ALMÁSI CSABA SÁNDOR – BÁRTFAI FANNI – DR. BONNYAI TÜNDE – DR. GYARAKI RÉKA ESZTER – KISS SÁNDOR – MARGITICS JÓZSEF

A FŐVÁROS IVÓVÍZ-ELLÁTÓ RENDSZERE ELLEN INTÉZETT INFORMATIKAI TÁMADÁS POTENCIÁLIS KÖVETKEZMÉNYEI ÉS AZOK FELSZÁMOLÁSÁNAK MEGOLDÁSI LEHETŐSÉGEI

Bevezetés

Az elmúlt évek eseményei azt mutatják, hogy egy adott nemzetet a legnagyobb veszélyek már nem csak fizikailag, hanem a kibertérben is fenyegetik. A technológiai fejlődés adta lehetőségeknek köszönhetően nem csak az ipari szférában jellemző az úgynevezett rendszerbe történő kapcsolódás, hanem a lakosság alapvető ellátását biztosító infrastruktúrák esetében is egyre gyakrabban fordul elő. Bár sok eszköz egy rendszerbe történő kapcsolása nagyban megkönnyíti a mindennapi munkát és javítja az adott szolgáltatás színvonalát, azonban az így létrejött komplex rendszer sérülékenysége is jelentősen nő.

Ebből adódóan mind nemzetközi, mind hazai vonatkozásban egyre nagyobb hangsúlyt kap az ún. kritikus infrastruktúrák informatikai biztonságának kérdésköre, éppen ezért szükségesnek éreztük azt, hogy elemezzük egy adott létfontosságú rendszerelem informatikai támadásának lehetséges hatásait, illetve a helyreállítás során felmerülő kérdéseket és problémákat. Választásunk a Fővárosi Vízművekre esett, mert hazánk egyik legnagyobb ellátási képességével rendelkező ivóvíz-szolgáltatója. A Vízművek honlapján elérhető 2015-ös jelentés szerint két millió főt látnak el naponta fogyasztásra alkalmas vízzel és kezelik az általuk termelt szennyvizet. Ez naponta egy millió m^3 kapacitást jelent, amelyet 5 200 km vízhálózat tesz lehetővé.[65]

[65] http://vizmuvek.hu/files/public/Fovarosi_vizmuvek/tarsasagi_informaciok/FVM_Eves_Jel_HUN.pdf p. 10. (letöltés ideje: 2017.08.12.)

A pályamunka első részében az általunk elméletben megalkotott támadás menetét ismertetjük, amely felépítésében elsőként az internetes és egyéb, bárki számára szabadon hozzáférhető információkra támaszkodtunk, hiszen egy ártó szándékú egyén, vagy csoport is nagy valószínűséggel ezekből a forrásokból szerezné meg azokat a szükséges adatokat, amelyek elengedhetetlen fontosságúak egy hasonló volumenű támadás sikeres kivitelezéséhez.

A második fejezetben bemutatjuk a kialakult helyzet kezelésének egyes dimenzióit. A tervezés elsődleges szempontja – a pályamű elkészítésekor hatályos jogszabályok betartása mellett – a minél gyorsabb és eredményesebb válaszlépések kivitelezése, annak érdekében, hogy a lakosság számára szükséges ivóvízkészlet elérése és a szennyezett víz fogyasztásából fakadó fertőzések megakadályozása a lehető leghamarabb biztosítható legyen.

Szeretnénk azonban hangsúlyozni azt, hogy csak elméleti síkon jelentjük ki a tanulmányban leírt támadási technikák sikerességét és ezért elméleti síkon elemeztük a lehetséges következményeket is. Nem állt és jelenleg sem áll szándékunkban ötleteket adni senkinek egy esetleges támadáshoz, pusztán az általunk feltárt hiányosságokra kívánjuk felhívni a figyelmet, illetve egy olyan „rendkívüli eseményre vonatkozó forgatókönyv" megalkotása volt a célunk, amely a jövőben alapot adhat egy hasonló krízishelyzet tényleges kezeléséhez. A szerzők abban bíznak, hogy az általuk megfogalmazott preventív javaslatok hozzájárulnak ahhoz, hogy hasonló esemény a jövőben ne történhessen meg.

A budapesti ivóvíz-ellátó rendszer ellen intézett támadás kivitelezésének lépései

A Budapest ivóvízellátását biztosító szolgáltató (a továbbiakban: Szolgáltató) elleni támadás során a cél a lehető legnagyobb károkozás, ezért annak egy forró, nyári estére történő időzítése több szempontból is célszerű. Az időpont kiválasztásánál nem csak az játszathat szerepet, hogy a város lakosságának megnő az ivóvíz-fogyasztása és a vezetékes víz felhasználása: a nyáron szükséges fejenként napi 2,5-3 liter közötti vízfogyasztás mellett mindenképp figyelembe kell venni azt, hogy egy 4 fős család átlagos napi ivóvíz tisztaságú víz felhasználása megközelítőleg 600 liter[66]. Mindehhez hozzáadódik a – hőség elleni

[66] http://okoenergia.hu/vizfogyasztasi-statisztika/ (letöltés ideje: 2017.10.05.)

védekezésként elrendelt – közúthálózat és kiemelt zöldterületek locsolása és hűtése[67], illetve a magánkertek öntözése.

Különösen kiemelendő, hogy csak 2017 júniusában 391 635 fő turista tartózkodott[68] a majdnem két millió lakoson kívül a fővárosban. A fenti adatokat figyelembe véve ez a létszám jelentős többlet terhet ró mind a vízszolgáltatóra, mind a közlekedési infrastruktúrára. Különösen fennáll az utóbb említett szegmens terheltsége, amikor a főváros ad otthont egy olyan nagyobb volumenű rendezvénynek – például a 2017 nyarán megrendezett FINA világbajnokság –, amely nem csak megnövekedett számú látogatót vonz, hanem esetleges forgalomelterelésekkel is járhat.

A fent említett turisztikai adatokon túl a nyári időszak a szabadságolásokat is magába foglalja. Feltételezhető tehát, hogy ekkor a vízszolgáltatónál is csökkentett számú dolgozói állomány áll rendelkezésre, mindamellett az emberi tényezőt figyelembe véve – a hőség hatására – a koncentrációs képesség is csökken, miközben a szolgáltatás igénybevétele hatványozottan nő. Ez az állapot kedvez az úgynevezett social engineering típusú, informatikai támadások végrehajtásának, amelyek főként a célszemély hiszékenységére, gyanútlanságára alapoznak és használják ki azt.

Figyelembe véve a fent ismertetett okokat, a nyári kánikula idejére időzített többlépcsős, fiktív támadási terv az alábbiak szerint épülhet fel.

1. Informatikai támadás

Az informatikai támadás megtervezésekor első lépésben a célpont informatikai infrastruktúrájáról próbáltunk meg minél több adatot elérni nyílt forrásból. Az első gyors keresés közben segítségünkre volt többek között a főváros vízszolgáltatójának jubileumi kiadású honlapja, ahol megemlítik, hogy *„Az elektronika átveszi az irányítást: a termelő berendezések szabályozását frekvenciaváltók végzik, a gépházakat komputervezérléssel irányítják, felügyelik, a köztéri munkák folyamatirányítottak, mindezt egy központi diszpécserszolgálat tartja kézben.”*[69] Az idézett szövegen kívül találtunk képeket a központi

[67] http://www.orientpress.hu/cikk/2017-08-02_a-fovaros-kuzd-a-hoseggel (letöltés ideje: 2017.10.05)

[68] https://www.budapestinfo.hu/hu/szallashely-statisztika---minden-mutato-emelkedett-2017-elso-feleveben-budapesten-is (letöltés ideje: 2017.08.26)

[69] http://vizmuvek.hu/jubileum/ (letöltés ideje: 2017.08.22.)

irányító központról, amelyek megalapozták azokat a felvetéseinket, hogy a sebezhető emberi tényezővel számolhatunk. Ez az információ elősegíti a rendszer elleni támadás eszközének megválasztását, amely két típusú, vírus által okozott károkban nyilvánul meg. Az első vírus egy úgynevezett ramsomware, amely a levelező rendszeren keresztül behatolva titkosítja a fájlállományokat és akadályoztatja a belső kommunikációt, ezáltal felerősíti és elnyújtja a második féreg okozta károkat.

2013-ban az interneten megjelent egy részletesebb cikk a Szolgáltató akkor modernizált termelésirányító rendszeréről (a továbbiakban: SCADA), ahol mind a routerek, mind a PLC[70] eszközök esetében a konkrét termékcsaládok kerültek megnevezésre.[71] A korszerűsítés közbeszerzési pályázat kiírásával kezdődött meg. Mivel 2013 óta nem találtunk nyílt forrású kereséssel olyan közbeszerzési pályázatot, ami ehhez hasonló, nagyobb volumenű informatikai beruházásról szól, illetve maga a rendszer is 20-30 éves élettartamot ígér, ezért nagy valószínűséggel feltételezhetjük, hogy az eszközök többsége napjainkban is a négy évvel ezelőtt beszerzett termékekből áll. Ez az adat azért jelentős, mert felveti két sebezhetőség lehetőségét is, amelyek összefügghetnek egymással. Az amerikai SANS intézet 2017-es, több száz IT-biztonságért felelős szakember bevonásával készített felméréséből[72] az derült ki, hogy a rengeteg, még mindig fel nem patch-elt[73] vagy az önálló védelemmel nem rendelkező hálózati eszköz súlyos veszélyt hordozhat magában. Ezeken a réseken keresztül pedig bejuthat egy olyan, a Stuxnethez[74] hasonló kártevő, amelyet előzőleg akár a Darkneten vásárolhattak meg.

---

[70] Programozható logikai vezérlő, amely olyan bonyolultabb munkafolyamatokat vezérel, amik több, önálló szabályozással is rendelkező egységből állnak.

[71] https://sg.hu/cikkek/it-tech/96470/lecsereli-informatikai-halozatat-a-fovarosi-vizmuvek (letöltés ideje: 2017.08.22.)

[72] http://www.information-age.com/risks-facing-industrial-control-systems-reach-all-time-high-123467315/ (letöltés ideje: 2017.10.07.)

[73] Az adott programhoz tartozó, utólag javított fájlok eltérését tartalmazó információcsomag.

[74] 2010 nyarán bukkant fel Fehéroroszországban az a kártevő, amely kifejezetten SCADA rendszerekben okozott károkat. A vírus képes volt felismerni a natanzi erőmű Siemens gyártmányú PLC eszközeit és annak alapértelmezett programját felülírva úgy tette tönkre az általuk vezérelt atomdúsító centrifugákat, hogy a státuszjelző üzeneteket meghamisította, így az operátorok nem észleltek semmi rendkívüli eseményt mindaddig, amíg hallható jelei nem voltak a felgyorsult centrifugáknak. http://hadmernok.hu/2010_4_kovacs_sipos.pdf (letöltés ideje: 2017.10.07.)

