valamint többszörösen továbbgyűrűző hatásait. A megállapítások célszerű

munkafolyamatonként összegezni – melyre a 3. számú Melléklet mutat példát – majd ezeket elemezve azonosítani azokat kapcsolatokat, hatásokat, melyek a szervezet szempontjából létfontosságúak lehetnek.

A 2. számú Mellékletben vázolt fiktív példához kötve a fentieket, több munkafolyamat elemzését követően levezethető, hogy a pénzügyi rendszer értelemszerűen kritikus fontosságú, melynek zavartalan működését azonban csak két fő végzi, szükség szerint egymást kölcsönösen helyettesítve, mivel ők rendelkeznek ehhez jogosultsággal, végzettséggel. Azonban ilyen kis létszámnál ez a szakterület rendkívül sérülékeny, mivel bárminemű rendkívüli esemény (járvány, betegség, baleset, közlekedési káosz, rossz időjárás) bekövetkeztekor az érintettek nem jutnak el munkahelyükre, tehát ez a funkció akár huzamosabb ideig is leállhat, és feszített utalási határidőknél ez akár azonnali hatásokat indukál.

Mivel egy működési és biztonsági interdependencia térkép különösen érzékeny adatokat (üzleti titkokat, belső folyamatok, konkrét technológiai, műszaki paramétereket, azonosított kockázatokat) tartalmaz az információs infrastruktúrákról, ezért az üzleti titokként, bizalmasan kezelendő, nyilvánosságra nem kerülhet, tartalmát csak az arra felhatalmazott személyek ismerhetik meg.

Azonban az információs társadalom, illetve a nemzetgazdaság szempontjából kiemelt fontosságú információs infrastruktúrák esetében a működési és biztonsági interdependencia térképet – jogszabályok keretei között, megfelelő protokollok kidolgozását követően és folyamatos aktualizálás mellett – célszerű lehet megosztani az állam e funkcióra kijelölt szervezeteivel, szerveivel.
E megosztás kölcsönös előnyökkel járna, mivel egyrészt az állami szereplők iránymutatást kaphatnának az elhárítási tevékenység súlypontjairól, az információgyűjtés potenciális irányairól, az infrastruktúrák aktuális biztonsági helyzetéről, érzékenységükről – ezáltal növelve a rendelkezésre álló korlátos erőforrásaik hatékonyságát. Másrészt pedig a speciális állami szervezetek – már az előzőekben tárgyalt – különleges feladatköreik, jogi felhatalmazásaik és képességeik alapján olyan információk birtokába kerülhetnek, melyeket már célirányosan – a működési és biztonsági interdependencia térkép információi alapján – a veszélyben lévő érintettekkel meg tudnak osztani, mely révén pedig az infrastruktúrák biztonságának színvonala és a védelem költséghatékonysága növelhető.

V. 2. Megelőzés

Az információs rendszerek elleni támadások jelentős része kivédhető lenne egy jól átgondolt megelőzési stratégia kidolgozásával, illetve betartásával és betartatásával, mivel ezáltal jelentősen lecsökkenthető a támadási felületek nagysága, és megnehezíthető a műszaki, valamint a humán oldalról jelentkező behatolási csatornák kiépítése.

Az információs infrastruktúrák üzemeltetőinek a megelőzés érdekében folyamatosan fejleszteniük kell a biztonsággal kapcsolatos eszközeiket, módszereiket, illetve biztonsági kultúrájukat, valamint alkalmazniuk kell a jogszabályokat, ajánlásokat és szorosan együtt kell működniük a különböző állami szervekkel. Meg kell teremtenie azokat a belső körülményeket, melyek hozzájárulhatnak a megkívánt biztonság szint eléréséhez és fenntartásához (például megfelelő végzettséggel és gyakorlattal rendelkező munkavállalók foglalkoztatása, folyamatos képzése, akiknek feladat- és felelősségi körükkel arányos javadalmazásuk révén lojalitása megkérdőjelezhetetlen).

A különböző kockázatelemző metódusok rendszeres alkalmazásával (például a CRAMM-modell) és/vagy az üzemeltető szervezettől független auditálások révén feltárhatók a rendszert érintő hiányosságok, biztonsági rések, melyek egyben meg is adhatják a biztonsági fejlesztések, rezsimintézkedések módosításának irányát. [129]

Nyilvánvaló, hogy a nemzeti kritikus infrastruktúrák védelmét, ezen belül információs támadások elleni védelmét az adott állam igényei, követelményei alapján, irányítása és koordinálása mellett, az államon kívül számos más szereplő együttműködésével kell megvalósítani. A kritikus infrastruktúrák védelme tehát egy olyan tevékenységrendszer, amelynek jelentős része az adott állam hatáskörén kívül kerül megvalósításra. [130] Ugyanakkor ez az állam részéről egységesített adat- és információkezelési, védelmi irányelveket, központi irányítást, szabályozást, ellenőrzést követel meg, amely nem lehet az üzemeltetők önállósági körébe tartozó feladat, és nem lehet szolgáltatói és termékverseny területe sem. Az államnak ebben a környezetben a magántulajdonban lévő vállalatok irányába egyfajta új – nemzetbiztonsági és közrendvédelmi – szolgáltatásként is értelmezhető tevékenységet kell végeznie ahhoz, hogy a kritikus információs infrastruktúrák, és így az információs társadalom működése is zavartalan legyen.

V. 2. 1. Az infrastruktúraüzemeltetők lehetséges feladatai a megelőzésben

Az információs infrastruktúrák folyamatos üzem- és információbiztonságához kapcsolódó feltételrendszerének kialakítása és fenntartása – mindig igazodva a hatályos jogszabályi környezethez – alapvetően az üzemeltetők feladata. Ennek során elengedhetetlen a fentiekben tárgyalt komplex információbiztonság szakterületeinek kialakítása, illetve azon túlmutatóan az alábbi kérdéskörök vizsgálata, melyek szintén befolyásolhatják az infrastruktúrák biztonsági helyzetét:

- A szakszerű és folyamatos üzemeltetéshez szükséges humán erőforrások

  A biztonságos üzemeltetéshez elengedhetetlenül fontos a jól képzett, tapasztalt és a megfelelő biztonsági kultúra jelentőségét megértő, elfogadó és elsajátító munkaerő, akiknek mindezek mellett rendelkezniük kell a megfelelő szintű biztonsági tanúsítványokkal is.

  Ezzel párhuzamosan a munkáltató részéről is szükséges a munkavállalói igényekhez közelítő juttatási rendszer kialakítása a szakemberek megtartása, a lojalitás fenntartása, a korrupció, az adatszivárogtatás és az esetleges ipari kémkedés megakadályozása érdekében.

- A szükséges eszközpark megléte a folyamatos szolgáltatás-ellátáshoz

  Az üzemeltetőknek az információs infrastruktúrák felhasználóinak igényeit maradéktalanul kielégítő szolgáltatások folyamatos biztosításának érdekében – összhangban finanszírozási politikájukkal, pénzügyi helyzetükkel – olyan berendezéseket, infrastruktúraelemeket kell, hogy alkalmazzanak, melyek az adott műszaki paraméterek között hibamentesen működnek, ésszerű határok között zavar- és zajállóak, kibertámadás esetén pedig kiesésük a rendszer egészének stabilitását lehetőleg nem befolyásolja. Az időszakosan fellépő extrém nagy felhasználói igények által generált terhelések sem veszélyeztethetik jelentősen a rendszer üzem-, valamint adatbiztonságát.

- A technológiai fejlődés hatása a rendszer biztonságára

  Az infokommunikációs eszközök dinamikus fejlődése, új technológiák térnyerése az üzemeltetők számára versenyképességi okokból, illetve egyéb új szolgáltatások bevezetése kapcsán szükségessé teszi azt, hogy egyes rendszerelemeket, illetve eszközcsoportokat folyamatosan fejlesszék, cseréljék, mivel ezek avulása az

üzembiztonságot veszélyeztethetik, inkompatibilitási problémákat okozhatnak, sérülékennyé teszik az infrastruktúrát.

Továbbá az információs rendszerben nem rendszeresített, a beépített eszközöknél fejlettebb, és rosszindulatúan, de akár jóindulatúan is felhasznált technológiák – például inkompatibilis kliensgépek hatásainak „kezeletlensége" – szintén negatívan befolyásolhatják a rendszer általános szolgáltatási szintjét.

- A beszerzett eszközök forrása, származása, ennek hatása a biztonsági helyzetre
  A kritikus információs infrastruktúrák kiépítése, bővítése és fejlesztése során előfordulhat, hogy a gyártó, illetve a beszállító gazdasági társaságok önhibájukon kívül – tervezési, konstrukciós, gyártási hibákból kifolyólag – nem megfelelő műszaki paraméterekkel rendelkező, vagy éppen – a későbbi jogellenes beavatkozás érdekében – szándékosan manipulált rendszerelemeket kívánnak beépíteni. A szándékos manipulációk mögött meghúzódhatnak gazdasági, vagy bizonyos országok esetében hatalmi, vagy hírszerzési törekvések.
  Az ebből fakadó kockázatoknak az elkerülése érdekében indokolt a gyártói, beszállítói kör folyamatos ellenőrzése, illetve a kritikus funkciókat ellátó berendezések típusengedélyeinek, egyedi tanúsítványainak beszerzése, illetve bizonyos eszközök esetében pedig a különböző frissítések képességeinek ellenőrzése.

- A beszállítói kör megbízhatósága
  A kritikus infrastruktúrákat üzemeltetők az esetek egy részében nem rendelkeznek, vagy nem is kívánnak fenntartani bizonyos feladatok ellátásához szükséges fejlesztői, karbantartói, adatkezelői és raktározási kapacitásokat (outsourcing). A fontos részfeladatok végrehajtásába bevonásra kerülő alvállalkozói kör biztonsági kockázatokat rejthet magában, mivel előfordulhat, hogy az ott foglalkoztatott személyi kör (szaktudása, lojalitása, kapcsolati köre), a vállalkozás pénzügyi helyzete, technológiai fejlettsége nem teszi alkalmassá a feladat ellátására, ezért az üzemeltető objektumaiban megjelenő személyek, vállalkozások, valamint tevékenységük folyamatos ellenőrzése csökkentheti a kockázatokat.

- A rezsimintézkedések aktualizáltsága, betartásának szintje

  A szolgáltatóknál kezelt különböző szintű minősítéssel rendelkező információk védelme kiemelt feladata minden szervezetnek, melynek megvalósítását legtöbb esetben szabályzatokra építik. Azonban sok esetben a szabályzatokban foglaltak a szervezeti felépítéssel és működéssel, valamint a technológiai megoldásokkal nem állnak összhangban. További probléma lehet, hogy a szabályzatban foglalt intézkedések nem, vagy nem szakszerűen kerülnek végrehajtásra, ezért szükséges lehet azok a szervezettől független külső szerv által történő elfogulatlan – lehetőség szerint visszatérő – ellenőrzése.

