Kovács László

CYBER TERRORIZMUS

Gondoltak Önök már arra, hogy mi történne akkor, ha nem lenne áram — mondjuk nemcsak néhány óráig —, hanem néhány napig, vagy akár néhány hétig? Erre persze könnyedén azt lehet válaszolni a 21. századi ember magabiztosságával: Micsoda kérdés, kérem! Ilyen egyszerűen nem fordulhat elő! Ez csak a Hollywoodi, nagy fantáziával megáldott forgatókönyvírók képzeletében lehetséges, valami B kategóriás kevésbé sikerült akció vagy katasztrófafilmben. És persze lehet, hogy ez igaz is.

Álljunk meg azonban egy pillanatra, és játszunk el a gondolattal: Tényleg, mi is történne az oly nagyon és oly sokszor felmagasztalt, a mindennapokban már a high-tech eszközöket is készség szinten alkalmazó, az internet lévén — Friedman jelzőjével élve — „kilapított" világunkkal, abban az esetben, ha akadozik, vagy egyáltalán nem működik a villamos-energiaszolgáltatás. Akár csak egy hétig. Vagy csak néhány napig. Rémálom, ami soha nem következhet be? Függetlenül az azt kiváltó okoktól, az elmúlt hónapokban vagy években már láthattunk néhány elég ijesztő példát arra, hogy mit is okoz valójában egy-egy, nemcsak néhány kisebb települést, hanem egész régiókat, vagy akár országokat is érintő áramszünet. Két kiragadott példa a közelmúltból: 2003. augusztusában az Egyesült Államok keleti partvidékének és Kanada egyes területeinek jelentős része maradt áram nélkül napokra. A másik példa időben sokkal közelebbi: 2006. őszén egy Németországban bekövetkezett baleset miatt Nyugat-Európa jelentős részén szünetelt az áramszolgáltatás, szerencsére csak néhány óráig. Természetesen a rendszerek felkészültek egy-egy helyi üzemzavar hosszabb-rövidebb ideig történő áthidalására. Abban azonban nem lehet kétségünk, hogy olyan nagy áramszünetek kezelése, mint amelyeket az előző példákban láthattunk nem egyszerű feladat, és bizony — a probléma nagyságától, az adott műszaki megoldásoktól, illetve földrajzi kiterjedéstől, vagy akár az időjárástól is függően —, akár napokig is eltart, amíg a rendszer, vagy a szolgáltatás működése helyreáll.

Mindez azt támasztja alá, hogy a többi információs infrastruktúrához hasonlóan a villamosenergia-szolgáltatás is rendkívül sérülékeny. Jogos a jelző, amellyel ezeket a sérülékeny, ámde mégis mindennapi életünkben nélkülözhetetlen rendszereket illetjük: *kritikus infrastruktúrák.*

Az eddig elmondottakból rögtön adódik egy sor további kérdés is. Mindjárt az első: kritikus információs infrastruktúráink jelentős része a cyber tér-

ből[1] elérhető, akkor hogyan lehetséges az, hogy ez idáig még csak nem is hallottunk olyan nagy, a cyber térből érkező támadásról, amelynek célpontjai ezek a rendszerek lettek volna?

A kérdés jogos. A válasz azonban nem egyértelmű, hiszen gyakran csak találgatunk, amikor az okokat keressük. Az biztos — hiszen számos bizonyíték áll a rendelkezésünkre, ráadásul olyan bizonyíték, amely nem is valamiféle titkos csatornán kerül hozzánk, hanem mindenki számára látható módon akár az interneten is felfedezhető —, hogy a terrorista szervezetek hasonlóan az átlagemberhez használják, sőt mi több, kihasználják az információtechnológia előnyeit. A terrorista szervezetek ugyanúgy megtalálhatóak a cyber térben, mint a többi 1 milliárd felhasználó. Saját weblapokat üzemeltetnek, ahol tagokat toboroznak, hirdetik az „ügy" fontosságát, végrehajtott akciókat mutatnak akár videó filmekkel is illusztrálva. Használják az internetet kapcsolattartásra, akciók koordinálására, egyeztetésre, pénzadományokat gyűjtenek, és különböző pénzügyi tranzakciókat végeznek. Teszik mindezt anélkül, hogy különösebb kockázatot vállalnának, hiszen a különböző titkosító programok és algoritmusok segítségével még az egymás közötti elektronikus levelezésük is viszonylag rejtett maradhat a titkosszolgálatok előtt.

A felvetett kérdésre adandó választ tovább nehezíti, hogy az elmúlt években az a trend látszik inkább igazolódni, hogy a terrorista szervezetek inkább kihasználják a high-tech[2] nyújtotta előnyöket egy-egy low-tech[3] színvonalú akció végrehajtása érdekében, semmint támadnák azt. Ez egyrészt azt jelenti, hogy az interneten könnyűszerrel találhatnak információt a házilag elkészíthető robbanóanyagokról, amelyet azután egy hagyományos — low-tech — terrorista akcióban használhatnak fel. A másik ok szintén a high-tech-ben keresendő. A high-tech terrorista oldali alkalmazásával szintén sikeresek lehetnek abban, hogy információkat és adatokat szerezzenek arról, hogyan lehet elkerülni akár high-tech akár low-tech akciók végrehajtása során a high-tech ellenőrző, vagy terroristaellenes szolgálatokat, hatóságokat. Az internet valójában egy aranybánya akkor, amikor *adatbányászat* segítségével olyan információk megszerzéséhez juttathatja a terrorista szervezetet, amelyek e nélkül a cyber segítség nélkül csak roppant nagy kockázattal, valamint óriási anyagi és humán erőkkel lennének csak megoldhatók.