1.1. A bejuttatás módszerei

Számos, az emberi naivitásra és jóhiszeműségre alapozó social engineering technika létezik. Jelen támadás során a két legnépszerűbb módszer segítségével „juttattuk be” a két kártékony kódot a rendszerbe.

1.1.1. E-mailben történő vírusküldés

Napjainkban még mindig nagy sikerrel alkalmazható a social engineering trükkjeit használó, rosszindulatú elemeket tartalmazó levelekkel történő vírusterjesztés.

A gyanútlan felhasználó megnyit egy fertőzött e-mail csatolmányt (általában ismeretlen, vagy ismerősnek tűnő feladótól), vagy egy rosszindulatú linket egy közösségi oldalon, vagy beérkezett levélben. Sok támadó rövidített URL-eket használ a rosszindulatú linkek elfedésére, így még nehezebb észrevenni, hogy az útvonal például egy fertőző kódot tartalmazó (JavaScript fájl) oldalra mutat. Bár ez a legnépszerűbb módszer, egyre inkább kezd elterjedtebb lenni a TOR-hálózaton megtalálható RaaS (Ransomware as a Service) megoldás is, ahol a rosszakaró gyakorlatilag egy szolgáltatásként vásárolja meg a hackerektől a támadást, amelynek esetleges bevétele után bizonyos részesedést kap az "eladó"[75]. Szerverek közvetlen megtámadására is van lehetőség, ha a támadó távoli asztali kapcsolaton, vagy terminálon keresztül elkezdi brute force-olni[76] a gyenge jelszavakat[77]. Amint sikerül így belépnie a gépre, már képes titkosítani az ott található adatokat. A fertőzött gépre történő

[75] Ilyen RaaS platform a felhasználó barát Satan platform is, ahol egyszerűen lehet a notPetya-hoz vagy a WannaCry-hoz hasonló vírust szolgáltatásként venni.

(Cisco Midyear Cybersecurity Report p. 23.) https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1456403/Cisco_2017_Midyear_Cybersecurity_Report.pdf?elqTrackId=f6ccd8439e9945639096a9846044695a&elqaid=5897&elqat=2 letöltés ideje: 2017.10.07.)

[76] Nyers erő segítségével történő jelszó feltörés, amelynek lényege, hogy nagy teljesítményű számítógépek lehetséges jelszó karaktersorozatok nagyon nagy számú permutációját próbálják végig a támadáskor, viszonylag rövid időn belül.

[77] 2017 januárjában a Keeper Security jelentése szerint a három leggyakoribb jelszó 2016-ban az *„123456”,* az *„123456789”* és a *„qwerty”* voltak. (The Most Common Passwords of 2016. https://keepersecurity.com/public/Most-Common-Passwords-of-2016-Keeper-Security-Study.pdf letöltés ideje: 2017.10.05.)

településekor a zsarolóvírus általában praktikusan megkeresi a jpg, .xls, .xlsx, .png, .doc, .docx, .ppt, stb. kiterjesztésű fájlokat, mivel a személyes és szenzitív adatok[78] nagyrészt képek és dokumentumok formájában vannak tárolva. Ezen adatok enkriptálása után történik meg maga a zsarolás: pénz (általában Bitcoin) ellenében ígérik, hogy feloldják a titkosítást.

A fent ismertetett módszerek közül ebben az esetben a számlaként álcázott -pdf kiterjesztésű fájlban történt a zsarolóvírus bejuttatása. Annak érdekében, hogy a levelezőrendszer ne szűrje ki automatikusan a kártevőt tartalmazó levelet, úgynevezett megbízható e-mail címeket használtunk, amelyekhez a hozzáférést a gyenge jelszavak feltörése és a hozzájuk tartozó gyanútlan felhasználói magatartás biztosították[79].

1.1.2. Az ajándékba küldött vagy elhagyott adathordozó eszköz

A PLC eszközöket megtámadó kártevő pendrive-on történő bejuttatásához, az egyik alapvető emberi tulajdonság, a kíváncsiság adta lehetőségeket használtuk ki.

A parkolóban elhagyott pendrive ötlete elég egyszerűnek és kézenfekvőnek tűnhet, azonban pont ez az egyszerűség kérdőjelezi meg a módszer hatékonyságát. Az alapelv az, hogy a vírust egy adathordozó tartalmazza, amelyet „véletlenül" a kiszemelt dolgozó autójának közelében hagynak el, aki kíváncsiságból felveszi és csatlakoztatva a számítógépéhez a vírus észrevétlenül bejuthat a hálózatba. A módszer jelentős kockázatának tekintjük, hogy nem garantálható az, hogy a célszemély fogja megtalálni, vagy egyáltalán felvenni az eszközt.
A módszer továbbfejlesztett változata, az „ajándékba küldött" pendrive trükk azonban több sikerrel kecsegtethet, így a Szolgáltató elleni támadás során is ezt a bejuttatási technikát

[78] Ebben az esetben a szenzitív adat lehet minden, a személyügyi osztály által kezelt személyes adat vagy a munkavállaláshoz elengedhetetlen szükségességű orvosi alkalmassági és vizsgálati dokumentumok), amelyeket a törvény fokozottabban véd – az információs önrendelkezési jogról és az információszabadságról 2011. évi CXII. törvény 3. § (3) alapján.

[79] Az IBM Security 2016-os tanulmánya szerint a ransomware-ek által fertőzött e-mail-ek száma 6000%-kal növekedett az előző évhez képest. A támadók egyre keményebben próbálkoznak azzal, hogy a felhasználókat a saját levelezésükön keresztül fertőzzék meg. Ezek az e-mail-ek általában számlákat, kimutatásokat, jegyzeteket és egyéb, fontosnak tűnő tartalmú csatolmányokat tartalmaznak. (http://invenioit.com/security/ransomware-statistics-2016/ letöltés ideje: 2017.10.09.)

választottuk. Ebben az esetben egy konkrét személynek kézbesítik a fertőzött eszközt, egy olyan legendával övezve, amely szerint az adathordozót vagy valamilyen nyereményjátékon nyerte, esetleg egy partnercég, vagy más szolgáltató vállalat küldte ajándékba. Még hihetőbbé lehet tenni a történetet, ha egy bizonyos eseményhez kötjük a küldött eszközt.

A közösségi oldalon előzetesen leinformált[80] személynek küldött adathordozó esetében bármelyik történet hihető lehet, főleg akkor, ha az valamilyen cég, vagy olyan esemény emblémájával díszített, amely a közelmúltban került megrendezésre és tudjuk, hogy a címzett biztosan részt vett rajta. Anyagi vonzatát tekintve kimondottan könnyen kivitelezhető módszer, hisz pár ezer forintért szinte bárhol lehet logóztatni ilyen tárgyakat. Apró mozzanat, ám rendkívüli mértékben el tudja altatni a gyanakvást.

1.2. Az informatikai rendszerekben okozott károk

A Szolgáltató informatikai rendszerének alaprendeltetése, hogy a főváros ivóvíz-ellátását biztosító komplex rendszer folyamatosan működjön. Budapest vízellátását kettő vízbázis biztosítja:

→ az Északi vízbázis (Szentendrei-sziget), amely a város ellátásának 70%-átt biztosítja, valamint

→ a Déli vízbázis (Csepel-sziget), amely a maradék 30%-ot szolgáltatja.

A víztermelés módja azonban mind a két területen egyforma: a parti szűrésű vizet csápos kutak nyerik ki a Dunából. A kitermelt vízből elsőként a vas- és mangántartalmat vonják ki oxidációs eljárás folytán ózon segítségével. Ezt követően a szerves anyagokat távolítják el, végül pedig klórral fertőtlenítik az ivóvizet, hogy a mikrobák és férgek is elpusztuljanak a vízből[81]. A tisztítás után a víz egy tározó medencébe kerül (a Gellért-hegy

[80] A célszemély digitális lábnyomának felkutatására például remek eszköz lehet a http://www.uk-osint.net/ honlap. Ennek segítségével többek között az adott felhasználó összes Facebookos tevékenységét listázni lehet: elsőként a felhasználó adatlapjának URL címének bemásolásával egy numerikus azonosítót generálunk, majd annak segítségével megkapjuk például azt, hogy hány fényképen szerepelt, illetve milyen eseményeken vett részt. Mivel a legtöbb konferencia rendelkezik ún. Facebook-os eseménnyel, ahol a részvétel visszaigazolható, könnyen kaphatunk valós képet arról, mely rendezvények „reklámajándékaként" tudjuk a vírushordozó eszközt célba juttatni.

[81] http://budapest.hu/Documents/varosfejlesztesi_koncepcio_2011dec/11_Kozmuvek_jav.pdf (letöltés ideje: 2017.10.08.)

oldalában lévő szabadon látogatható) néhány órára, ahol keverőlapátokkal áramoltatják, így folyamatosan friss oxigénhez jut.

Feltételezzük, hogy a levelező rendszeren keresztül bejuttatott ramsomware és a PLC eszközöket célzó kártevő az informatikai rendszerben – egymástól függetlenül – ellehetetleníti működést. A zsaroló vírus esetében a kártevő, amely a fentebb említett – e-mailen történő – bejuttatási módnak köszönhetően került az informatikai rendszerbe, hozzáfér a hálózati meghajtókon tárolt fájlokhoz, azokat titkosítja és csak 900 dollár értékű Bitcoin megfizetése után bocsájtja rendelkezésre a feloldó kulcsot. Ennek köszönhetően a belső kommunikáció akadozik, valamint a munkavégzés ellehetetlenül.

Szinte a bejuttatott zsarolóvírussal egy időben a másik kártevő sikeresen felülírta a SCADA rendszer eszközei logikai vezérlőegységeinek alap programjait, aminek következtében a klóradagolás megszűnt, a keverőlapátok is leálltak, de a vízminőséget ellenőrző eszközök a szokásos 0,5 mg/liter klórértéket mutatják. Az áramoltatás hiányában az előzetesen nem tisztított vízben néhány óra alatt elszaporodnak a baktériumok és vírusok, amelyeknek jelentős az egészségre gyakorolt negatív hatásuk. Ennek kivitelezésére az éjszakai idősáv tűnt a legmegfelelőbbnek, mert reggelre szaporodnak el a vízben a baktériumok annyira, hogy tömeges megbetegedéssel lehessen számolni a délelőtti órákban, valamint a lakosság ivóvíz-felhasználása a reggeli, illetve az esti időszakban emelkedik meg jelentősen.