- A kritikus infrastruktúra fizikai védelmével kapcsolatos intézkedések

  A rendszerelemek fizikai védelmére az üzemeltetőnek – a fenyegetések kockázatával és az érintett rendszerelem kritikusságával arányos – intézkedéseket kell foganatosítnia. Ezek felmérése érdekében folyamatosan monitoroznia kell az érintett rendszerelemek környezetét, és indokolt esetben emelnie kell biztonsági rendszabályok szintjét (például szigorítani a beléptetés rendjét), vagy újabb fizikai védelmi eszközöket kell beépíteni (például térfigyelő rendszer képességeinek bővítése).

- A hatályos jogszabályoknak való megfelelés

  Bizonyos kritikus információs infrastruktúrák üzemeltetésének az egyik alapfeltétele a hatályos jogszabályoknak való megfelelés, mely garantálja a különböző metódusok, módszerek egységes értelmezését, ebből kifolyólag megkönnyítik az együttműködés lehetőségét az érintett felek (például hatósági szervek, más információs infrastruktúrák) között. E célok érdekében indokolt a különböző jogszabályok, szabványok folyamatos nyomon követése, változások esetében pedig a belső jogszabályok megváltoztatása, illetve már a jogalkotás kezdeti szakaszaiban lévő normákat is célszerű figyelembe venni (például a perspektivikus beruházások során).

V. 2. 2. Állami szervek lehetséges feladatai a megelőzésben

A kritikus infrastruktúrákat üzemeltetők a kiberterrorizmus megelőzésének területén érdemi lépéseket tehetnek, azonban a fenyegetések elhárításának vonatkozásában jellemzően nem

rendelkeznek megfelelő szakmai ismeretekkel, illetve jogszabályi felhatalmazással. Természetesen itt nem arra kell gondolni, hogy nem képesek egy előre lefektetett és ellenőrzött protokoll alapján egy támadást elhárítani, vagy annak hatását csökkenteni, hanem arra, hogy az állam birtokában lévő monopóliumok (például jogalkotás, vagy a titkos szolgálati eszközök) alkalmazásával a megelőzés – és olykor a kárcsökkentés – hatékonysága jelentősen növelhető. Ezek az eszközök az alábbiak lehetnek:

- Az információs infrastruktúrákra veszélyt jelentő eszközök gyártásának, kereskedelmének ellenőrzése

  Az infokommunikációs eszközök többsége az elektromágneses spektrumot használja, így a támadások során megjelennek az elektronikai felderítés, zavarás, megtévesztés és pusztítás eszközei is. A kiberterroristáknak számos olyan eszköz kerülhet a birtokába, mellyel jogellenes tevékenységét a támadott objektumok megközelítése nélkül is végrehajthatja.

  A nemzetközi szabályozás ezen eszközök birtoklására és használatára vonatkozóan eltérő, így bizonyos országokban ezek az eszközök (például GPS-, GSM Jamming) minden gond nélkül beszerezhetők, akár az interneten keresztül is megrendelhetők, így Magyarországra is kisebb-nagyobb erőfeszítéssel behozhatók, illetve egy részük a kereskedelmi forgalomban lévő alkatrészek átalakításával is létrehozható.

  Ezért szükséges az e körbe tartozó eszközök legális kereskedelmének ellenőrzése, illegális kereskedelmének felderítése, esetlegesen birtoklásuk tilalmának elérése, szükség szerint büntetőjogi szankcionálása.

- Jogszabályok alkotása, betartatása

  A kereskedelmi és a büntetőjogi szabályozáson túl az állam különböző – a technológiai fejlődést dinamikusan lekövető – jogszabályok, ajánlások, szabványok megalkotásával tudja befolyásolni a kritikus infrastruktúrák üzemeltetőinek tevékenységét, hogy azok az elvárt standardok szintjén működjenek.

  Ugyanakkor elengedhetetlenül szükséges annak folyamatos vizsgálata is, hogy a jogszabályok hatálya alá tartozó szervezetek az elvárásokat milyen színvonalon teljesítik, mennyiben felelnek meg az előírásoknak, illetve az esetleges jogszabálysértések milyen veszélyeket indukáltak, milyen károkat okoztak.

- Megelőzés megközelítése a technológia oldaláról

  Az információs infrastruktúrák elemeit alkotó hardverelemeknek meg kell felelniük, biztonsági, célszerűségi és megbízhatósági követelményeknek, azonban az üzemeltetők részéről a gazdasági és a financiális megfontolások könnyen felülírhatják ezeket az alapvető feltételeket. A hardverelemek biztonságosságát megfelelő szakértői és engedélyezési rendszerrel kell garantálni, amely vonatkozik az új technológiai fejlesztésekre is. Célszerű a hardverelemek beszerzésénél figyelembe venni a gyártók részéről felmerülő kockázati tényezőket, és ezek ismeretében visszatérően ellenőrizni és tesztelni az eszközöket.

- A megelőzés megközelítése a humán tényezők oldaláról

  Az üzemeltetők személyzeti politikája nem minden esetben van összhangban a nemzetbiztonsági érdekekkel (például nem ellenőrizhető háttérrel rendelkező külföldi állampolgárságú munkavállalók foglalkoztatása), ezért az érzékeny beosztásokban foglalkoztatott alkalmazottak biztonsági ellenőrzése elengedhetetlen.

  Bizonyos esetekben pedig a beszállítói kör által foglalkozatott, ismeretlen hátterű munkavállalók körülményeinek ellenőrzésére (életvitelükre, kapcsolati körükre) is érdemes fókuszálni, mivel ők is birtokába kerülhetnek védendő információknak.

- Rezsimintézkedések meglétének és betartatásának ellenőrzése

  A kritikus információs infrastruktúrákat üzemeltetőknek a kockázatokkal arányos, megfelelő védelmet biztosító rezsimintézkedéseket kell alkotniuk, melyek betartásának szintjét, aktualitását visszatérően szükséges vizsgálni.

  Ezeket az ellenőrzéseket nyílt és leplezett módon is célszerű végrehajtani, melynek végrehajtói lehetnek az üzemeltető szervezet erre létrehozott szervezeti egységei, külső auditáló szervezetek, illetve lehetnek az államnak e célból létrehozott szervei is (felügyeletek, hatóságok, biztonsági szolgálatok).

- A védendő infrastruktúra biztonsági helyzetét érintő nyílt információk beszerzése

  Az információs rendszereket érintő fenyegetések megelőzésének területén folytatott tevékenység eredményes ellátásához szükséges azon ismeretek beszerzése, melyek révén fel lehet mérni a meglévő kockázatokat, azok mértékét,

illetve megszüntetésének módját. Ez a fajta információgyűjtő tevékenység történhet a nyomtatott és az online szaksajtó tanulmányozása révén, ahol tematizálva kerülnek összegyűjtésre az egyes részterületekkel kapcsolatos új ismeretek, tesztek, tapasztalatok és kutatási eredmények.

További információs felület lehet a különböző tudományos konferenciákon történő részvétel, ahol hasznos információk birtokába kerülhetnek a szakemberek, illetve a különböző internetes felületek (például hacker-fórumok) rendszeres nyomon követésével esetlegesen a védendő rendszer – valamint az ott alkalmazott technológiák – gyengeségeiről is lehetőség nyílik ismereteket szerezni, melyek a megelőzés során hatékonyan hasznosíthatók.

- Intézményi rendszer fenntartása

  A kritikus információs infrastruktúrák védelmében kiemelt szerep hárulhat az állam által kialakított, fenntartott intézményrendszernek (például hatóságoknak, felügyeleteknek, CERT-eknek). Fontos küldetése lehet a fenyegetések azonosításában, megelőzésében, a kockázatok becslésében, illetve az állami szervek, valamint az információtechnológia területén működő szolgáltatók, gazdasági társaságok tapasztalatainak hozzáférhetővé tételében, nemzetközi kapcsolattartásban, támadások előrejelzésében, elhárításában, a keletkezett károk enyhítésében, felszámolásában.

V. 2. 3. Állami szervek feladatai a fenyegetések felderítésében

Az információs infrastruktúrák védelme, illetve az ehhez kapcsolódó preventív jellegű háttértevékenység során felmerülhetnek olyan sajátos és perspektivikus feladatok, melyek hatékony és jogszerű végrehajtására csak az állam e célra létrehozott, különleges felhatalmazással rendelkező információgyűjtésre specializált szervezetei képesek.

- Kiberterroristák tevékenységének ellenőrzése

  A kiberterrorizmus elleni védekezés során figyelembe kell venni, hogy bizonyos személyi kör speciális képessége, illetve magas szintű informatikai, programozói tudása révén képes arra, hogy információs infrastruktúrákat bénítson meg, az abban található adatokhoz hozzáférjen, illetve azokat megváltoztassa, elérhetetlenné tegye, így ők kiemelt célpontjai lehetnek a terrorista ideológia terjesztésének.

Az egyik ilyen személyi kör a „fekete kalapos hackerek", akik illegális informatikai cselekményeket hajtanak végre, míg a „fehér kalapos hackerek", akik a tudásukat a „jó ügy" szolgálatába állítják. Utóbbiak jóindulatúak, jellemzően biztonsági cégeknél dolgoznak, ott különböző biztonsági rendszereket tesztelnek, javítanak. A rosszindulatú hackerek ugyanakkor jogellenes tevékenységük során különböző személyek – köztük akár védett állami vezetők, hírességek – bizalmas, érzékeny adataihoz, az állami, a politikai és gazdasági szféra védett, esetleg minősített adataihoz, továbbá a társadalom kiemelt információs infrastruktúráihoz férhetnek hozzá, melyek felhasználásával komoly károkat okozhatnak, ezért irányukba – prognosztizált romlottságuk okán – a kiberterroristák részéről fokozott érdeklődés várható.

Az érintettek jogellenes tevékenységének elhárítása, akadályozása, illetve a már végrehajtott cselekmények elkövetőinek azonosítása érdekében szükséges az általuk használt internetes felületek, kommunikációs csatornák azonosítása, ellenőrzése, kapcsolatépítési törekvéseik felderítése, virtuális személyiségek megalkotása révén beépülés a csoportokba, valamint már azonosított kiberterroristák, hackerek együttműködésbe történő bevonása.

- Felsőoktatási intézmények lehetőségeinek kiaknázása

  A felsőoktatási intézmények a legelsők között kerülnek kapcsolatba az új technológiákkal, technikákkal, mivel ezek az intézmények egyrészt fejlesztésekkel kapcsolatos kutatásokat végeznek, másrészt pedig egy széleskörű szakismereti rendszer koncentrációjaként az új technológiák fejlesztésére, használatára képes szakembereket oktatnak. Ennek okán pedig azonnal értesülnek az információs infrastruktúrákra fenyegetést jelentő új körülményekről.