---

[1] Cber tér: ezen a fogalmon alapvetően a számítógépes hálózatok hardver és szoftver eszközei által behatárolt virtuális teret értjük.

[2] High-tech: az információtechnológia felhasználásával létrehozott rendkívül fejlett technikai színvonalú eszköz, szolgáltatás, eljárás, megoldási mód

[3] Low-tech: hagyományos vagy átlagos technikai színvonalú eszköz, szolgáltatás, eljárás, megoldási mód

Attól azonban, hogy eddig még nem következett be egy a cyber térből érkező támadás, a veszély még fenn áll. Itt van a mindennapjainkban. Ez a veszély nyugati típusú, jóléti társadalmainkat nagyon komolyan fenyegeti, és pont abból a tényből ered, ami e társadalmak működésének alapja. Ez pedig nem más, mint a már oly sokszor hangsúlyozott függőség azoktól a rendszerektől, amelyek a háttérben, gyakran meglepően láthatatlan módon működtetik azt, amit mi mindennapi életnek nevezünk. Ezek a rendszerek a 21. században azok az *információs infrastruktúrák*, amelyeken keresztül például a már említett villamos energia a lakásainkba, a munkahelyeinkre, a kórházakba, az iskolákba, a gyárakba, és gyakorlatilag életünk minden területére eljut. Természetesen a villamos energia rendszereken kívül számos olyan információs infrastruktúra támogat minket — akár számunkra valóban láthatatlan módon is —, amelyek nélkülözhetetlenek a mindennapjainkhoz. Gondoljunk bele, mi lenne velünk rohanó világunkban közlekedési infrastruktúra nélkül. Mi lenne velünk kommunikációs rendszerek, például mobiltelefon nélkül. Pedig ez csak egy-kettő azon rendszerek közül, amelyek mindenképpen szükségesek a 21. század emberének ahhoz, hogy a világ ezen a felén éljen, és hogy egyáltalán éljen.

Ismét egy kis gondolatjátékra kérnénk a Kedves Olvasót. Gondolkozzunk néhány pillanatig egy terroristacsoport vezetőjének a fejével:

Miért kellene robbantani, embert rabolni, repülőgépet eltéríteni, amikor céljainkat sokkal hatékonyabban, ráadásul sokkal kevesebb kockázattal is el tudjuk érni. Hogyan lehet mindezt elérni a hagyományos módszerek nélkül? A válasz: információtechnológia. Használd ki annak előnyeit és meglásd magad is megdöbbensz mennyire egyszerű s hatékony.

Használd ki, hogy nem tud mobiltelefon nélkül élni. Használd ki, hogy nem tud internet nélkül élni. Használd ki, hogy nem tud televízió nélkül élni. Használd ki, hogy nem tud létezni villamos energia nélkül. Ott csapj le rá, ahol a legsebezhetőbb. Vedd el tőle, amire a legbüszkébb. Foszd meg attól a magabiztosságtól, amit a tudás nyújt a számára. Vedd el tőle az információt, és meglásd a sötétben, ketrecében fel s alá rohangáló, megrémült, csapdába esett vadállathoz fog hasonlítani. Legyőzheted, ha megfosztod attól, ami a legfontosabb a számára: vedd el tőle az információt és a kommunikációt. Győzni fogsz, hiszen félelmet s rettegést okozol. Még azt sem tudja mi történt, ki tette ezt vele, s pláne nem, hogy miért. Elbizakodott és büszke. Pedig tudat alatt tisztában van a legsebezhetőbb pontjaival. Tisztán látja a diagnózist: FÜGGŐSÉGBEN SZENVED! Mégsem tesz ellene semmit. Meg sem próbálja elkerülni a végzetet. Ez a mi fegyverünk!

Reméljük, egy ilyen gondolatmenet soha nem játszódik le egy terrorista fejében sem, hiszen mindannyian el tudjuk képzelni a következményeket.

De attól, hogy nem akarunk tudomást venni a ránk leselkedő veszélyek puszta létezéséről sem, azok még nagyon is valóságosan itt vannak. Természetesen nem csak Magyarország vonatkozásában, hanem — talán még hatványozottabban — az olyan nagy országok esetében is, mint az Egyesült Államok, vagy akár a Nyugat-Európai vezető országok: Franciaország, Németország, Anglia. Ezért olyan nemzetközi összefogásra van szükség a cyber terrorizmus elleni védekezés területén, mint amilyen a hagyományos terrorizmus esetében 2001. szeptember 11-e után létrejött. Ebben a munkában a tudományos kutatással, felkészítéssel, és a felkészüléssel nekünk is részt kell vállalnunk.

Végezetül, ha a feltételezésen túl elfogadjuk azt a tényt, hogy az eddig elmondottak valódi veszélyt jelentenek, akkor Fukuyama analógiáján — persze egy kicsit más szemszögből vizsgálva — joggal kérdezhetjük: tényleg véget ér a történelem, ha a cyber terrorizmus teret nyer?

A kissé bizonytalan válasz: NEM. Ma még.

De ha nem teszünk semmit: vajon mi lesz holnap? Holnap is NEM lesz a válasz?