1.3. A lakosságra gyakorolt élettani hatások

Az ivóvízhálózatba került, az ivóvízminőségi követelményeknek nem megfelelő tisztaságú víz használata következtében számolni lehet tömeges emésztőrendszeri megbetegedéssel, amelynek hatását a 2006-ban történt miskolci esethez lehet hasonlítani, amikor tömegesen fordultak orvoshoz meg E. coli és calici fertőzés miatt[82]. Mindez elsősorban és kezdetben hányással, hasmenéssel járó tüneteket okoz, de közvetetten láz, tartósan pedig kiszáradás állapotába sodorhatja a beteget.

[82]Epidemiológiai Információs Hetilap – 13. évf. 23. sz. 2006. június 16. pp. 291-296. http://epa.oszk.hu/00300/00398/00208/pdf/00208.pdf (letöltés ideje: 2017.10.07.)

Elsősorban a kisgyermekek és idősek vannak kitéve a fertőzés miatti kiszáradás veszélyeinek. A fertőzés a beteg és idős, legyengült szervezetet jelentősen befolyásolhatja, valamint azokat a betegeket érintheti súlyosan, akik speciális kórházi ellátásra szorulnak. Az ő ápolási feladataikat nehezíti az, hogy a tömeges fertőzések miatt számos gyermek, illetve felnőtt jelentkezik kórházi ellátásra, ezért az egészségügyi intézményekben a betegek feltorlódnak, ezáltal növelve a továbbfertőzés lehetőségét és valószínűségét.

2. Fizikai támadás

Annak érdekében, hogy az okozott károk szélesebb körben fejtsék ki hatásukat és a kezelés/elhárítás nehezebben legyen kivitelezhető, elengedhetetlen lépésként ítéltük meg a fizikai támadás szükségét.

A külföldi, illetve sajnos a hazánkban is előforduló mintát alapul véve a Budapesti Közlekedési Zártkörűen Működő Részvénytársaság (a továbbiakban: BKV Zrt.) autóbusz garázsainak közelében, valamint egy metróvonalon, a reggeli csúcsidőszakban történő bombatámadás végrehajtása adja a támadássorozat második fázisát, amelynek következében a kialakuló közlekedési káosz akadályozni fogja az alternatív vízkészletek eljuttatását a város különböző pontjaiba, ezáltal a krízishelyzet tovább eszkalálódhat.

A művelet megtervezésekor, ahogyan az előbbiekben, nyílt forrású információkat használtunk fel, amelyhez a városban történő életvitelszerű tartózkodásból fakadó ismeretek, illetve az interneten fellelhető adatok szolgáltak támpontul.

2.1. A fővárosi tömegközlekedési csomópontokról elérhető nyilvános információk elemzése

Elsőként a két legnépszerűbb metróvonalat összehasonlítva kiválasztottuk azt az állomást, ahol a robbanószert tartalmazó táska elhelyezésre kerül. A forgalmi adatok elemzése az M2 és az M3 vonalat szállítási kapacitására, napi utas-számára, legnagyobb forgalmú állomására, valamint ennek csúcsforgalmára terjedt ki:

M2 vonal		M3 vonal	
Legnagyobb szállítási kapacitás (utas/h/ir.)	2 3 000	Legnagyobb szállítási kapacitás (utas/h/ir.)	2 8 200
Napi utasszám (munkanapokon)	4 51 627	Napi utasszám (munkanapokon)	6 26 179
Legnagyobb forgalmú állomás napi utasforgalma (fő)	7 7 521	Legnagyobb forgalmú állomás napi utasforgalma (fő)	7 5 976
Legnagyobb forgalmú állomás csúcsórai utasforgalma (felszállók)	1 1 297	Legnagyobb forgalmú állomás csúcsórai utasforgalma (felszállók)	9 792

1. sz. ábra: A vizsgált metróvonalak forgalmi adatai[83]

A két metróvonal közös pontja az, hogy mindkét esetben a Deák Ferenc téri megálló a legnépszerűbb és a leginkább terhelt, a reggeli csúcsidőben körülbelül százezer fő halad át a területen, ezért a robbanószerkezetet a legnagyobb pusztítás érdekében ott célszerű elhelyezni reggel 8 óra körül, mert a nagy tömegben egy-egy elhagyott táska kevésbé kelt nagy feltűnést.

Az interneten – jelenleg bárki számára – elérhető információk szerint Budapesten öt autóbusz garázst üzemeltet a BKV Zrt., amelyek pontos címe szintén nyilvános, így a kész robbanó csomagok könnyen célba juttathatók, legegyszerűbben hajléktalanok közreműködésével, akik szerepe abban merül ki, hogy az általuk nem ismert tartalmú táskákat a kijelölt helyekre leteszik bizonyos pénzösszeg fejében.

Feltételezzük, hogy a két, egymást követő robbantás-sorozat a helyszínek alapos megválasztásával a maximálishoz közeli rombolási hatásfokot érte el.

2.2. A bombák készítésének módszere, az alapanyagok beszerzésének lehetőségei

A 2016-os Teréz körúti robbantás[84] kapcsán vetődött fel ismét, hogy hazánkban milyen „hatékonysággal” lehet a bűnüldöző szervek figyelmének felkeltése nélkül robbanószerkezeteket előállítani. Az interneten számos módszer fellelhető a házilag

[83] A táblázat forrásai: http://metros.hu/vonal/jellemzok_m2.html; http://metros.hu/vonal/jellemzok_m3.html (letöltés ideje: 2017.10.01.)

[84] 2016. szeptember 24-én este a Teréz körúton egy üres üzlethelyiség bejáratánál robbant fel az a hátizsákba rejtett bomba, amely súlyosan megsebesített két rendőrt. Bár számos járókelő haladt el a csomag előtt, a támadó célpontjai kifejezetten rendőrök voltak. A robbantás nagysága, illetve az, hogy a támadó közvetlen közelről hozta működésbe a szerkezetet, arra enged következtetni, hogy már korábban is készíthetett hasonló pokolgépeket, annyira pontosan voltak az összetevők kimérve, illetve többször is ki kellett próbálnia a szerkezetet, ami alapján meg tudta azt állapítani, hogyan lehet úgy legközelebb a robbantáshoz, hogy ő azt sértetlenül ússza meg. http://hvg.hu/itthon/20160926_Hidegverrel_lepett_at_aldozatain_a_robbanto (letöltés ideje: 2017.10.01.)

elkészíthető pokolgépekről. A két leghíresebb mű az *Anarchist Cookbook*[85] és az Iszlám Állam Inspire nevű magazinjában megjelent *Make a bomb in the kitchen of your Mom*[86]. Az itt szereplő robbanószerkezetek vegyi összetételét tekintve megegyeznek abban, hogy olyan, szinte bárhol beszerezhető alapanyagokból állnak, mint például az aceton, a hidrogén-peroxid és sósav. Ezeken kívül az időzített és/vagy késleltetett működtetésű, házi készítésű robbanószerkezetek szerkezeti felépítésüket tekintve egy zárt áramkörből, gyújtási láncból állnak, az időzítő, késleltető szerkezetnél megszakítva[87]. Az elektromos indító szerkezet alapja is lehet egyszerű használati tárgy, mint például egy karóra, vagy akár egy mobiltelefon.

A megszerzett ismeretek birtokában elkészített távvezérlésű pokolgépeket ezek után már csak egy hátizsákba kell helyezni, majd azokat a hajléktalanok által eljuttatni az alapos mérlegelést követően kiválasztásra került pontokra. A hátizsákok beszerzésénél arra kell ügyelni, hogy azok nehezen lekövethető, a lehető legátlagosabb darabok legyenek, amelyek bármelyik aluljáróban vagy kínai üzletben készpénzes fizetés során megvásárolhatóak.

2.3. A robbantások által okozott károk összegzése, hatása a lakosságra

A fent említett módszerekkel elhelyezett bombák robbanásakor nem csak a kiesett metróvonal pótlására szolgáló buszok üzembe állítása lehetetlenül el. A robbantások helyszínét – várhatóan nagy sugarú körben – teljesen lezárják, a helyszínekre vezető útvonalakon jelentős mértékben korlátozzák a gyalogos és gépjárműves közlekedést, különös tekintettel a mentők és a tűzoltó egységek számára biztosítandó felvonulási utak érdekében. A robbantási helyszíneken tartózkodók menekülése és pánikreakciója várhatóan negatívan befolyásolja a mentési tevékenységet, míg a város távolabbi pontjain feltorlódott tömegek a

---

[85] 1970-ben William Powell írta, tiltakozva az USA vietnámi háborúban aktívan részvevő kormányzata ellen. Bár a könyv lassan 50 éves lesz, a mai napig fellelhető az interneten, illetve folyamatosan bővítik azt. https://uniteyouthdublin.files.wordpress.com/2015/01/anarchist-cookbook-william-powell.pdf (letöltés ideje: 2017.08.22.)

[86] 2010 nyarán jelent meg a magazin, amelynek 33. oldalán a mai napig elérhető a tartalom. https://azelin.files.wordpress.com/2010/06/aqap-inspire-magazine-volume-1-uncorrupted.pdf (letöltés ideje: 2017.08.27)

[87] Daruka Norbert: A bűnös célú/terror jellegű robbantások és az ellenük való védekezés lehetőségei, különös tekintettel a tűzszerész feladatok ellátására. Doktori (PhD) értekezés p. 40. http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2014/daruka_norbert.pdf (letöltés ideje: 2017.08.26.)

mindennapos, reggeli forgalmi dugók méretét duzzasztják tovább. A helyzetet leginkább az az már megtörtént esemény szemlélteti, amikor 2016 decemberében az M2 metró Pillangó utcai megállójánál két szerelvény összeütközött[88]. A baleset következtében a reggeli csúcsforgalom egyik csomópontjától (Örs vezér tér) a Puskás Ferenc Stadion metróállomásig csak pótló buszok közlekedtek, amelyek kapacitása eleve nem volt elegendő az utasok száma tekintetében. Az ezzel párhuzamosan kialakult, jelentős forgalmi dugót tovább súlyosbította, hogy az utasok a gyorsabb utazás reményében a taxi társaságokhoz fordultak. Aznap reggel 9 órára a XIV. kerületben egyik személyszállítást végző társaság autója sem volt elérhető, így a város más pontjairól érkezőkre is átlagosan 40 percet kellett várni.

Ilyen körülmények között belátható az, hogy az ivóvíz-ellátás pótlására tett intézkedések keretében történő vízosztás azokon a helyeken is akadályokba fog ütközni, ahol leginkább szükség van emberi fogyasztásra alkalmas vízre (pl.: elsősorban egészségügyi és szociális intézmények).

Az ismertetett következmények mellett nem elhanyagolható az utazó közönség általános elégedetlensége, ami negatív irányba fogja befolyásolni a közhangulatot, ez pedig a támadás harmadik lépésének kivitelezésékor elengedhetetlen fontossággal bír.