Nem hanyagolható el továbbá az a körülmény sem, hogy az eddigi tapasztalatok szerint az információs rendszereket ért sikeres, vagy épp sikertelen támadások jelentős része a felsőoktatási intézmények hallgatóinak – ritkább esetben pedig oktatóinak – köréből kerülnek ki, akik a frissen szerzett ismereteiket „élesben" tesztelhetik, ezért az irányukba kiépített humánforrás-kontingens érdemi információkat szolgáltathat az információs infrastruktúrák védelme során.

Egyrészt a fentiekből, másrészt pedig abból, hogy a terrorizmus általánosságban megpróbál a fiatalok körében ideológiát terjeszteni, illetve támogatókat gyűjteni,

következik, hogy a kiberterrorizmus fokozottan veszélyezteti a műszaki, ezen belül az információs technológiákkal foglalkozó intézmények hallgatóit, így akár fizikai, akár kiberkörnyezetükben a kiberterroristák felbukkanhatnak.

- Az információtechnológia területén működő egyéb cégek lehetőségeinek felhasználása

  Az infokommunikációs szférában számos támogató infrastruktúrát üzemeltető gazdasági társaság működik, amelyeknél a humánerőforrásokkal kapcsolatos lehetőségek megegyezhetnek a felsőoktatásban vázoltakkal, azonban az általuk nyújtott szolgáltatások miatt külön figyelmet érdemelhetnek, mivel ezen szereplők megbízható és stabil szolgáltatása (például tanúsítvány szolgáltatók, szoftverfejlesztők, rendszertervezők, stb.) elengedhetetlenül fontos ahhoz, hogy a más szolgáltatók, infrastruktúrák működése zavartalan legyen.

  Továbbá léteznek olyan vállalkozások is, melyek szolgáltatásai alkalmasak lehetnek arra, hogy esetlegesen jogellenes cselekményeket leplezzenek, ezáltal az elkövetők ne legyenek felderíthetők (szerverfarmok, proxy szolgáltatások), ezért e vállalkozások, illetve munkavállalóik fokozottan ki vannak téve a kiberterroristák érdeklődésének, kapcsolatépítési törekvéseinek, és szokatlan, életszerűtlen, vagy rendkívüli körülmények felbukkanása esetén jelzésekkel élhetnek a biztonsági szervek irányába.

- A nyílt információk hasznosítása

  A nyílt információs csatornák folyamatos monitorozásával információk szerezhetőek be a kiberterrorizmus támogató és logisztikai módszereiről, azok irányairól, illetve az esetleges elhárító jellegű tevékenység hatékonyságáról, valamint ennek hatására a módszerekben bekövetkező változásokról. A különböző internetes felületeken (mind a kiberterroristák, mind pedig a jóhiszemű szakértők) rendszeresen publikálnak olyan technológiai újításokról, új fenyegetésekről, a különböző infrastruktúrákat különböző módon ért támadásokról, melyeket hatékonyan fel lehet használni a védendő információs rendszer megóvása során, ugyanakkor az elkövetői körről, illetve azok céljairól, terveiről is lehet következtetéseket levonni.

  A védelem szempontjából pedig a nyílt információs rendszerek adatainak folyamatos nyomon követésével az elhárító jellegű tevékenység – főleg a

prevenció tekintetében – eredményesen kiegészíthető, mivel ezeken a csatornákon számos olyan információ megtalálható, fellelhető, amelyek az adott információs infrastruktúra védelme során felhasználhatók.

Az információs társadalom interneten szerveződő közösségeinek online és nyílt kapcsolattartásainak figyelemmel kísérésével, olyan szakértő személyek felkutatása is lehetővé válik, akik támogathatják a védelmi feladatokat.

V. 3. Összegzés, következtetések

A korábbi fejezetekben tárgyaltak alapján jól látszik, hogy a kibertámadások típusai mennyire sokrétűek lehetnek, illetve a kiberterrorizmusban érintett elkövetők motivációi és céljai is alapjaiban különbözhetnek egymástól, ezért ezekre a körülményekre mind a megelőző, mind pedig az védekező-elhárító tevékenység során kiemelt figyelmet szükséges fordítani.

Az információs infrastruktúrák komplex információbiztonsága, illetve ennek megvalósítása rendkívül összetett feladat, mivel az egyenszilárdságú rendszer kialakítása során különböző – például költségvetési, jogszabályi, technológiai, politikai – okokból kifolyólag számos, az elérni kívánt eredmény ellen ható kompromisszumot kell kötni, ami az ideális, biztonságos állapottól eltérő végeredményt hoz.

Az információbiztonság szakterületeit általában külön-külön tárgyalják, azonban köztük oly mértékű interdependencia áll fenn, ami elengedhetetlenné teszi azt, hogy a védelmi stratégia kialakítása során együtt, lépésről-lépésre építkezzenek a szakterületek, folyamatosan vizsgálva és elemezve azt, hogy a szakterületek lépései milyen pozitív és negatív hatásokat indukálnak más területeken. A védelmi rendszerek üzemeltetése során pedig folyamatosan – még ha szervezeten belül is, de az adott alrendszer üzemeltetőitől függetlenül – ellenőrizni kell, hogy a technológiai színvonal, a személyi és a fizikai biztonság, illetve a rendkívüli események megjelenésekor a reagálási képesség eléri-e a kívánt szintet.

Ugyanakkor az információs infrastruktúrák tekintetében azonosítani kell az olyan funkciókat, vagy paramétereket, melyek a globális működés szempontjából nem fontosak, ezért a védelmükre aránytalanul nagy erőforrások fordítása nem indokolt, mivel itt egy kibertámadás kárt, presztízsveszteséget nem okoz. Például míg egy rendészeti célú kommunikációs infrastruktúrában az elemek közötti összeköttetés akadályozása azonnal jelentkező problémát jelent, addig egy kontinentális lemezek elmozdulását mérő geológiai rendeltetésű hálózatban

ez akár hónapokig sem okoz jelentős fennakadást, így e rendszerek védelmét jelentősen más szempontok alapján dolgozzák ki.

Az információs infrastruktúrák ellen indított és napvilágra került támadások publikus adatainak elemzését követően levonható az a következtetés, hogy a kiberterroristák érzékenyebb támadásokat intézhetnek, ha nem egy védelmi szakterület gyengeségét használják ki, hanem olyan biztonsági réseket találnak, mely több szakterület gyengeségének kölcsönhatásából ered. Például egy sértett alkalmazott (személyi biztonság) sérülékenységekre vonatkozó információk átadásával (dokumentumbiztonság), különleges helyzetek megteremtésével (fizikai biztonság), eszközök telepítésével (elektronikus információbiztonság) segíti az eredményes támadás megvalósulását. E jelenség rávilágít arra is, hogy a komplex információbiztonság szakterületeinek kölcsönös függőségét a védelmi stratégia tervezése és kialakítása során mindenképpen figyelembe kell venni.

Az információs infrastruktúrák védelme az információs társadalomban mind a magánszektorra, mind az államra újszerű feladatokat ró. Az államnak, az érintett információs infrastruktúrák általa is igénybe vett szolgáltatásai miatt jól felfogott érdeke és egyben kötelessége is valamilyen módon hozzájárulni az érintett rendszerek biztonságának megteremtéséhez. Egy államnak nem minden esetben van közvetlen felügyeleti lehetősége a közigazgatási, a nemzetgazdasági, a társadalmi, illetve a védelmi folyamatok kiszolgálását biztosító rendszerek felett, azonban a védelmet nem bízhatja teljes mértékben az érintett üzemeltetőkre, gazdasági társaságokra. Tekintettel arra, hogy – mint ahogy erre már utaltam – az információs infrastruktúrák működésére hatással bíró tulajdonosok érdekei, a piacgazdaságból adódó nyomások, valamint ezek tükrében meghozott kompromisszumok nem kívánt módon befolyásolhatják az üzembiztonságot, valamint a rendszerben kezelt – az állam számára is fontos – adatok sérthetetlenségét.
Fentiek alapján szükséges olyan új módszerek metódusok kidolgozása, bevezetése – melyre példa az aszimmetria vizsgálat, illetve a működési és biztonsági interdependencia térkép – melyek alkalmasak arra, hogy eddig nem észlelt kockázatokat azonosítsák, és megteremtsék a megelőzés lehetőségét.

Hazánkban a rendszerváltás óta az információ infrastruktúrákat magánkézben lévő gazdasági társaságok birtokolják és üzemeltetik, azonban az elmúlt időszakban a kritikus rendszerek tekintetében – a közvetlen állami befolyásolás, irányítás érdekében – egyfajta

visszarendeződés figyelhető meg (például EDR, NTG állami tulajdonba kerülése), mely világszinten érzékelhető tendencia.

Az államnak jogában áll olyan követelményrendszereket, szabványokat felállítani, jogszabályokat alkotni, melyek hozzájárulhatnak az információs infrastruktúrák kívánt biztonsági szintjének eléréséhez. Az adatvédelmi, az engedélyezés ügyi, a felügyeleti, a rendészeti és a nemzetbiztonsági szervek révén pedig lehetősége is van arra, hogy az általa támasztott követelmények megvalósulását, a jogszabályok betartását ellenőrizze, továbbá az üzemeltetők részéről az esetlegesen feltárt hiányosságokat, vagy épp a rendszert támadók cselekményeit szankcionálja.

A fentiek mellett a jogalkotás területével szemben követelményként kell támasztani, hogy vegye figyelembe az adott kor technológiai fejlettségét, a prognosztizálható trendeket, az új társadalmi jelenségeket és a különböző folyamatok szabályozásánál – a jogellenes cselekmények megvalósítását segítő, illetve a védelmet akadályozó aszimmetrikus jelenségek elkerülése érdekében – az életszerűségre és a hatékonyságra kell, hogy törekedjen.

Összegzett következtetések

A terrorizmusnak, mint jelenségnek a tanulmányozásakor levonható az a következtetés, hogy annak metodikája, célkitűzése kialakulása óta alapvetően nem változott. Az adott ideológia nevében, céltalanul, véletlenszerűen alkalmazott erőszak révén mindig is bizonyos társadalmi csoportok elnyomása, félelemben, bizonytalanságban tartása és a csoport tagjainak fizikai pusztítása volt a célja, mely alapvető cél az idők során mit sem változott, így ez a megállapítás a jelenkorra is igaz. Azonban a jelenségben egy momentum folyamatosan, korszakról-korszakra fejlődött, mégpedig az alkalmazott eszközökben, mivel az adott kor vívmányai, technológiai színvonala, tudományos eredményei mindig visszatükröződtek, illetve eszköztárában a mindenkori csúcstechnika – feltalálásukat, kifejlesztésüket követően – rövidesen megjelent.