3. Mesterségesen szított megmozdulások a fővárosban

A Szolgáltató ellen intézett informatikai támadás, illetve a város több pontján történt robbantás rövid időn belül a médiaszolgáltatók vezető hírei között szerepel, folyamatos és több oldalról érkező tudósításokra lehet számítani. A kezdeti zűrzavar miatt a dezinformáció ez esetben is komoly veszélyforrásnak számít, amely a lakosság viselkedését és a közvéleményt jelentősen befolyásolhatja. Az álhírek felbukkanását egy ideig lehetetlen kiszűrni, valamint a sajtóhoz eljuttatott információk valódiságát – elsősorban idő hiányában – szinte lehetetlen ellenőrizni. A szenzációhajhászás időszakában (az első egy órában) megindulnak a találgatások, illetve a fél információk alapján az egymást generáló hamis, vagy csak féligazságot tartalmazó hírek villámgyors terjedése.

[88] http://hvg.hu/itthon/20161205_baleset_miatt_nem_jar_a_2es_metro (letöltés ideje: 2017.08.12.)

Mindez a fővárosban várhatóan kisebb-nagyobb csoportok „összeverődéséhez” vezethet, vagy megmozdulásokat generálhat, amelyek a „kritikus tömeg elmélet” mentén akár tüntetés jellegű problémagócokká nőhetik ki magukat.

Ezt az általános tömegviselkedést kívánjuk felhasználni arra, hogy a Szolgáltató informatikai és a tömegközlekedés fizikai támadását követően, a rendvédelmi szerveket túlterheljük, aminek köszönhetően a kárelhárítás akadályoztatva lesz.

3.1. A közösségi oldalak és a média szerepe

Ahogyan arra Kovács László és Krasznay Csaba is rámutatott a Digitális Mohács című műben: *„már komoly befolyásoló tényezőként számolhatunk ezekkel a hírportálokkal a lakosság egészét tekintve. Itt következik a pszichológiai hadviselés következő fázisa. Ha nem is könnyű feladat, mégis lehetséges hamis híreket elhelyezni a különböző hírportálokon, azok meglévő és többször bizonyított sebezhetősége és sérülékenysége miatt. Amennyiben ezek a hamis hírek egymással összefüggnek, illetve a különböző blogokon is megjelennek, már komoly mértékű pánikot is okozhatnak.”*[89]

Az úgynevezett „médiahack” több irányból történő, célzott manipulálása biztosítja a lakosság egységességének megbontását. A robbantásokat követően a bulvársajtónak eljutatott, megbízhatónak beállított, neve elhallgatását kérő, rendvédelmi szervekhez közel álló forrásoktól kapott információk azt sugallják, hogy a támadássorozat mögött az Iszlám Állam[90] áll, amelynek tagjai a magyarországi muszlim közösségben rejtőznek. Ez az információ, illetve hamis profilokkal történő gyűlöletkeltés a közösségi oldalakon hamar fellobbantja a muszlim kisebbség iránti ellenszenvet, amelynek következtében fizikai atrocitásokkal is lehet számolni.

Feltételezhető, hogy a robbantások után a lakosság inkább bezárkózik, ezért az egyetlen mód, amellyel nagyobb tömegeket az utcára lehet szólítani, a reggeli robbantásokban elhunyt áldozatokra való nyilvános megemlékezés kezdeményezése. Ahhoz, hogy ez a legszélesebb

[89] Kovács László, Krasznay Csaba: A digital Mohács. p. 49.

[90] Az elmúlt hónapokban, Európában elkövetett terrortámadásokért azonnal vállalt felelősség, valamint az, hogy a szervezet kísérletet tett arra, hogy magára vállalja a 2017 októberének első napjaiban elkövetett Las Vegas-i merényletet, még inkább hihetővé teszi az Iszlám Államhoz fűzhető kapcsolódás tényét.

közönséghez elérjen[91], célszerű Facebookon meghirdetni egy eseményt, figyelemmel arra is, hogy a terrorveszélyhelyzet kihirdetése után az előre bejelentett tüntetéseket a gyülekezési jog korlátozásával valószínűleg nem fogják engedélyezni. Így azonban tűnhet egy „spontán" összegyűlésnek.

Célszerűnek tartjuk azt is, hogy a megemlékezés időpontjában a muszlim közösségnek is szervezzünk egy megemlékezést a „Not in my name[92]" jegyében azért, hogy kifejezhessék részvétüket és hangot adhassanak annak, hogy nem osztják a radikális muszlim nézeteket.

3.2. A tömeges megmozdulásokból eredő kockázatok vizsgálata

Az előzőekben felvázolt szerveződések – az álhíreknek köszönhetően – hamar fordulhatnak tömeges, elégedetlen, akár politikailag is átitatott, ellenséges demonstrációba.

A terrortámadás alapvető traumája és az egész nap közösségi oldalakon hergelt, valamint bulvársajtóban megjelent ellenséges és megosztó cikkek hatására a résztvevők egy eleve felfokozott lelki állapotban érkeznek a helyszínekre. Mindezt egy-két „beépített személy" könnyen kiaknázhatja pár elejtett megjegyzéssel, gondolunk itt a muszlim tömegben egy hangosan elkiáltott „megérdemelték sorsukat a hitetlenek", vagy a gyászoló tömegben a muszlim közösséget okoló mondatokra. A tömegben elvegyülő, konfliktust szító egyének szinte láthatatlanok maradnak, de a két csoport összeütközése gyakorlatilag elkerülhetetlen. Az ilyen jellegű tömeges rendbontás nemcsak az ivóvíz általi fertőzés további terjedését segítheti elő, hanem a kialakuló konfliktushelyzetben esetlegesen megsérült emberek ellátásával is tovább terheli az amúgy is kapacitása végén járó egészségügyi ellátó rendszert.

Rendvédelmi szempontból azonban felmerülhet az is, hogy a tömeg potenciális célpontot nyújt egy újabb merényletre, így a rendőrség a feloszlatás vagy a biztosítás dilemmájába kerül.

---

[91]Okkal feltételezhető a részvételi hajlandóság az alapján, hogy a más országokban elkövetett terrorcselekmények kapcsán – együttérzésük kifejezésére – emberek ezrei változtatják meg a közösségi oldalakon szereplő profilképeiket az érintett ország zászlajára.

[92]http://www.thehindu.com/news/national/what-is-not-in-my-name-all-about/article19194499.ece (letöltés ideje: 2017.10.07.)

A biztosítás újabb erőket von el a hatóságoktól, akik a nyomozáson és a krízishelyzet felszámolásán dolgoznak, azonban ha a feloszlatás mellett döntenek, sajnos fennáll annak a veszélye, hogy a demonstrálók/megemlékezők a rendőrökre támadnak, akik a testi kényszer alkalmazása miatt ellenszenvet váltanak ki a lakosságból, amely akár ismételten akadályozhatja a szakszerű intézkedéseket. Bármely változatot is választják, a támadók elérték céljukat: az alkotmányos rend felborult, illetve a lakosság egységessége is, amely tovább súlyosbítja a következménykezelés nehézségeit.

A kialakult krízis kezelésének dimenziói

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 3. melléklete[93] a kritikus infrastruktúrák között nevesíti az ivóvíz-szolgáltatás létesítményeit. A kritikus infrastruktúrák a lakosság alapvető ellátásában nélkülözhetetlen szerepet töltenek be, ezért védelmüket állami és üzemeltetői szempontból is prioritásként kell kezelni.

A tanulmány második részében a fővárosban uralkodó helyzet felszámolásához szükséges intézkedéseket, illetve a meghatározott jogszabályok alkalmazása által teendő válaszlépéseket ismertetjük. Megvizsgáljuk továbbá a magánszektor bevonásának egyes lehetőségeit, amelyek a beavatkozói, a kárelhárításért felelős, a nyomozati és a rendfenntartásra rendelt szervek tevékenységét segíthetik.

1. Az eseménysor kezelésének katasztrófavédelmi szempontú összefoglalása

Tárgyalt helyzetben terrortámadás történt, tehát az Országgyűlés a kormány kezdeményezésére meghatározott időre terrorveszélyhelyzetet hirdethet ki az Alaptörvény 51/A. cikk értelmében, amelynek kihirdetéséhez, meghosszabbításához a jelen lévő országgyűlési képviselők kétharmadának szavazata szükséges.

[93] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 3. melléklete

„(4) A Kormány a terrorveszélyhelyzet idején rendeletet alkothat, amellyel - sarkalatos törvényben meghatározottak szerint - egyes törvények alkalmazását felfüggeszthetti, törvényi rendelkezésektől eltérhet, valamint egyéb rendkívüli intézkedéseket hozhat.

(5) A Magyar Honvédséget a (3) bekezdés szerinti intézkedések hatályossága és a terrorveszélyhelyzet idején akkor lehet felhasználni, ha a rendőrség és a nemzetbiztonsági szolgálatok alkalmazása nem elegendő."[94]

A Kormány első intézkedései között azonnal kirendeli a rendvédelmi szervek megerősítésére a Magyar Honvédséget (a Magyar Honvédség *belföldi* alkalmazása), elsősorban a kiemelt létesítmények (például kritikus infrastruktúrák) védelmére. A helyzet kezelésére a katasztrófavédelem alaprendeltetését és működését tekintve a veszélyhelyzeti (Magyarország Alaptörvénye, 53. cikk) állapotnak megfelelő intézkedések történnek. A beavatkozás jogszabályi alapját és hátterét Magyarország Alaptörvényéből következően

→ a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény, valamint

→ a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvények jelentik.

Rendkívüli esemény során kettő, kifejezetten a Kormány döntéseit előkészítő kormányszerv láthat el javaslattevő, véleményező, illetve szakmai tanácsadó tevékenységet a védelmi-, illetve a honvédelmi igazgatás területein:

→ a Honvédelmi Igazgatási Koordinációs Tárcaközi Munkacsoport (a továbbiakban: HIKOM), valamint

→ a Katasztrófavédelmi Koordinációs Tárcaközi Bizottság (a továbbiakban: KKB).

A HIKOM alaprendeltetése a Honvédelmi Tanács[95] és a Kormány speciális működési feltételeinek biztosításával összefüggő feladatok tárcaközi egyeztetése. Feltételezett helyzet belbiztonsági természetéből adódóan nem indokolja fenti munkacsoport működtetését,

[94] Magyarország Alaptörvénye *51/A. cikk*

[95] A Honvédelmi Tanács összehívása a honvédelmi típusú különleges jogrendben (hadiállapot kinyilvánítása vagy idegen hatalom fegyveres támadásának közvetlen veszélye, rendkívüli állapot) esetén lehetséges.

azonban a Honvédelmi Minisztérium létre hozhat a KKB munkáját támogató, szakértő munkatörzset.