Az információs folyamatok fejlődésével, illetve ezeket a folyamatokat befogadó, támogató, egyre modernebb és hatékonyabb infrastruktúrák kialakulásával, majd globalizálódásával megszületett a kibertér. Az információs infrastruktúrákban megjelent új technológiák, műszaki megoldások segítették az információs folyamatokat, majd mikor ezek átléptek egy kritikus méretet, köréjük, illetve szolgáltatásaik köré szerveződött a társadalom végtelenül sok funkciója, mely révén így a társadalom megkapta az információs jelzőt. Ennek már nemcsak a fejlődéséhez, de zavarok nélküli működéséhez is elengedhetetlen a kellő mennyiségű információ folyamatos megszerzése, áramlása és rendelkezésre állása.
Fenti megállapításokból ugyanakkor levezethető, hogy a terrorizmus számára – céljainak elérése érdekében – szükségszerű, hogy az információs társadalomban is „gyökeret eresszen”, mind úgy, hogy a terroristák maguk is belépnek, integrálódnak e társadalomba, ki- és felhasználják lehetőségeit, valamint eszközeit, mind pedig úgy is, hogy e társadalom ellen fejtik ki tevékenységüket, hogy megzavarják folyamatait, mely révén elérik alapcéljukat, félelmet és bizonytalanságot gerjesztenek. Tehát a kiberterrorizmusnak, mint a terrorizmus és a kibertér közös halmazának a megjelenése gyakorlatilag a műszaki-technológiai fejlődés törvényszerű velejárója.

Levezethető, hogy a kibertér sajátosságaiból adódóan megkönnyíti azt, hogy az információs társadalom tagjai bizonyos radikalizálódási hajlam és megfelelő hatások mellett kiberterroristává válhassanak. Egyrészt a különböző terrorcsoportok a kibertérben könnyebben fejtik ki propaganda és toborzótevékenységüket, mivel a földrajzi és

államhatárok nem jelentenek akadályt, célcsoportjaik „igényei", valamint szimpatizánsaik elvárásai szerint könnyen tudják üzeneteik tartalmát, illetve a közlés módját differenciálni, ami jelentősen növeli hatékonyságukat, mivel könnyen „egymásra találnak" szimpatizánsaikkal. Másrészt a kibertérben végrehajtott jogellenes cselekmények végrehajtása egyfajta biztonságos burokban – sokszor az „otthon melegében" – történik, ezért az elkövetők fizikálisan meg sem közelítik az áldozatot, nem kerülnek vele kapcsolatba. E körülmény következtében másként – jellemzően nem negatívan élik – meg tettüket az elkövetők, pszichésen nem alakul ki bennük tudat, hogy a cselekményükkel kárt, sérelmet okoznak, másokat veszélybe sodornak, és ez fokozottan igaz, ha cselekményük jogellenes mivoltával, vagy annak következményeivel – tájékozatlanságuk okán – alapvetően nincsenek is tisztában. Harmadrészt az elkövetések eszköze logikai támadások esetében gyakorlatilag az információs társadalom „alapeszköze", a bárki számára hozzáférhető számítógép, míg fizikai hatáson alapuló támadások esetében ezek az eszközök viszonylag könnyen beszerezhetők, átalakíthatók, megalkothatók. Negyedrészt pedig a kibertér számos olyan szolgáltatást és lehetőséget nyújt, mely a terrorcsoportok számára a megkönnyíti kapcsolattartást, tevékenységük finanszírozását, illetve lehetővé teszi számukra konkrét terrortámadások kivitelezését is.
Továbbá a kibertér az anonimizálódásra, a digitális nyomok elrejtésére is kiváló lehetőségeket biztosít, mely egyrészt az elkövetők folyamatos, lebukás nélküli – akár önképzésen alapuló – kísérletezgetését teszi lehetővé, másrészt pedig az „először kipróbálókat" bátorítja a jogellenes cselekményük végrehajtására.

A fentiek tükrében pedig prognosztizálható, hogy a kiberterrorizmus a terrorizmuson belül – az információs társadalom fejlődésével összhangban – egyre nagyobb részt fog kihasítani.

A kiberterrorizmus eszközrendszerét vizsgálva nagy valószínűséggel előjelezhető, hogy a terrorcselekmények, illetve az erre irányuló kísérletek jelentős részét várhatóan a logikai eszközök alkalmazása révén fogják végrehajtani. Ennek oka, hogy a fizikai hatáson alapuló eszközök alkalmazása lényegesen nagyobb szervezést, háttérismeretet, alkalmazhatóságra vonatkozó információt, anyagi ráfordítást és ebből fakadóan pedig jóval nagyobb elköteleződést igényel, mint a logikai eszközök alkalmazása. A kiberterroristák döntő hányada számára a logikai eszközök alkalmazása lényegesen könnyebb, mivel az interneten keresztül a különféle módszerek, leírásai, alkalmazhatósági feltételei, továbbá a különböző sérülékenységekre vonatkozó információk könnyen elérhetőek, illetve maguk a támadókódok

is viszonylag könnyen beszerezhetők (akár toolkit-ek formájában), meglévő, vagy megszerezhető szakismeret birtokában a már rendelkezésre állók átalakíthatók, „testre szabhatóak", de akár meg is alkothatók és többször, vagy párhuzamosan is alkalmazhatóak. Mindezek mellett birtoklásuk és fejlesztésük szinte egyáltalán nem kimutatható, alkalmazásuk megfelelő intézkedések mellett biztonságos, kockázatmentes.

A kiberterroristává válás folyamatának, valamint a fizikai hatáson alapuló és a logikai eszközök metodikájának, képességeinek tanulmányozása által levonható az a következtetés, hogy a széles körben elérhető, vagy megalkotható eszközök révén a kiberterroristák – professzionális eszközök és mélyreható szakismeretek hiányában – jelenleg az információs infrastruktúrákat rendszerszinten nem képesek veszélyeztetni. Ugyanakkor lokálisan, vagy bizonyos alrendszerek tekintetében képesek érzékelhető, kimutatható zavarokat és viszonylag nagy kárt is okozni, melyek – bár médiaérdeklődésre számot tartanak – az információs társadalom globális folyamatait nem zökkentik medrükből, mindannak ellenére sem, hogy a társadalom egyes entitásait a támadás anyagilag, érzelmileg érzékenyen érintheti.
A fenti állítás – miszerint a kiberterroristák rendszerszinten nem veszélyeztetik az információs társadalmat – az elmúlt időszakban globális szinten problémát okozó kibertámadások („Petya", „WannaCry" és különböző verzióik) tükrében is megállja a helyét, mivel felmerült annak – természetesen nem ellenőrizhető – gyanúja, hogy ezek a támadókódok sikeresen támadott állami szervektől eltulajdonított, onnan kikerült professzionális kiberfegyverek adaptációi, melyeket a „felsőkaszthoz" tartozó hackerek pénzszerzés érdekében „testre szabtak".

Az okozott kár, illetve zavar azonban jelentősen növelhető, ha a kiberterroristák találnak olyan biztonsági réseket, aszimmetriákat és interdependencia kapcsolatokat, melyekről az üzemeltetők, illetve az incidensben érintettek (például rendészeti szervek, üzleti partnerek) nem tudtak, illetve nem kezeltek.
Az előzőekből levonható az a következtetés, hogy az aszimmetria jelensége, illetve annak különböző dimenziói az információs infrastruktúrák aktív és passzív védelme, illetve a már bekövetkezetett kibertámadások hatásainak felmérése, elhárítása, a károk enyhítése, valamint az elkövetőik azonosítása terén egyre nagyobb problémát fog jelenteni. Amennyiben a támadók képesek azonosítani a védelem gyengeségeit, az interdependens kapcsolatokat, az aszimmetria potenciális területeit és cselekményeiket ezek figyelembevételével tervezni, akkor rendkívüli mértékben megnehezíthetik az információs infrastruktúrák működését,

védelmét, illetve az ellenük fellépni kívánó hatóságok tevékenységét. Ez pedig rá is világít a komplex, az egyenszilárdságú védelem szükségességére. Az alkalmazott védelmi rendszernek minden, a tervezésekor bekalkulált körülmény megjelenésekor garantálnia kell az információs infrastruktúra szolgáltatásainak folytonosságát, a kezelt információk biztonságát. A védelmi rendszer kiépítése azonban nem csak egy egyszeri feladat, hanem folyamatos monitorozó, információgyűjtő, tervező és fejlesztő tevékenység, mely a biztonság minden dimenzióját kell, hogy érintse.

Tudományos eredmények

A kiberterrorizmus definíciója

A kibertérben végrehajtott, a terrorizmussal összefüggésbe hozható jogellenes tevékenységek, cselekménysorozatok tanulmányozása során megszerzett tapasztalatok, ismeretanyagok összegzését követően megalkottam a kiberterrorizmus definícióját. A definícióban egyesítve jelenik meg az a sajátosság, hogy a kiberterrorizmus az információs infrastruktúrákra egy időben tekint célpontként és a végrehajtás eszközeként.

A kiberterrorizmus módszereinek kategorizálása

A különböző terrorcsoportok kibertérben folytatott tevékenységének, illetve kifejezetten a kiberterrorizmushoz kapcsolódó cselekmények tanulmányozása során megszerzett tudásanyag, valamint a jogi háttér és saját tapasztalatok szintetizálását követően kategorizáltam a kiberterrorizmus módszereit, illetve a kategóriákba tartozó tevékenységeket.

Az aszimmetria vizsgálat

Az információs infrastruktúrák vonatkozásában mind az üzemeltetők, mind pedig a védelmi, rendészeti feladatokban érintett állami szervek számára – működésük hatékonyságának és teljesítőképesség növelése érdekében – aszimmetria vizsgálat lefolytatását javaslom, melynek eredményeképpen napvilágra kerülhetnek olyan momentumok, illetve ezeknek különféle kombinációi, melyek nem várt módon gátolhatják, gyengíthetik a különböző incidensekre, behatásokra adandó válaszok eredményességét.

A működési és biztonsági interdependencia térkép

Az információs infrastruktúrák üzemeltetési és biztonsági körülményeiben rejlő összefüggések, valamint a különböző külső-belső hatások következményeinek feltárása érdekében működési és biztonsági interdependencia térkép bevezetésére teszek javaslatot, melynek célja, hogy mind az infrastruktúrák védelmében közreműködő állami szereplők, mind pedig az üzemeltetők a különböző szakterületeket érintő esetlegesen megjelenő negatív hatások eredőjét a működés, illetve a komplex információbiztonság teljes spektrumában láthassák.

Ajánlások

1. Javaslom a doktori értekezésben összefoglaltakat felhasználni az információs infrastruktúrákhoz, valamint a kiberterrorizmushoz, illetve e szakterületekhez kapcsolódó egyéb egyetemi alap és mesterképzések tananyagaként.

2. Javaslom az értekezés kiberterrorizmus mibenlétét, módszereit és eszközeit tárgyaló részeit a rendészeti és a nemzetbiztonsági szervek e területen foglalkoztatott állományának továbbképzési tananyagaiba beintegrálni.

3. Javaslom az értekezésben megfogalmazott észrevételeket, ajánlásokat felhasználni az információs infrastruktúrák információbiztonsági szakembereinek tanfolyami képzésein, továbbképzésein.