A KKB a katasztrófavédelemmel összefüggésben döntés-előkészítő, valamint a katasztrófák elleni felkészüléssel, megelőzéssel, védekezéssel és helyreállítással kapcsolatban koordinációs feladatokat lát el. A KKB, a katasztrófák elleni védekezéssel kapcsolatos tudományos, elemző- és értékelő tevékenysége mellett – operatív munkaszerve útján – koordinálja a védekezésben részt vevő központi államigazgatási szervek védekezéssel kapcsolatos szakmai tevékenységét, javaslatot tesz a felmerült védekezési költségek biztosítására, és a rendelkezésre álló, illetve vis maior pénzeszközök felhasználására.

A feltételezett esemény következtében kihirdetett terrorveszélyhelyzet a veszélyhelyzetnél magasabb szintű jogrendi tényállás, azonban a KKB-t a veszélyhelyzeti különleges jogrendi állapotnak megfelelően alkalmazzák, amellyel a kiemelt létesítmények üzemzavara, működési elégtelensége, működésképtelensége és a lakosság alapvető ellátásában keletkező üzemfolytonosság akadozása/szünetelése kezelhető. Az 1824/2015. (XI. 19.) Korm. határozat alapján továbbá kritikus szintre emelik a terrorfokozatot, a védelmi igazgatás rendszere összességében tehát terrorelhárítási prioritással működik, míg a katasztrófahelyzet elhárítása és kezelése a veszélyhelyzeti állapotnak megfelelően szerveződik.

A katasztrófaveszély időszakában és a veszélyhelyzet során ellátandó feladatokat, valamint a veszélyhelyzetre vonatkozó sajátos irányítás szabályait a Katasztrófavédelmi törvény végrehajtási rendelete[96] tartalmazza, amely részletezi a területi és helyi védelmi igazgatási szintek katasztrófák elleni védekezéssel összefüggő feladatait. A magyar védelmi igazgatási rendszer hierarchiája alulról építkezik az alábbiakban részletezett formában.

[96] A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. tv. végrehajtásáról szóló 234/2011. (XI. 10.) Korm. rendelet.

Települési szint (főpolgármester, polgármester)

A Katasztrófavédelmi törvény alapján – veszélyhelyzet időszakában – a hivatásos katasztrófavédelmi szerv által kijelölt tiszt segíti a polgármester védekezéssel/beavatkozással kapcsolatos tevékenységét és közreműködik az okozott károk felmérésében.

Egyeztetve más rendvédelmi, közigazgatási és a gazdálkodó szervek kijelölt kapcsolattartóival, összegzik a károsult eszközrendszert (például buszok, lakóingatlanok, egyéb létesítmények), hogy abból meghatározhatók legyenek a helyreállításhoz szükséges erőforrások. A polgármester részt vesz továbbá a védekezésben részt vevő erők váltásának, pihentetésének és ellátásának szervezésében is. Erre a célra kijelölhetők például sportlétesítmények tornacsarnokai, vagy konferenciatermek, amelyről – szükség esetén – hatósági határozatot kell hozni (katasztrófavédelmi célú gazdasági és anyagi szolgáltatások fővárosi szintű igénybevétele). Jelen esemény kezelése kapcsán, gazdálkodó szervezetek meghatározott körét érintően, igénybe kell venni például ivóvíz/élelmiszer/takarmány szállítására alkalmas szállítóeszközöket, szerelvényeket, tartályokat, mobil mosdóhelyeket és fertőtlenítő szereket, valamint ezek szállítókapacitását, a szállításukra alkalmas járműveket.

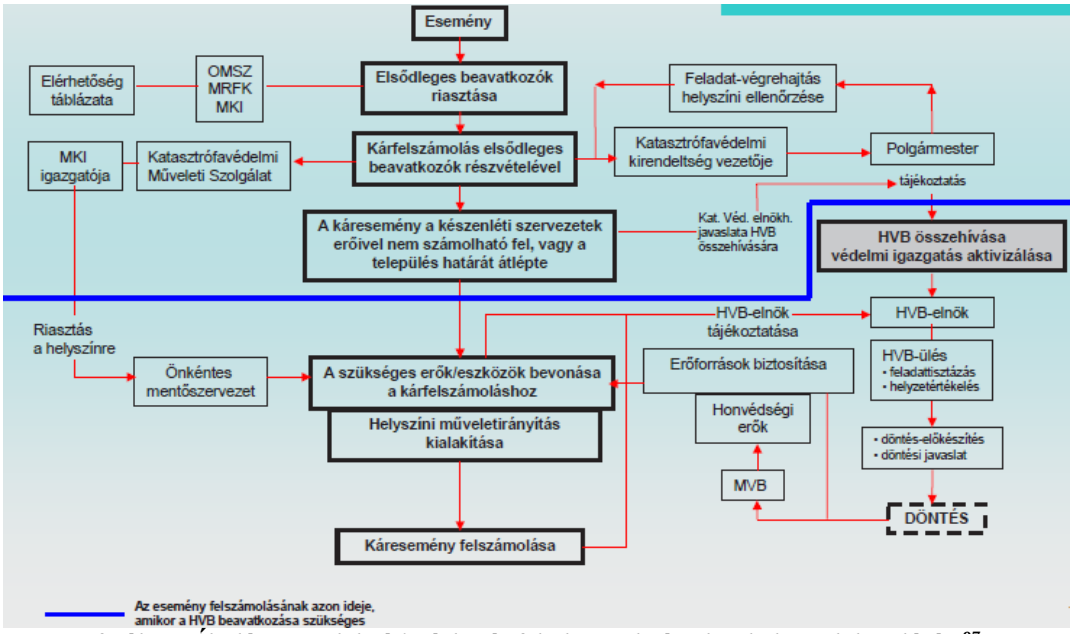
A polgármester a katasztrófavédelmi szempontból I. és II. veszélyességi osztályba sorolt településen (a katasztrófák elleni védekezésre való felkészülési, védekezési és helyreállítási szakmai feladataiban, továbbá a rendvédelmi és honvédelmi feladataiban közreműködő) közbiztonsági referenst jelöl ki. A felvázolt terrortámadás által érintett kerületek jelentős része az I. és a II. kategóriákba van sorolva *a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény IV. fejezetének* hatálya alá tartozó üzemek általi veszélyeztetettség alapján. Ebből adódóan a kijelölt referens feladatai a tárgyalt cselekmény időszakában:

- → előkészíteni a polgármester védekezéssel kapcsolatos szakmai döntéseit a lakosság és a létfenntartáshoz szükséges anyagi javak védelme érdekében,
- → kapcsolatot tartani a védekezést irányító és a védekezésben közreműködő szervekkel, erről tájékoztatni a polgármestert,
- → részt venni a kitelepítés, kimenekítés, befogadás és visszatelepítés feladataiban, amennyiben szükséges.

Helyi szint (Helyi Védelmi Bizottság, a továbbiakban: HVB)

A HVB a Megyei Védelmi Bizottság irányítása alatt működik, meghatározza a beavatkozás/védekezés helyi feladatait, ellenőrzi azok végrehajtását, illetve elrendeli a települési polgári védelmi erők bevonását, koordinálja a védekezésben részt vevő polgármesterek védekezési tevékenységét. A HVB elnöke a katasztrófavédelmi feladatok ellátásával kapcsolatos döntésekről tájékoztatja a Fővárosi Katasztrófavédelmi Igazgatóság igazgatóját, felelős továbbá a lakosság veszélyhelyzeti tájékoztatásáért. A fővárosi kerületekben is HVB működik, amelyek illetékességi területe a fővárosi kerületekhez igazodik. Tevékenysége keretében gondoskodik a helyreállítás meghatározott sorrendjének és ütemének megvalósításáról, folyamatos kapcsolatot tart az érintett létesítményekkel. Intézkedik továbbá a védekezéshez igénybe vehető állomány és eszközök átcsoportosításáról és bevonásáról, illetve a lakosság alapvető ellátásának biztosításáról a normál életkörülmények helyreállításáig.

Feltételezett esemény kapcsán a robbantás-sorozat elsősorban és időbeliségét tekintve a katasztrófavédelem tűzoltó erőinek beavatkozását igényli. Az első robbantást követően exponenciálisan emelkedik a Fővárosi Katasztrófavédelmi Igazgatóság főügyeletére beérkező, a robbanásokról szóló hívások száma, illetve később a szennyezett, bűzös ivóvízzel kapcsolatban is egyre több lakossági bejelentés érkezik, ami jelentősen leterheli a Tevékenység-irányítási Központot (a továbbiakban: TIK) és nagymértékben megnehezíti az egységes segélyhívás-fogadást a 112-es telefonszámon. A TIK hamarosan tömeges jelzésként fogja kezelni az esemény bejelentéseit, hogy biztosítsa a fővárosi erők, eszközök és események átláthatóságát, ezzel egy időben, a jelentési rendnek megfelelően, értesítik a fővárosi katasztrófavédelmi igazgatót. Az első bejelentést követő egy órán belül az illetékes polgármesterek tájékoztatása megtörténik, összeülnek az érintett helyi védelmi bizottságok, majd a fővárosi védelmi bizottság is. Eközben a Kormány az Országgyűlés összehívására intézkedik. Az alábbi ábra szemlélteti az eseménysor eszkalálódásának kezelését területi szintig.



2. ábra: Általános cselekvési vázlat és feladatrend váratlan helyzetek kezelésére[97]

Területi szint (Megyei Védelmi Bizottság, tárgyalt estben Fővárosi Védelmi Bizottság, a továbbiakban: FVB)

Az FVB a KKB operatív munkaszerve – közvetetten a kormány – irányítása alatt működik, meghatározza a védekezés területi feladatait, ellenőrzi azok végrehajtását, elrendeli a területi polgári védelmi erők bevonását, a hatáskörét meghaladó esetekben kormánydöntést kezdeményez, koordinálja a védekezésben részt vevő helyi védelmi bizottságok, polgármesterek tevékenységét.

A felvázolt helyzetben az FVB legfontosabb feladata a lakosság tájékoztatása mellett (későbbiekben kifejtve) fenntartani a tűzoltóvíz-utánpótlást és megszervezni ennek kivitelezését. Erre alkalmas lehet a Dunából történő felszívásos táplálás láncolatának kialakítása. Ezzel párhuzamosan a veszélyes anyagokkal foglalkozó üzemeket haladéktalanul tájékoztatni kell a víz összetételének megváltozásáról, és intézkedni szükséges a visszafordíthatatlan vegyi reakciók megelőzésére. Ha indokolt, az érintett üzemi és létesítményi kör működését határozatlan időre be kell szüntetni.