4. Javaslom az értekezés megállapításait az információs infrastruktúrák komplex védelmének tervezésekor, az üzemeltetésre vonatkozó stratégiák megalkotásakor, illetve a jogszabályi feltételek, környezet kialakításakor felhasználni.

Irodalomjegyzék, hivatkozások

1. Frank Webster: Theories of the lnformation Society, by Routledge, Oxon, 1997., ISBN 0-203-96282-6, pp. 8.;
2. Fritz Machlup: The production and distribution of knowledge of United States, Princeton University Press, 1962., ISBN: 06910035641962.;
3. John Goddard: New Technology and the Geography of the UK Information Economy. In Robins, K. (ed) 1992. Understanding Information: Business, Technology and Geography, eh. 11, 178-201. London: Belhaven;
4. Nádasi András: Információtörténelem, Eszterházy Károly Főiskola, Eger, 2011.; pp. 114.;
5. Európai Bizottság - COM(2017) 608 final;
6. UN Manual on the Prevention and Control of Computer Related Crime (ENSZ tanulmány a számítógépes bűnözés megelőzéséről és szabályozásáról);
7. Dr. Dornfeld László, Keleti Arthur, Barsy Miklós, Kilin Józsefné, Berki Gábor, Dr. Pintér István: Műhelymunkák, A virtuális tér geopolitikája, Geopolitikai Közhasznú Alapítvány, ISBN 978-963-9816-36-7, pp. 313.;
8. Haig Zsolt, Várhegyi István: A cybertér és a cyberhadviselés értelmezése, Hadtudomány, Hadtudományi Társaság, Budapest, 2008., ISSN 1215-4121, pp. 2.;
9. Dr. Szenteleki Károly, Rózsa Tünde: Információs rendszerek, Debrecen, 2007., ISBN 978-963-973-267-4; pp. 22.;
10. Huszár Zsuzsanna: Info-kommunikációs technológiák, Pécsi Tudományegyetem egyetemi jegyzet, Digitális tananyagok, 2006.;
11. Dr. Gyurkó György: Informatikus szakmai ismeretek, Budapesti Gazdasági Főiskola, Budapest, 2011.; pp. 16.;
12. Ujváriné dr. Melich Katalin: A gazdasági informatika alapjai, Perfekt Zrt. 2008., ISBN 978-963-394-734-0;
13. Facskó Ferenc: Informatika Segédlet, Nyugat-magyarországi Egyetem, Sopron 2013., pp. 8.;
14. Papp Zoltán: Az információ támadása annak tulajdonságain keresztül, Hadmérnök VI. Évfolyam 4. szám, 2011., ISSN 1788-1919, pp. 229.;
15. Haig Zsolt, Várhegyi István: Hadviselés az információs hadszíntéren, Zrínyi Kiadó, Budapest, 2008., ISBN 9633273919;

16. Papp Zoltán: Az információ támadása annak tulajdonságain keresztül, Hadmérnök VI. Évfolyam 4. szám, 2011., ISSN 1788-1919, pp. 227.;
17. Váti KHT.: Az infrastruktúra szerepe a területi fejlődésben, a térszerkezet és az infrastruktúra fogalmai;
http://www.terport.hu/webfm_send/295
Letöltve: 2010. május 20.;
18. Critical Foundations: Protecting America's Infrastructures: The Report of President's Commission on Critical Infrastructure Protection, Washington, 1997., https://fas.org/sgp/library/pccip.pdf
Letöltve: 2015. december 1.
19. Európai Unió 2008/114/EK. az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről;
20. Utyenkov, N. A.: Az infrastruktúra, amint a területfejlesztés tényezője, 1972. - In: Kőszegfalvi György, Sikos T. Tamás: Városok és falvak infrastruktúrája, Budapest, 1993.;
21. Reimut Jochimsen: Theorie der Infrastruktur: Grundlagen der marktwirtschaftlichen Entwicklung, Mohr (Siebeck), 1966;
22. Munk Sándor: Információs színtér, információs környezet, információs infrastruktúra, Nemzetvédelmi Egyetemi Közlemények VI.: (2) pp. 133-154.;
23. Forgó Sándor: Médiumismeret, Médiainformatikai Kiadványok, Eszterházy Károly Főiskola, Eger, 2011.;
24. Rubóczki Edit: Biztonságosan a felhőben. A publikus felhők biztonsági kérdései, - Vállalkozásfejlesztés a XXI. században IV. tanulmánykötet, Óbudai Egyetem, 2014., pp. 442.;
25. Várhegyi István, Makkay Imre: Információs korszak, információs háború, biztonságkultúra, OMIKK, Budapest, 2000.;
26. Varga János Péter: Kritikus információs infrastruktúrák értelmezése, Hadmérnök, III. Évfolyam 2. szám, 2008., ISSN 1788-1919, pp. 150.;
27. Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, Doktori értekezés, Budapest, 2007., pp. 21.;
28. Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM (2005.) 576 final;

29. Az Európai Parlament és a Tanács (eu) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről;
30. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről;
31. A Bizottság közleménye - A létfontosságú infrastruktúrák védelmére vonatkozó európai programról, COM/2006/0786 final;
32. Papp Zoltán, Pándi Erik, Töreki Ákos: A fenyegetettség egyes aspektusai az információs infrastruktúrák tekintetében, Kommunikáció 2009., ZMNE, Budapest, 2009., pp. 159.;
33. Fehér Krisztián: Kezdő hackerek kézikönyve, avagy informatikai támadások és kivédésük, BBS-INFO Kiadó, Budapest, 2016., ISBN 978-615-5477-44-7;
34. Kelemen Roland, Pataki Márta: A kibertámadások nemzetközi jogi értékelése, Katonai Jogi és Hadijogi Szemle 3. Évfolyam 1. szám, Magyar Katonai Jogi és Hadijogi Társaság, 2015., ISSN 2064-4558:56;
35. Haig Zsolt, Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák, ZMNE, 2012.;
36. Krasznay Csaba: A magyar elektronikus közigazgatási alkalmazások információbiztonsági megoldásai, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, (2011. november);
37. Dr. Nagy Zoltán András: Bűncselekmények számítógépes környezetben, Ad Librum, Budapest, 2009., ISBN 978-963-9888-92-0, pp. 34.;
38. Erdősi Péter: Az üzleti hírszerzés és az ipari kémkedés, Budapesti Műszaki és Gazdaságtudományi Egyetem, 2005., pp. 3.;
39. Kovács László: Az információs terrorizmus eszköztára, Hadmérnök, Robothadviselés 6. Tudományos Szakmai Konferencia, 2006., ISSN 1788-1919;
40. Schutzbach Mártonné: Az informatikai rendszerek biztonságának kockázatelemzése a védelmi szférában, doktori értekezés, ZMNE, Budapest, 2004., pp. 83.;
41. Tálas Péter: A terrorizmus anatómiája, Zrínyi Kiadó 2006., ISBN 963-327-412-5;
42. Charles Townshend: A terrorizmus – Magyar Világ Kiadó, Budapest, 2003., ISBN 963907523;
43. Pongrácz Alex: A politika folytatása más eszközökkel? Avagy gondolatok az állam és az erőszak kérdésköréről, Államtudományi műhelytanulmányok, Nemzeti Közszolgálati Egyetem, Budapest, 2017. évi 17. szám, pp. 5.;

44. U. S. Code of Federal Regulations - 28 C.F.R. Section 0.85;
45. U. S. Code of Federal Regulations – Title 18 Part I. Chapter 113B § 2331.;
46. A Európai Tanács 2002/475/IB. számú kerethatározata a terrorizmus elleni küzdelemről - 1. cikkely;
47. A 2012. évi C. törvény a Magyar Büntetőtörvénykönyvről;
48. Dr. habil. Krajnc Zoltán: Az aszimmetrikus hadviselés, fenyegetés alapkérdései; Repüléstudományi Közlemények, 2008. évi Különszám, Repüléstudományi Konferencia 2008. április 11.;
49. Tomolya János, Padányi József: A terrorizmus és a gerilla-hadviselés azonosságai és különbségei, Az MHTT 2013. évi pályázatára benyújtott közlemény, pp. 134.;
50. Sárkány István: A terrorizmus jelene és jövője, Hadtudományi Társaság, Hadtudományi Szemle 2015/1-2., (2015.), ISSN 1215-4121, pp. 144.,
51. NATO Tükör 16, 2001/2002. Tél, pp. 13.;
52. Gabriel Weimann: Terrorism in CyberSpace: Next Generation, Columbia University Press, 2015, ISBN 9780231801362, pp. 267.;
53. Nazura Abdul Manap and Pardis Moslemzadeh Tehrani: Cyber Terrorism: Issues in Its Interpretation and Enforcement, International Journal of Information and Electronics Engineering, Vol. 2, No. 3, May 2012, pp. 410.;
54. https://www.rsaconference.com/writable/presentations/file_upload/tv-w11-the-future-of-cyberterrorism.pdf
Letöltve: 2018. április 26.;
55. Dr. Resperger István – Biztonsági kihívások, kockázatok, fenyegetések és ezek hatásai Magyarországra 2030-ig, Felderítő Szemle, 2013. 3. szám, ISSN 1588-242X, pp. 34.;
56. Istanovszki László: A szervezett bűnözés elleni harc új stratégiája és taktikája, Hadtudomány 2015/1-2, Hadtudományi Társaság, Budapest, 2015., ISSN 1215-4121, pp. 139.;
57. Dr. Balogh Zsolt György: Jogi informatika, Dialog Campus Kiadó, Budapest-Pécs, 1998., pp. 264-265.;
58. Vályi Gábor: Szocializációs szintér, a család, Nemzeti Szakképzési és Felnőttképzési Intézet, Budapest, 2008., pp. 5.;
59. Szegediné Lengyel Piroska: Számítógépes bűnözés, avagy fiatalok a cyber-térben, Hadmérnök V. Évfolyam 2. szám, ZMNE, 2010., pp, 375.;
60. Dr. Csúri András: A fiatal felnőttkor, mint büntetőjogilag releváns életszakasz, doktori értekezés, Szegedi Tudományegyetem, Szeged, 2008.;

61. Istvánffy András: A terrorizmus, mint rituális kommunikáció, Beszélő Online 10. évfolyam, 8. szám, 2005., ISSN: 1588-0125, http://beszelo.c3.hu/cikkek/a-terrorizmus-mint-ritualis-kommunikacio,
Letöltve: 2016. október 10.;
62. Dr. Komor Levente: Személyes vezetés, Szent István Egyetem egyetemi jegyzet, Gödöllő, 2011., pp. 43.;
63. Guido Steinberg: Jihadismus und Internet: Eine deutsche Perspektive, https://www.swp-berlin.org/fileadmin/contents/products/studien/2012_S23_sbg.pdf
Letöltve: 2018. március 10.;
64. Khalid Sultan: The „ISIS" Online Media War: A Construction of Ideology through Terrorism; Pakistan Journal Peace & Conflict Studies, Vol.1, No.2., 2016., pp.8.;
65. Imran Awan: Cyber-Extremism: ISIS and the Power of Social Media, Social Science and Public Policy; DOI 10.1007/s12115-017-0114-0 Soc (2017) 54, pp. 138-149;
66. Luna Shamieh, Zoltán Szenes: The Propaganda of ISIS/DAESH through the Virtual Space - DATR, 2015., 7(1):7-31, 30 April 2015., pp. 16-17.;
67. Shehabat, Ahmad; Mitew, Teodor; and Alzoubi, Yahia. "Encrypted Jihad: Investigating the Role of Telegram App in Lone Wolf Attacks in the West." Journal of Strategic Security 10, no. 3, 2017., pp. 27-53.;
68. Chayanin Kengsuwan: Legal measures for phishing offense, Faculty of Law Thammasat University, 2012., pp. 5.;
69. Ralph van Uden: A cég pénzét ma előbb lopja el az igazgató, mint egy bankrabló, Deloitte, 2009.,
http://hvg.hu/gazdasag/20090629_csalas_gazdasagi_bunozes_uj_tendenciak
Letöltve: 2017. április 20.;
70. Trend Micro Incorporated Research Paper 2012 Russian Underground 101, pp. 8., http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf
Letöltve: 2017. december 1.
71. FBI: U.S. Leads Multi-National Action Against GameOver Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator
https://www.fbi.gov/news/pressrel/press-releases/u.s.-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware-charges-botnet-administrator,

Letöltve: 2016. november 13.;

72. Dan Turkel: Victims paid more than $24 million to ransomware criminals in 2015 - and that's just the beginning
http://www.businessinsider.com/doj-and-dhs-ransomware-attacks-government-2016-4
Letöltve: 2017. január 20.;
73. FBI: Incidents of Ransomware ont he Rise,
https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise
Letöltve: 2017. augusztus 11.
74. Mark Maremont, Christopher S. Stewart: FBI Says ISIS Used eBay to Send Terror Cash to U.S.
https://www.wsj.com/articles/fbi-says-isis-used-ebay-to-send-terror-cash-to-u-s-1502410868,
Letöltve 2018. 04. 12.;
75. http://mandiner.hu/cikk/20131209_wowozik_megfigyelhettek,
Letöltve: 2015. március 12.;
76. Istvánffy András: A terrorizmus, mint rituális kommunikáció, Beszélő Online 10. évfolyam, 8. szám, 2005.,
http://beszelo.c3.hu/cikkek/a-terrorizmus-mint-ritualis-kommunikacio
Letöltve: 2016. október 10.
77. Király Zoé Adrienn: A terrorizmus médiainterpretációja és a terrorista szervezetek médiahasználatának változása a digitális korban,
http://epa.oszk.hu/02600/02692/00003/pdf/EPA02692_politanulmanyok_2016_12-20.pdf
Letöltve: 2018. január 22.
78. Beraczkai Antal: A nemzetközi terrorizmus elleni harcban résztvevő szövetséges és magyar katonai biztonsági erők felkészítése és műveleti tevékenysége, Doktori értekezés, ZMNE, Budapest, 2009., pp. 38.;
79. Liz Sly, Dan Lamothe, Craig Timberg: U.S. military reviewing its rules after fitness trackers exposed sensitive data
https://www.washingtonpost.com/world/the-us-military-reviews-its-rules-as-new-details-of-us-soldiers-and-bases-emerge/2018/01/29/6310d518-050f-11e8-aa61-f3391373867e_story.html?utm_term=.2d45b14f27a0
Letöltve 2018. január 30.

80. Scott Shane: The Fake Americans Russia Created to Influence the Election, The New York Times, 2017.,
https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html
Letöltve: 2017. október 29.
81. Kelemen Roland, Pataki Márta: A kibertámadások nemzetközi jogi értékelése, Katonai Jogi és Hadijogi Szemle 3. Évfolyam 1. szám, Magyar Katonai Jogi és Hadijogi Társaság, 2015., ISSN 2064-4558. pp. 69.;
82. Alexander Dinger, Ulrich Kraetzer: Waffenfotos auf Amris Handy blieben unentdeckt, Berliner Morgenpost, Berliner, 2017.,
https://www.morgenpost.de/berlin/article212670829/Panne-Polizei-wertete-Amris-Handy-mit-Waffenfotos-nicht-aus.html
Letöltve: 2017. december 28.;
83. Zachary Cohen: New audio adds to mystery of attacks on US diplomats, CNN, 2017., https://edition.cnn.com/2017/10/13/politics/cuba-us-diplomats-acoustic-weapons/index.html,
Letöltve: 2018. január 21.
84. Haig Zsolt: Információs társadalmat fenyegető információalapú veszélyforrások. Hadtudomány, XVII. évf. 3. sz., 2007., ISSN 1215-4121;
85. Franz-Stefan Gady: Japan's largest company is ISIS' Car maker of Choice
https://kep.cdn.index.hu/1/0/644/6441/64415/6441572_4a328cd8dbf92e3b2621989a5b9025d9_wm.jpg
Letöltve: 2016. február 25.;
86. https://thediplomat.com/wp-content/uploads/2015/10/thediplomat_2015-10-08_10-11-39-386x289.jpg
Letöltve: 2017. március 2.;
87. MH Összhaderőnemi Elektronikai Hadviselési Doktrína, MH DSZOFT Kód: 11222. HM HVK Felderítő Csoportfőnökség kiadványa, 2005., pp. 6-8.
88. Haig Zsolt, Várhegyi István: A cybertér és a cyberhadviselés értelmezése, Hadtudomány, Hadtudományi Társaság, Budapest, 2008., ISSN 1215-4121, http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf
Letöltés: 2009. 04. 22.;
89. Haig Zsolt, Kovács László, Ványa László, Vass Sándor: Elektronikai hadviselés, Nemzeti Közszolgálati Egyetem, Budapest, 2014., ISBN 978-615-5305-87-0;

90. Bartha Tibor: A nem halálos fegyverek és alkalmazásuk lehetőségei az MH nem háborús műveleteiben, Doktori értekezés, ZMNE, Budapest, 2005., pp. 60.;
91. Csuka Antal, Előházi János: Irányított energiájú fegyverek és veszélyeik a számítógépes rendszerekre, Hadmérnök III. Évfolyam 3. szám., Budapest, 2008., ISSN 1788-191986;
92. Dr. Kovács Tibor: A terroristák láthatatlan fegyverei, ZMNE Terrorizmus Konferencia, Budapest, 2006.;
93. http://www.amazing1.com/emp.htm
Letöltve: 2015. április 12.;
94. www.fegyverlabor.hu
Letöltve: 2014. június 3.;
95. https://www.researchgate.net/figure/Schematic-diagram-of-Marx-generator-used-in-this-work_fig1_259081390,
Letöltve: 2017. november 3.;
96. Szatmári S., Gogolák Z., Szabó G., Ketskeméty I.: Magyar szabadalom No.192928: "Kapcsolási elrendezés nagyáramú, nagyfeszültségű elektronikus kapcsolóelem kialakítására.", 1985.;
97. Ványa László: Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre, Doktori értekezés, ZMNE, Budapest, 2001.;
98. Carlo Kopp: The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction, https://www.globalsecurity.org/military/library/report/1996/apjemp.htm
Letöltve: 2015. március 2.
99. Haig Zsolt: Számítógép-hálózati hadviselés rendszere az információs műveletekben. In: Bolyai Szemle, ISSN: 1416-1443, 15/1., 2006., pp. 54-73.;
100. Becz T., Martos B., Pásztor Sz., Rigó E., Tiszai T., Tóth B.: Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai, IHM-MTA SZTAKI, Budapest, 2004.;
101. Kerecsendi András: Hálózatbiztonság, Eszterházy Károly Főiskola, Kézirat, Eger, 2013., pp. 90.;
102. Victor Velasco: Introduction to IP Spoofing, InfoSec Reading Room, SANS Institute, 2003.,
https://www.sans.org/reading-room/whitepapers/threats/introduction-ip-spoofing-959
Letöltve: 2011. november 20.;

103. Sooel Son and Vitaly Shmatikov: The Hitchhiker's Guide to DNS Cache Poisoning, The University of Texas at Austin,
https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf
Letöltve: 2017. szeptember 8.
104. Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II., Hadmérnök VIII. Évfolyam 3. szám, 2013., pp. 201.;
105. Bakacsi Géza, Csákány Béla: Egy szegedi néptanító emlékezete Ponticulus Hungaricus XIV. évfolyam 7-8. szám, 2010.
http://members.iif.hu/visontay/ponticulus/rovatok/limes/gaspar_dezso_elete.html
Letöltve: 2014. március 16.;
106. Neumann János: Az önmagát reprodukáló automata elmélete (Theory of Self-Reproducing Automata) 1966 University of Illinois Press Urbana and London
http://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf
Letöltve: 2015. január 16.;
107. Gyebrovszki András: Folyamatos fenyegetés a kibertérben, Hadmérnök, IX. Évfolyam 3. szám, ZMNE, Budapest, 2014., pp. 138.;
108. Trojan Horses, PH066-Skoudis.book, 2003., pp. 251.
https://cdn.ttgtmedia.com/searchSecurity/downloads/Malware_Ch06.pdf
Letöltve: 2015. október 11.;
109. Scott Hobbs: Cyber Threats: Viruses, Worms, Trojans, and DoS Attacks, Global Information Assurance Certification Paper, SANS Institute, 2000.;
110. Fleiner Rita: SQL injekcióra épülő támadások és védekezési lehetőségek, Hadmérnök III. Évfolyam 4. szám, ZMNE, 2008., ISSN 1788-1919, pp. 119.
111. Keith J. Gomes: Distributed Denial-of-Service (DDoS), Cybersecurity Cyber-Attack Series, xahive, 2016;
112. Gyányi Sándor: DDOS támadások veszélyei és az ellenük való védekezés, Hadmérnök, 2007., ISSN 1788-1919;
113. Szabó István: Tűzfalszabályok felderítése, Híradástechnika,
www.hiradastechnika.hu/data/upload/file/2006/2006_5/HT_0605-3.pdf
Letöltve: 2013. május 9.;
114. Tom Palmaers: Implementing a vulnerability management process, InfoSec Reading Room, SANS Institute, 2013.;