[97] Baán Mihály, Bors István, Csiffáry Tamás, Hári László, Kocsis Lajos, Szentes László: Magyarország védelmi igazgatása a közigazgatás új környezetében

Tekintettel az ivóvíz fertőzés miatti megbetegedések, a terrorcselekményben megsérült, valamint az egyéb tömeges megmozdulások során sérüléseket szenvedett személyek számára, egészségügyi szakállományt kell vezényelni a területileg illetékes kórházakba, elsősorban a további fertőzéses megbetegedések kezelésére történő felkészülés céljából. Budapest Főváros Kormányhivatala Népegészségügyi Főosztályának bevonásával fel kell készülni a járványokra és a szükséges ellenanyag-mennyiségre, megfelelő típusú és mennyiségű fertőtlenítőszerek beszerzésére. Szintén gazdálkodó szervezetek útján kell megszervezni ideiglenes mosdóhelyek kihelyezését, fertőtlenítését, illetve az ott keletkező szennyvíz folyamatos gyűjtését és szállítását. A fertőtlenítőszerek nagy mennyiségű szállítására és kijuttatására a honvédség szállító-, és mentesítő eszközei a legalkalmasabbak. Biológiai veszély esetén fent kell tartani a mentesítés és fertőtlenítés folytonosságát, a folyamatos utánpótlást, illetve számításba véve a behatási időt.

A Nemzeti Közlekedési Hatóság bevonásával le kell állítani a főváros területére belépő járműforgalmat és meg kell tervezni annak elkerülhetőségét, számolva az utak és hidak befogadó kapacitásával.

Fenti feladatok kiemelt létszámú rendőri biztosítást igényelnek, ezért további rendőri erőket kell vezényelni a fővárosba, a honvédség erre nem elegendő és nincs felkészítve kifejezetten rendvédelmi feladatok ellátására. A rendőri erők átcsoportosítása során kiemelt figyelmet kell szentelni a Rendőrség határvédelmi feladatainak ellátására is.

Az FVB elnöke a katasztrófavédelmi operatív feladatok ellátásához – a Fővárosi Katasztrófavédelmi Igazgatóság közreműködésével – a célnak megfelelően kialakított és felszerelt, folyamatosan üzemképes állapotban tartott vezetési pontot és annak támogatása érdekében operatív munkaszervet működtet. A védekezési feladatok végrehajtását (az FVB döntésének megfelelően) a Fővárosi Katasztrófavédelmi Igazgatóság igazgatója, vagy az által kijelölt személy hangolja össze. A fővárosi védelmi bizottság területi operatív munkaszervével folyamatosan együttműködik valamennyi érintett helyi védelmi bizottság mellett működő helyi operatív munkaszerv.

A lakosság védelmének alapvető módszerei a helyi és a távolsági védelem (kimenekítés, kitelepítés, átmeneti jellegű elhelyezés befogadó helyen, elzárkózás). Vizsgált esemény során a lakosságvédelem legindokoltabb módszere a helyben megszervezett ellátás, az alábbi feladatok végrehajtásával:

→ folyamatos ivóvíz és élelmiszer biztosítása,

→ lemosó- és fertőtlenítő anyagok biztosítása,

→ mosdó- és fertőtlenítő helyek telepítése.

Kizárólag az önellátásra képtelen, vagy különösen veszélyeztetett személyeket (például várandós, vagy csecsemőjét gondozó nők) célszerű erre a célra kialakított befogadó helyeken – a megfelelő szakellátás biztosítása mellett – elhelyezni. A főváros összes érintett vízfogyasztójának kimenekítése akadályozná a veszélyhelyzeti szolgálatok beavatkozó- és logisztikai tevékenységét, valamint lassítaná a helyreállítást is.

A BM Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: BM OKF) készíti elő a közszolgálati műsorszolgáltatók által végzett lakosság tájékoztatási háttéranyagokat, a veszély jellegére vonatkozó tájékoztatót és a követendő magatartási szabályokat tartalmazó közleményeket. A Fővárosi Katasztrófavédelmi Igazgatóság szervezi a lakosság közvetlen – helyben szokásos módon történő – tájékoztatásával kapcsolatos területi és helyi feladatokat, folyamatosan együttműködve és egyeztetve az üzemzavarban érintett kritikus infrastruktúra üzemeltetőjével, a rendőrséggel, a honvédséggel és az országos tiszti főorvossal. A veszélyhelyzeti tájékoztatás tartalma ez esetben:

→ a bekövetkezett esemény, a helyzetkezelés részcselekményei;

→ a megtett és tervezett lakosságvédelmi intézkedések;

→ az elrendelt korlátozások és az irányadó magatartási szabályok;

→ a további tájékozódási lehetőségek.[98]

[98] 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

Központi szint (Országgyűlés, Kormány, KKB)

Ahogy az már említésre került, a vizsgált esetben az Országgyűlés a Kormány kezdeményezésére terrorveszélyhelyzetet hirdet ki és felhatalmazza azt rendkívüli intézkedések bevezetésére. A terrorcselekmény létfontosságú rendszerek és létesítmények működésének megzavarásával közvetlenül veszélyezteti az élet- és vagyonbiztonságot, tárgyalt helyzetben humán járvánnyal, vagy járványveszéllyel, állatjárvánnyal, a felszíni és felszín alatti vizek haváriaszerű szennyezésével, amelyek elhárítása érdekében a Kormány – a fent bemutatott védelmi igazgatási struktúrán keresztül – rendkívüli intézkedéseket vezet be. A védekezés/beavatkozás időszakában a KKB látja el a Kormány számára történő döntés-előkészítési feladatokat. Jelen terrorcselekmény vonatkozásában a kialakult helyzet kezelése szempontjából különösen fontos a KKB jogszabály szerinti összetétele:

Elnök	belügyminiszter		
Elnökhelyettes	az elnök által kijelölt tag		
Tagok	honvédelmi miniszter	igazságügyi miniszter	
	külgazdasági és külügyminiszter	nemzetgazdasági miniszter	
	emberi erőforrások minisztere	nemzeti fejlesztési miniszter	
	földművelésügyi miniszter	Miniszterelnökséget vezető miniszter	
	miniszterelnök kabinetfőnöke által kijelölt állami vezető	belügyminiszter rendészeti államtitkára	
Állandó, tanácskozási jogú tagok	BM OKF főigazgatója	országos rendőrfőkapitány	Honvéd Vezérkar főnöke
	KKB Tudományos Tanácsának elnöke		
	KKB NVK vezetője		
	KKB adminisztratív feladatait ellátó szervezeti egység vezetője		
Elnök	Bevándorlási és Menekültügyi Hivatal főigazgatója		

döntése és meghívása alapján, tanácskozási jogú tagok	büntetés-végrehajtás országos parancsnoka
	polgári nemzetbiztonsági szolgálatok főigazgatói
	KKB NVK vezetőjének szakmai helyettese
	Országos Atomenergia Hivatal főigazgatója
	országos főállatorvos
	Országos Meteorológiai Szolgálat elnöke
	Országos Mentőszolgálat főigazgatója
	Nemzeti Adó- és Vámhivatal elnöke
	Nemzeti Média- és Hírközlési Hatóság elnöke
	Állami Egészségügyi Ellátó Központ főigazgatója,
	az Országos Vízügyi Főigazgatóság főigazgatója
	Pest Megyei Kormányhivatal kormánymegbízottja
	annak az MVB-nek az elnöke, akit a napirenden szereplő kérdés érint

3. sz. ábra: A KKB összetétele[99]

A 3. sz. ábrán szürke hátterű cellák mutatják, hogy az eseménykezelés során meghatározó szerepet betöltő szervek magasszintű képviselete biztosított. Ugyanakkor a felvázolt esemény sajátosságaira való tekintettel indokolt lenne megvizsgálni annak szükségességét, hogy a KKB ülésén állandó jelleggel, tanácskozási joggal részt vevők körébe delegálják – legalább terrorveszélyhelyzet kihirdetett időszakában – a Terrorelhárítási Központ főigazgatóját és a Nemzeti Nyomozó Iroda igazgatóját (vagy a Készenléti Rendőrség, mint felettes szerv parancsnokát).

Országos szintű koordinációt, az érintett és közreműködő szervek hatékony és eredményes együttműködését igényli az alábbi – a területi és helyi szervek által megkezdett, azok képességeit és kapacitásait feltételezhetően meghaladó – feladatok végrehajtása:
→ a csatornázási művek összes szivattyújának leállítása, a rendszer „leengedése”;

[99] A Katasztrófavédelmi Koordinációs Tárcaközi Bizottság létrehozásáról, valamint szervezeti és működési rendjének meghatározásáról szóló 1150/2012. (V. 15.) Korm. hat.

→ lakosság folyamatos és hiteles tájékoztatása, társszervek tájékoztatása a végrehajtott feladatokról, nemzetközi média valós információkkal történő ellátása;
→ tűzoltóvíz biztosítása felszívásos táplálás módszerével a Dunából több, folytonos csatornát fenntartva, vízszállítók vezénylése a főváros kerületeibe;
→ ivóvíz és élelmiszer (a kitelepítésben/kimenekítésben érintettek) biztosítása a lakosság számára, vízszállításra és kiosztásra alkalmas eszközök, tartányjárművek bevonása (élelmiszeriparból pl. tejszállítók kb. 24 tonna kapacitással);
→ kórházi ügyeletek megerősítése, felkészülés az emésztőrendszeri betegségek és fertőzések tömeges kezelésére, ellenanyag-készletek megerősítése, nemzetközi segítségnyújtás igénybevétele (UN OCHA, EU polgári védelmi mechanizmus);
→ lakossági mobil mosdó- és fertőtlenítő helyek telepítése;
→ fenti feladatok kiemelt rendőri (nem honvédségi) biztosítása;
→ fertőtlenítőszer-készletek beszerzése és kijuttatása, volumen tekintetében a dekontaminálásra csak a Magyar Honvédség képes;
→ a fővárosba belépő (civil) járműforgalom korlátozása, szükség esetén leállítása.

2. A bűnüldöző szervek feladatai

Jelen szituációban egy olyan rendkívüli eseményt kell felszámolnia a hatóságoknak, amely a folyamatos rendelkezésre állást ellehetetleníti úgy, hogy az informatikai támadás sikeres végrehajtásával okkal feltételezhetővé válik, hogy bármely ivóvíz-szolgáltatásért felelős rendszer sérülékenysége jelentős mértékben megnövekedett. A nyomozás szempontjából fontos tisztázni, hogy a kritikus infrastruktúra védelem rendszerében nevesített víz ágazaton belül, az 5 alágazatból egyet érintett közvetlenül a támadás, mégpedig az ivóvíz-szolgáltatás alágazathoz tartozó létesítményeket. Közvetetten azonban akár a felszín és felszín alatti vizek minőségének ellenőrzése, összességében pedig a vízbázisok védelme alágazatokhoz tartozó rendszerek is érintettek lehetnek.