115. Dr. Haig Zsolt, Hajnal Béla, Dr. Kovács László, Dr. Muha Lajos, Sik Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana, ENO Avisory Kft., 2009., pp. 71.,
116. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról;
117. Schutzbach Mártonné: Az informatikai biztonságot fenyegető tényezők, http://portal.zmne.hu/download/konyvtar/digitgy/nek/2003_2/12_schutzbach.pdf Letöltve: 2014. 02. 03. pp. 128.;
118. Horváth László: Az információbiztonság nemcsak informatikai biztonság, http://aam.hu/ftp/az_infobizt_nemcsak_2005_oktober_1.pdf Letöltve: 2014. 02. 06.
119. Dr. Haig Zsolt: Az információbiztonság komplex értelmezése, Hadmérnök - Robothadviselés 6. Tudományos Szakmai Konferencia, Különszám, 2006., ISSN 1788-1919;
120. Kuris Zoltán: A komplex információvédelem új irányai a nemzeti minősített adatok védelmével összefüggésben, Hadmérnök V. Évfolyam 4. szám, 2010., ISSN 1788-1919, pp. 189.;
121. Kun Gergő, Pándi Erik: Fizikai biztonság megvalósítása egy nemzeti minősített adatkezelést végző katonai szerv esetében, Hírvillám, V. Évfolyam 1. szám, Budapest, 2014., ISSN 2061- 9499, pp. 79-91.;
122. Kerti András: Átviteli út biztonság, Hadmérnök, II. Évfolyam 4. szám, 2007., ISSN 1788-1919, pp. 60.;
123. Muha Lajos, Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Nemzeti Közszolgálati Egyetem, 2014, ISBN 978-615-5491-65-8, pp. 31.;
124. László Zsuzsanna: Rejtjelbiztonság, Hadmérnök, IV. Évfolyam 2. szám, 2009., ISSN 1788-1919, pp. 380.;
125. 43/1994. (III. 29.) számú Kormányrendelet a rejtjeltevékenységről;
126. Kassai Károly: A Magyar Honvédség információvédelmének – mint a biztonság részének – feladatrendszere, Doktori értekezés, ZMNE, Budapest, 2007.; pp. 50-51.;
127. Isaszegi János: Az aszimmetrikus hadviselés kialakulásának története, Hadtudomány 2015/1-2., Hadtudományi Társaság, Budapest, (2015.), ISSN 1588-0605, pp. 76.
128. Magyarósi Csaba: Behívja a feltört iPhone-okat a T-Mobile https://index.hu/tech/mobil/2009/08/07/behivja_a_feltort_iphone-okat_a_t-mobile/

Letöltve: 2015. február 4.;

129. Zs. Horváth, I. Kocsis: A CRAMM módszer alkalmazásának kiterjesztése: Proceedings of 8th International Engineering Symposium at Bánki, ISBN: 978-615-5460-95-1, 2016, pp. 16.;
130. Dr. Munk Sándor: A kritikus infrastruktúrák védelme információs támadások ellen, Hadtudomány, Budapest 2008/1., pp. 100.;
131. Ahmed M. AbdelSalam, Wail S.Elkilani, Khalid M.Amin: An Automated approach for Preventing ARP Spoofing Attack using Static ARP Entries, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014., ISSN 2156-5570;
132. Szabó Tibor: A terroristák modern eszközrendszere, Hadmérnök, X. Évfolyam 2. szám, 2015., ISSN 1788-1919, pp. 270.;

Mellékletek

1. számú melléklet

A különböző aszimmetriák „keveredése”. Azt az esetet vázolja, amikor a kiberterroristák a kommunikációjuk biztonsága érdekében hetente lecserélik eszközeiket, azonosítóikat, melyet a rendészeti szervek megkísérelnek lekövetni:

A kiberterroristák információs ciklusa:

A állapot (új eszközök, SIM-ek, azonosítók, stb.)							**B állapot** (új eszközök, SIM-ek, azonosítók, stb.)							**C állapot** (új eszközök, SIM-ek, azonosítók, stb.)							**D állapot** (új eszközök, SIM-ek, azonosítók, stb.) …					
1. nap	2. nap	3. nap	4. nap	5. nap	6. nap	7. nap	1. nap	2. nap	3. nap	4. nap	5. nap	6. nap	7. nap	1. nap	2. nap	3. nap	4. nap	5. nap	6. nap	7. nap	1. nap	2. nap	3. nap	4. nap	5. nap	6. nap

A rendészeti tevékenység információs ciklusa:

Humán felderítés szakasza	**Technikai adatok gyűjtése**	**Beszerzett adatok ellenőrzése**	**Belső és külső engedélyek beszerzése**	**Probléma észlelése**	**Az információgyűjtési folyamat újraindítása ...**
Információk megszerzése Adatgyűjtés szükségességének észlelése Iratok elkészítése, felterjesztése	Humán forrásból származó információk értékelése Iratok elkészítése, felterjesztése Kapacitások lefoglalása, műveletek egyeztetése Adatgyűjtések végrehajtása	Adatok ellenőrzése Adatári ellenőrzések	Előterjesztések és kísérő iratok elkészítése Iratok belső felterjesztése (engedélyező vezető) Iratok külső felterkesztése (bíró, miniszter)	Nincs információ Ellenőrzési folyamatok Visszatájékoztatás	

Aszimmetrikus pontok:

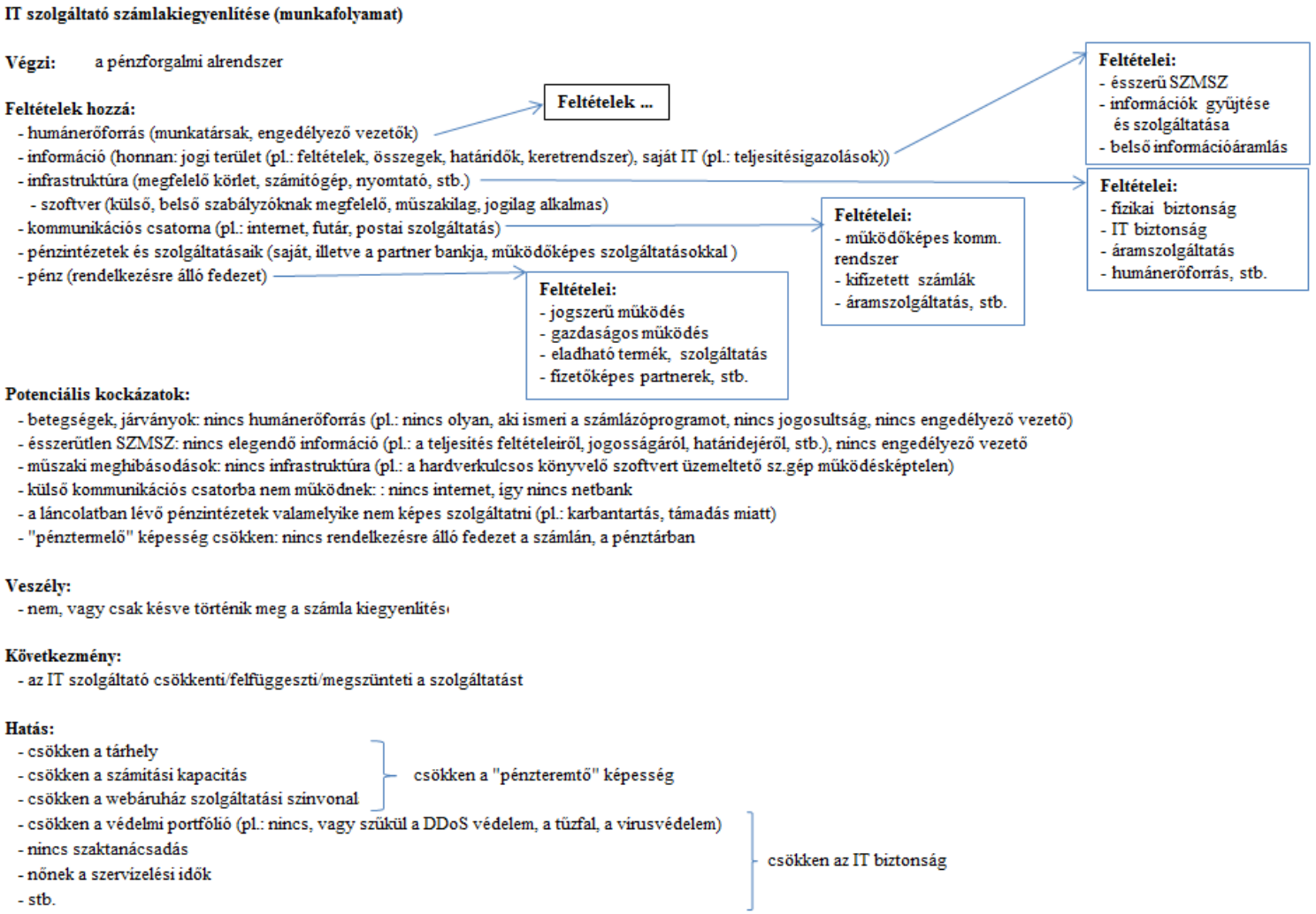
Humánerőforrások megbízhatósága Adatok szintetizálásának ideje Iratokkal kapcsolatos adminisztrációk Költségek	Iratokkal kapcsolatos adminisztrációk Kapacitások rendelkezésre állása Szakemberek képzettsége, rendelkezésre állása Költségek	Adatok szintetizálásának ideje Ellenőrzések adminisztrációja	Iratokkal kapcsolatos adminisztrációk Belső engedélyezési folyamatok menete Külső engedélyezési folyamatok menete Jogi kötelmek, anomáliák Engedélyezési szintek	Ellenőrzési folyamatok Iratok adminisztrációja

Mint látható, a rendészeti ciklus alatt a kiberterroristák négyszer váltottak eszközöket, azonosítókat, akár módszereket, amelyek közül a rendészeti erők legalább két ciklusról nem tudhatnak.

Megjegyzés:
A munkafolyamatok hossza nagyban függ az adott ügy természetétől (a kiberterroristák jelentette fenyegetés mértékétől, az érintettek számától), a rendészeti szerv belső szabályzóitól (szolgálati út hossza, adminisztratív követelmények).