Víz	**ivóvíz-szolgáltatás**
	felszíni és felszín alatti vizek minőségének ellenőrzése
	szennyvízelvezetés és -tisztítás
	vízbázisok védelme
	árvízi védművek, gátak

4. ábra: A víz ágazat struktúrája a magyar kritikus infrastruktúra védelmi rendszerben[100]

Egy ilyen volumenű támadássorozat szoros és hatékony együttműködést tesz szükségessé a bűnüldöző szervektől. A kialakult helyzet – a kibertámadástól kezdődően, a reggeli robbantásokon át, a károk helyreállításáig – a Rendőrség (elsősorban az Országos Rendőr-főkapitányság és a Terrorelhárítási Központ), a BM OKF és fővárosi illetékességű területi szerve, a Magyar Honvédség, a Kormányzati Eseménykezelő Központ, illetve a polgári nemzetbiztonsági szolgálatok (elsősorban a Nemzetbiztonsági Szakszolgálat és az Alkotmányvédelmi Hivatal) gyors, hatékony, szervezett és eredményes helyzetkezelését igényli, ami akár nemzetközi szervezetekkel történő együttműködésre is kiterjedhet.

A kibertámadás bekövetkezése után, a Szolgáltató IT biztonsági csoportjának jelentési kötelezettsége van a BM Ügyelet felé a 33/2011. (XII. 2.) BM utasítás[101] alapján. A nyomozást hivatalból, a Budapesti Rendőr-főkapitányság rendeli el[102], bűncselekmény elkövetésének gyanújával, a BM Ügyeletre[103] érkezett bejelentés alapján. A bűncselekmény egyediségét tekintve, az ügyet az országos rendőrfőkapitány a Készenléti Rendőrség Nemzeti

[100] a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 3. melléklete

[101] a Belügyminisztérium és a belügyminiszter irányítása alá tartozó szervek ügyeleti szolgálatai által teljesítendő tájékoztatási kötelezettség rendjéről, valamint a Kormányügyelet működéséről szóló 33 /2011. (XII. 2.) BM utasítás 4. pontja

[102] a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet 1. mellékletének 12.5 pontja

[103] A 33/2011. (XII. 2.) BM utasítás alapján az Országos Vízügyi Főigazgatóság bejelentést tesz a BM Ügyeleti Osztályon a rendkívüli eseményről, ezekkel összefüggő szükséges és halaszthatatlan intézkedések megtételéről.

Nyomozó Iroda (a továbbiakban: KR NNI) Kiberbűnözés Elleni Főosztálya hatáskörébe utalhatja, illetve a KR NNI vezetője szóban előterjesztést tehet az ügy átvételére[104].

2.1. Rendőrségi intézkedések

Jelen helyzetben a főváros ivóvíz-ellátását biztosító rendszerben történt kettős kibertámadás után, a rendőrség a Rendőrségről szóló 1994. évi XXXIV. törvény (a továbbiakban: Rtv.) a terrorcselekményre vonatkozó rendelkezéseit – kiemelt biztonsági intézkedés, csapaterő, bírói engedélyhez kötött titkos információgyűjtés – alkalmazhatja.

A helyszínen a Rendőrség az Rtv. által meghatározott kiemelt biztonsági intézkedéseket vezeti be. Eszerint a terrorcselekmény által érintett területet lezárják, ellenőrző-átengedő pontokat jelölnek ki, az oda belépőket, ott tartózkodókat ellenőrizik, ruházatukat átvizsgálják, vagy az ott tartózkodókat távozásra kötelezhetik. A hatásterületet érintő közúti, illetve tömegközlekedést irányítás alá vonják, korlátozhatják, szüneteltethetik, az ott álló járműveket elszállíttathatják, ha a kialakult helyzet indokolttá teszi[105]. Azt Rtv. 54. § szerint terrorcselekmény megakadályozására, megszakítására a rendőr lőfegyvert használhat[106]. A rendőrök továbbá csapaterőben alkalmazhatók terrorcselekmény felszámolására. A csapatszolgálat alkalmazásának szabályairól, lehetőségeiről bővebben a 11/1998. (IV. 23.) ORFK utasítás[107] rendelkezik.

A nyomozást – a hatásköri és illetékességi szabályokat figyelembe véve, tekintettel arra, hogy a tárgyalt eset terrorcselekmény – a KR NNI végzi[108]. A Rendőrség terrorizmus elleni harccal kapcsolatos feladatait ellátó szervének (Terrorelhárítási Központ) nincs nyomozati jogköre, a terrorcselekmények felderítése, megszakítása, megakadályozása mellett a

[104] a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet 9. §

[105] Rtv. 37/A. §

[106] Rtv. 54. § (1) c)

[107] a Magyar Köztársaság Rendőrségének Csapatszolgálati Szabályzata kiadásáról szóló 11/1998. (IV. 23.) ORFK utasítás

[108] a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet 13.1. és 13.2. pontjai

terrorcselekménnyel összefüggésben elkövetett más bűncselekmények megelőzéséért, felderítéséért, megszakításáért, illetve az elkövetők elfogásáért felelős[109].

2.2. A nyomozás előkészítése, információgyűjtés

A nyomozati tevékenységet alapvetően meghatározza az, hogy a felvázolt bűncselekmény szervezett módon történt elkövetése alkalmas arra, hogy a lakosságot megfélemlítse, illetve az ország társadalmi, gazdasági rendjét megzavarja, hiszen nemcsak a főváros ivóvíz-ellátását zavarták meg az elkövetők, hanem a robbantásokkal pánikot keltettek a főváros és közvetetten az egész ország lakosságában.

2.2.1. Kibertámadás

A KR NNI Kiberbűnözés Elleni Főosztály nyomozói a helyszínen megkezdik az információgyűjtést. A rendelkezésre álló információk szerint megállapítható, hogy kettős támadást történt.

→ Az első, egy számlaként álcázott pdf fájlkiterjesztésű dokumentumban egy zsarolóvírus jutott be az infrastruktúra belső levelező rendszerébe**.** Az üzenetet nem szűrte ki a biztonsági rendszer, mivel megbízható e-mail címről érkezett. A nyomozás során feltételezni kell, hogy a megbízható címhez történő hozzáférést a gyenge jelszavak feltörése és a hozzájuk tartozó gyanútlan felhasználói magatartás is eredményezhette.

→ A támadás másik eleme az emberi könnyelműséget kihasználó ajándékba küldött pendrive volt. A nyomozás megállapítja, hogy az elkövetők jól felépített legendával küldték ki az eszközt, amely szerint a címzett az adathordozót egy szakmai konferencián történő részvételét követő sorsoláson nyerte.

Összességében megállapítást nyer, hogy az ajándékként bejuttatott pendriveon egy olyan malware található, amely a Microsoft Windows operációs rendszert futtató gépeket fertőzi meg, és azokon terjed, de hatását végső soron a SCADA rendszeren fejti ki: nem csak kémkedik a célzott ipari rendszer után, hanem át is programozza azt.

[109] Rtv. 7/E. §

Bizonyítottá válik továbbá, hogy a megbízható e-mail címről kapott üzenet egy álszámlát tartalmazott, amelyet megnyitva egy ransomware került a rendszerbe. A ransomware e-mail segítségével terjed, amely mellékletként tartalmaz egy tömörített file-t (zip/rar/docm), valamint makrókat is magába foglal. Amennyiben ez megnyitásra kerül és a káros kód sikeresen lefut a rendszeren, egy távoli szerverről letöltődő ransomware kód titkosítja a dokumentumokat és más fájlokat a helyi és hálózati mappákban.[110] A zsarolóvírus titkosította a hálózati meghajtókon tárolt fájlokat és meggátolta a belső kommunikációt. A program felajánlotta, hogy 900 $ értékű Bitcoin megfizetése után szoftverhez tartozó dekódolást a felhasználó rendelkezésére bocsájtja, de ez nem teljes mértékben megbízható megoldás.

2.2.2. Fizikai támadások

A kibertámadás mellett a reggeli órákban fizikai támadások (bombarobbanások) érték a fővárost: a BKV Központ Zrt. autóbusz garázsainak közelében, valamint egy metróvonal megállójában, a reggeli csúcsforgalomban.

A fizikai támadásokról történő információszerzés érdekében azonnal intézkedni kell az érintett területek lezárására, majd vizsgálni kell a hatásterületeket. A Fővárosi Önkormányzat Rendészeti Igazgatóságtól be kell szerezni a térfigyelő kamerák felvételeit[111], majd elemezni kell azokat. A robbanás hatásfokát és károkozását vizsgálva meg kell állapítani, hogy milyen robbanószerkezetet használtak az elkövetők, illetve a bomba származási helyét, összetételét vizsgálva következtetni lehet a feltételezett elkövetőre is. Házilag készített bombák esetében az Iszlám Állam elnevezésű terrorszervezet által fenntartott Inspire és www.jihadology.net/ weboldalakat, illetve a Dabiq, vagy a Rumiyah című iszlám propaganda magazint, amelyek rendszeresen közreadnak ilyen típusú tartalmakat.

[110] http://neih.gov.hu/locky (letöltés ideje: 2017.10.03.)

[111] http://www.kozterulet-felugyelet.hu/sites/default/files/kepek/kozutkezeloi_kamerak_lista_.pdf (letöltés ideje: 2017.10.03.)

A rendőrség az érintett infrastruktúra központjában, illetőleg a városban keletkezett kaotikus állapotokra tekintettel, a Budapesti Rendőr-főkapitányság (a továbbiakban: BRFK) teljes állományát készenlétbe helyezi. Az Rtv. rendelkezései szerint a rendőrök csapaterőben alkalmazhatóak terrorcselekmény felszámolására[112], erre tekintettel intézkedéseket tehetnek a testi épséghez, a személyi szabadsághoz, a magánlakás, a magántitok és a levéltitok sérthetetlenségéhez, a személyes adatokhoz, valamint a tulajdonhoz fűződő jogok törvényben foglaltak szerinti korlátozására[113].

Terrorcselekmény elkövetése esetén a nemzetközi együttműködés keretében az Rtv. lehetőséget ad arra, hogy Magyarország területén az Európai Unió más tagállamának különleges intervenciós egysége intézkedjen. Ez az intervenciós egység egy olyan, más EU tagállam bűnüldöző egysége, amelynek speciális szakterülete a válságkezelés[114]. A rendfenntartás terrorveszélyhelyzet elrendelésekor a Magyar Honvédség (a továbbiakban: MH) egységeinek bevonásával történik. A MH egységeinek szakirányításáért és a készenlét szintjeinek fokozásáért a Honvéd Vezérkar főnöke felelős[115].