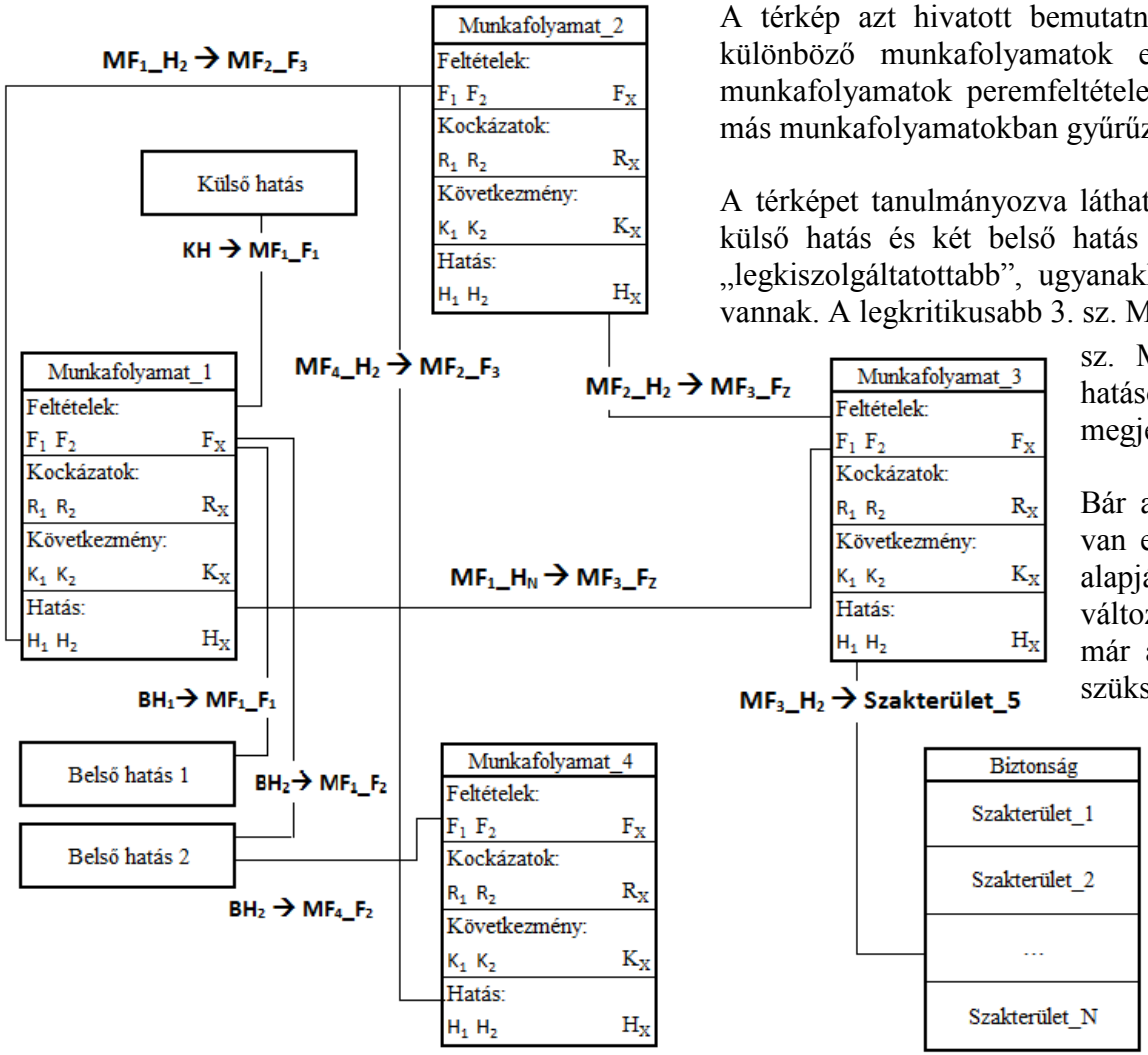
2. számú melléklet

A működési interdependencia térkép egy munkafolyamatra leképezve



3. számú melléklet

A működési és biztonsági interdependencia térkép elve:



A térkép azt hivatott bemutatni, hogy bizonyos külső és belső hatások, valamint a különböző munkafolyamatok esetleges negatív hatásai, miként befolyásolják más munkafolyamatok peremfeltételeit, és érintett munkafolyamatok negatív hatásai milyen más munkafolyamatokban gyűrűznek tovább, és hol válhatnak kritikus szintűvé.

A térképet tanulmányozva látható, hogy az 1. sz. Munkafolyamat peremfeltételeire egy külső hatás és két belső hatás közvetlen befolyással bír, így ez a munkafolyamat a „legkiszolgáltatottabb", ugyanakkor negatív hatásai két másik szakterületre is hatással vannak. A legkritikusabb 3. sz. Munkafolyamat eredményességére közvetlenül az 1. és 2. sz. Munkafolyamatok hatásai, valamint a külső és belső hatások, illetve a 4. sz. Munkafolyamat közvetett hatása megjelenti a veszélyt.

Bár a biztonsági helyzetre csak a 3. sz. Munkafolyamatnak van esetlegesen közvetlen hatása, de a térkép összefüggései alapján monitorozni lehet azokat a hatásokat, illetve azok változását, melyek e területen gyűrűznek be, és szükség esetén már a negatív hatások megjelenése előtt lehet intézkedni a szükséges beavatkozásra.

Rövidítések jegyzéke

Rövidítés	Idegen nyelven	Magyar nyelven
ARP	Address Resolution Protocol	címleképezési / meghatározó protokoll
CBRN	Chemical, Biological, Radiological and Nuclear	vegyi, biológiai, radiológiai és nukleáris
CERT	Computer Emergency Response Team	Számítógépes Vészhelyzetek Elhárításáért Felelős Csoport
CNA	Computer Network Attack	számítógép-hálózati támadás
CND	Computer Network Defence	számítógép-hálózati védelem
CNE	Computer Network Exploitations	számítógép-hálózati felderítés
CPU	Central Processing Unit	központi feldolgozó egység
CRAMM	CCTA Risk Analysis and Management Method	kockázatelemzési és -kezelési módszertan
DDoS	Distributed Denial of Service	elosztott szolgáltatás megtagadás
DNS	Domain Name System	domainnév szolgáltatás
DoS	Denial of Service	szolgáltatás megtagadás
EDR		Egységes Digitális Rádió-távközlő rendszer
EMP	ElectroMagnetic Pulse	elektromágneses impulzus
FBI	Federal Bureau of Investigation	Szövetségi Nyomozó Iroda
FIN	Finish	TCP kapcsolat bontásának kérése
GDP	gross domestic product	bruttó hazai termék
GPS	Global Positioning System	globális helymeghatározó rendszer
GSM	Global System for Mobile Communications	vezeték nélküli kommunikációs rendszer
HOIC	High Orbit Ion Cannon	egy DDoS program fantázianeve
ICMP	Internet Control Message Protocol	Internetes vezérlőüzenet-protokoll
IP	Internet Protocol	Internet Protokoll
ISDN	Integrated Services Digital Network	Integrált Szolgáltatású Digitális Hálózat
LAN	Local Area Network	helyi kiterjedésű hálózat
LOIC	Low Orbit Ion Cannon	egy DDoS program fantázianeve
MAN	Metropolitan Area Network	nagy városi hálózat
Nbtv		Nemzetbiztonsági törvény
NEMP	Nuclear Electromagnetic Pulse	nukleáris eredetű elektromágneses impulzus
NNEMP	Non Nuclear Electromagnetic Pulse	nem nukleáris eredetű elektromágneses impulzus
NSA	National Security Agency	Nemzetbiztonsági Ügynökség
NTG		Nemzeti Távközlési Gerinchálózat
PR	Public Relations	közönségkapcsolatok
Rtv		Rendőrségi törvény

SQL	Structured Query Language	strukturált lekérdezőnyelv
SYN	Synchronous Idle	szinkron üresjárat
TCP	Transport Control Protocol	átvitelvezérlő protokoll
TETRA	Trans European Trunked Radio	európai trönkölt rádió
TOR	The Onion Router	"A Hagyma Elosztó" routerhálózat
UDP	User Datagram Protocol	felhasználóit adatcsomag-protokoll
VPN	Virtual Private Network	virtuális magánhálózat
WAN	Wide Area Network	nagy kiterjedésű hálózat
Wifi	Wireless Fidelity	vezeték nélküli adatátvitel
WWW	World Wide Web	világméretű hálózat

Ábrák jegyzéke

Az értekezés témájában született publikációim

- Papp Zoltán: RFID – Új technológia veszélyei: RFID és az elektronikus útlevél, „Hadmérnök" V. évfolyam 4. szám, 2010. december, - pp 248-254., ISSN 1788-1919
- Papp Zoltán: Irányított energiájú fegyverek veszélyei a kommunikációs hálózatokra, „Hadmérnök" VI. évfolyam 4. szám, 2011. december, - pp 233-238., ISSN 1788-1919
- Papp Zoltán: Az információ támadása annak tulajdonságain keresztül, „Hadmérnök" VI. évfolyam 4. szám, 2011. december, - pp 224-232., ISSN 1788-1919
- Papp Zoltán: A helyzet-meghatározó rendszerek zavarása, „Hadmérnök" VII. évfolyam 1. szám, 2012. március, - pp 214-221., ISSN 1788-1919
- Papp Zoltán: A számítógép-hálózatok tűzfalainak támadása, „Hadmérnök" VII. évfolyam 2. szám, 2012. június, - pp 335-341., ISSN 1788-1919
- Papp Zoltán – Pándi Erik – Kerti András: A számítógép-hálózatok elleni támadások módszertana, „Kommunikáció 2009." nemzetközi szakmai-tudományos konferencia, 2009. október 14., - pp. 143-154. ZMNE Budapest, ISBN 978-963-7060-57-1
- Papp Zoltán – Pándi Erik – Töreki Ákos: A fenyegetettség egyes aspektusai az információs infrastruktúrák tekintetében, „Kommunikáció 2009." nemzetközi szakmai-tudományos konferencia, 2009. október 14., - pp. 155-163., ZMNE Budapest, ISBN 978-963-7060-57-1
- Papp Zoltán: Virtuális magánhálózati kapcsolatok, „Hírvillám" ZMNE Híradó Tanszék Tudományos Szakmai Kiadványa, I. évfolyam 1. szám, 2010. december, - pp 156-162., ZMNE Budapest, ISSN 2061-9499
- Papp Zoltán: RFID – Új technológia veszélyei, „Hírvillám" ZMNE Híradó Tanszék Tudományos Szakmai Kiadványa, I. évfolyam 1. szám, 2010. december, - pp 271-275., ZMNE Budapest, ISSN 2061-9499
- Papp Zoltán – Pándi Erik – Dorkó Zsolt: Információs rendszerek alkalmazási feltételeinek korlátozása, Tanulmány – 2010. – 92 p., ZMNE Egyetemi Könyvtár, Budapest
- Papp Zoltán: Information terrorism, „Hadmérnök" VIII. Évfolyam 4. szám, 2013. december, - pp. 217-222., ISSN 1788-1919
- Papp Zoltán: Professional areas of protection against information terrorism, „Hadmérnök" IX. Évfolyam 3. szám, 2014. szeptember, - pp. 207-213., ISSN 1788-1919

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani mindazoknak, kik támogatásukkal, iránymutatásukkal, a szükséges anyagok rendelkezésemre bocsátásával, tapasztalataik megosztásával és személyes konzultációk lehetőségével segítséget nyújtottak az értekezés elkészítésében.

Külön köszönet témavezetőmnek, Dr. Kovács Lászlónak, aki kezdetektől fogva segítséget nyújtott, támogatta kutatásomat, irányt mutatott a tudományos élet területén, és minden esetben készséggel állt rendelkezésemre érdemi tanácsaival.

Köszönettel tartozom opponenseimnek, Dr. Munk Sándornak és Dr. Rajnai Zoltánnak az értekezéshez kapcsolódóan megfogalmazott számos építő jellegű kritikai észrevételeikért, valamint Dr. Haig Zsoltnak és Dr. Ványa Lászlónak a műhelyvitán elhangzott javaslataikért, mellyel hozzájárultak az értekezés végső formájának kialakulásáért.

Végül hálás vagyok családomnak, akiktől hosszabb - rövidebb időre elszakított a kutatói munkám és az értekezés összeállítására fordított tevékenységem, de ők mindvégig türelemmel támogattak az felkészülésemben.