2.3. A kiberbűncselekmények nyomozási aspektusai

Európai Uniós szinten a tagállamok részéről is megfogalmazódott az igény egy megbízható, biztonságos kibertér létrehozására. Szükség volt egy közös terv megalkotására, amely a hálózati és információs rendszerek biztonsága mellett, garantálja a bűncselekmények megakadályozását, felderítését. Az Európai Unió kiberbiztonsági stratégiája[116] nemzeti szinten minimumkövetelményeket fogalmazott meg egy biztonságos kibertér létrehozása érdekében. E stratégia a követelmények között leírja a hálózati információs rendszerben illetékes nemzeti hatóságok kijelölésének szükségét, jól működő, hálózatbiztonsági vészhelyzeteket elhárító csoport (CERT – Computer Emergency Response Team) létrehozását

[112] Rtv. 58. § (1) d)

[113] Rtv.58. § (2)

[114] Rtv.62/C. §

[115] a Magyar Honvédség készenléte fenntartásának és fokozásának rendjéről szóló 30/2012. (V. 8.) HM utasítás

[116] Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságának és a Régiók Bizottságának – Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér

és a hálózat- és információbiztonságra vonatkozó nemzeti stratégia és nemzeti együttműködési terv elfogadását.

Az EU kiberbiztonsági stratégiája és a hozzá kapcsolódó irányelv[117] jogharmonizációja keretében létrejött a Kormányzati Eseménykezelő Központ[118] (GovCERT-Hungary), amely Magyarország információ-megosztó és incidens-kezelő szerve lett. Fő feladata a preventív információ-megosztás és operatív incidens-kezelés[119]. Fontos megemlíteni, hogy a Kormányzati Eseménykezelő Központ nem hatóság, nem rendelkezik nyomozati jogkörrel sem, de a nemzetgazdaság és az állami működőképesség szempontjából kritikus fontosságú informatikai rendszerek védelmében, elkövetett támadás felderítésében együttműködik a nyomozó hatóságokkal. Az azonnali reagálás képességének biztosítása érdekében a GovCert 7/24 ügyeleti szolgálatot működtet.

2.3.1. Nyomozati tevékenység és eredményei

Az elkövetők első lépésként feltehetőleg a ransomware szoftvert vásárolták meg a Darkneten. A fizetést kizárólag Bitcoinnal hajthatták végre, így valamilyen platformon kriptovalutához kellett jutniuk, amelyhez elengedhetetlen létrehozni egy Bitcoin pénztárcát. A Bitcoint átválthatjuk bármilyen nemzetközi tőzsdén, vagy akár a Budapesten található Bitcoin ATM használatával is. A nyomozás során feltárásra kerül, hogy Budapesten egyetlen ilyen ATM található a 1065. Budapest, Anker köz 1-3. szám alatt. A nyomozás keretében tehát az Anker Klubban lévő ATM elmúlt 6 havi tranzakciós listáját is elemezni szükséges[120].

A különböző innovatív és csúcstechnológiai eljárások mellett a rendőrség a kiberbűncselekmények nyomozása során alkalmazza a klasszikus nyomozati eljárásokat is. A Büntetőeljárásról szóló törvény szerint a nyomozás megindulásától kezdődően a

[117] 460/2004/EK rendelet Az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról

[118] az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény

[119] Nemzeti Kibervédelmi Intézet GovCert. http://www.cert-hungary.hu/node/1 (letöltés ideje: 2017.10.03.)

[120] Bitcoin ATM Forgalmazó (https://www.mrcoin.eu/hu/atm)

nyomozóhatóság tanú minőségben kihallgathatja az osztályon dolgozó személyeket[121], különös tekintettel azokat, akiknek sikerült feltörni az e-mail címét, illetve azt, aki megnyitotta a ransomware fájlt, továbbá azt is, aki az „ajándék" pendrive-t kapta. Ezzel a kihallgatás során a cselekményt megelőző idővonal állapítható meg.

A nyomozás keretében személyi szabadságot nem korlátozó kényszerintézkedések alkalmazhatóak, nevezetesen a lefoglalás[122] és a számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés[123]. A bűncselekmény végrehajtására használt pendrive-ot, továbbá az érintett számítógépeket lefoglalhatják, továbbá az érintett infrastruktúra információs részlegét kötelezhetik a megőrzésre, ami a bűncselekmény felderítése és a bizonyítás érdekében az információs rendszerben tárolt adat birtokosának, feldolgozójának, illetőleg kezelőjének az információs rendszerben tárolt meghatározott adat feletti rendelkezési jogának ideiglenes korlátozását jelenti.

A kiberbűncselekmények felderítésében nagy szerepet játszik IP (Internet Protocol) Cím beazonosítása. Ezt tulajdonképpen tekinthetjük a virtuális világban lévő ujjnyomnak is. Az internetszolgáltató folyamatosan tárolja a beazonosításhoz szükséges adatokat, amelyeket a nyomozó hatóság a felderítés sikere érdekében megkérhet a szolgáltatótól[124]. Az IP cím alapján történő nyomozást leginkább orientáló nyomként[125] alkalmazzák, mivel a hackercsoportok nyíltforrású WiFi használatával is elkövethetik bűncselekményüket.

Feltételezhető, hogy bizonyos körökben, az elkövetők egy ilyen sikeres kiber- és fizikai támadást nem fognak eltitkolni. A „bűnözői alvilágban" feltehetően nagy visszhangot kavar egy ilyen nagy volumenű támadás végrehajtása, ami hírnevet szerezhet az elkövetőknek. Az

[121] 1998. évi XIX. tv. a Büntetőeljárásról 79. §

[122] uo. 151. §

[123] uo. 158/A. §

[124] http://arsboni.hu/a-kiberbuncselekmenyek-nyomozasanak-uj-eszkozei/ (letöltés ideje: 2017.10.03.)

[125] A nyomozás során a hatóságok tudomására jutott IP címen keresztül nem juthatunk el közvetlenül a bűncselekmény elkövetőjéhez, mivel az adott eszközhöz több személy is hozzá férhet, illetve más helyszínen nyílt forrású internethez is csatlakozhatnak. Közvetett információként szolgálhat azonban, hogy ki, mikor és hol használhatja az adott informatikai eszközt.

ilyen forrásból származó információk megszerzésére a 2012. évi C. törvény a Büntető Törvénykönyvről, illetve a büntetőeljárásról szóló 1998. évi XIX. törvény ad felhatalmazást, az egyéb adatszerző tevékenységet, a bírói engedélyhez nem kötött, illetve bírói engedélyhez kötött titkos információgyűjtés intézménye útján. Ilyen esetekben a rendőrség a felderítés sikere érdekében fedett nyomozót alkalmazhat. A nyomozó hatóság a büntetőeljárás megindítása után bizonyítási eszközök felkutatására adatszerzést végezhet. Ennek során az ügyész engedélyével a nyomozó hatóság olyan tagját is igénybe veheti, aki e minőségét leplezi, továbbá más, bírói engedélyhez nem kötött titkos információgyűjtést is végezhet[126].

A rendőrség a bűncselekmények elkövetésének megakadályozására, felderítésére, az elkövető kilétének megállapítására, továbbá bűnmegelőzési, bűnfelderítési célok érdekében titokban információt gyűjthet[127]. A feladat teljesítése érdekében a rendőrség informátort, bizalmi személyt vagy titkosan együttműködő más személyt vehet igénybe, a nyomozás során az eljárás célját leplezheti, továbbá a rendőri jelleg leplezésére fedőokiratot állíthat ki. A rendőrség bírói engedélyhez kötött titkos információgyűjtést, titkos adatszerzést folytathat bűnüldözési célból, illetve súlyos bűncselekmények felderítésének érdekében. A tevékenység során a magánlakást titokban átkutathatja, technikai eszközök segítségével megfigyelheti, postai küldeményt ellenőrizhet, elektronikus hírközlés útján továbbított kommunikáció tartalmát megismerheti, rögzítheti, továbbá számítástechnikai eszköz vagy rendszer útján továbbított, vagy azon tárolt adatokat megismerheti, rögzítheti és felhasználhatja[128]. A titkos adatszerzést a bíró 90 napra engedélyezi, ez egy alkalommal, indítványra 90 nappal meghosszabbítható. Bár nyomozati jogkörrel nem rendelkezik, az információgyűjtésben részt vesz, továbbá speciális felderítési feladatokat lát el az Alkotmányvédelmi Hivatal. A terrorcselekmény felderítése során az államellenes vonalat keresi a tényállásban. Fontos, hogy az Alkotmányvédelmi Hivatal főigazgatója konkrét információ esetében 72 óráig engedélyezheti a titkos információgyűjtést is[129].

[126] 1998. évi XIX. tv. a büntetőeljárásról 178. §

[127] Rtv. 63. §

[128] Rtv. 69. §

[129] a Nemzetbiztonsági Szolgálatokról szóló 1995. évi CXXV. tv. 59. §

2.4. Robbantásokkal kapcsolatos nyomozati irányok

A robbantásokkal kapcsolatos nyomozás során a legfontosabb tényezők a tanúkutatás, a helyszínen rögzített anyagmaradványok, a kamerafelvételek beszerzése, a bombát elhelyező személyek felkutatása, illetve a bomba szakértői vizsgálata. Emellett a rendőrség bűncselekmények felderítése érdekében a lakosság segítségét kérheti. A robbanás helyszínének közelében lévő személyek jelentkezésére felhívást tehet, illetve a robbantó személyazonosságának felderítése érdekében nyilvánosan díjat tűzhet ki[130]. A nyomozás során azonban szelektálni kell a kapott információkat. Sok hamis/téves bejelentés és álhír is érkezhet a rendőrséghez, egyrészt a nyomravezetői díj miatt, másrészt az elkövetők védelme miatt próbálhatják meg álhírrel elterelni a nyomozást.

A hermetikusan lezárt területeken a rendőrség helyszínelői azonnal megkezdik a nyomrögzítést. A nyomrögzítés során feltételezhető, hogy DNS minta alapján azonosítható az a személy, aki a bombákat a helyszínekre helyezte.

A térfigyelő kamerák felvételeit a nyomozó hatóság az információgyűjtés során beszerzi és elemzi. A kerületi önkormányzati térfigyelő kamerákon túl, az egyéb adatszerző tevékenység során beszerezheti és megvizsgálhatja a környéken lévő hivatalok, intézmények, egyéb létesítmények tulajdonában álló biztonsági kamera felvételeit is[131]. A kamerák felvételeit használva megállapítható a bombát elhelyező személy személyazonossága, végigkövethető a haladási és távozási útvonala.

A szakértői vizsgálat megállapítja, hogy egy háztartásban elkészíthető, saját kezűleg összeállított szerkezetről van szó, amely Kínából, interneten rendelhető működési elektronikával és áramkörrel rendelkezik. A nyomozás fő irányvonalát ezek az információk adják meg: a rendelés során az elkövetőknek meg kell adniuk e-mail címüket, postai címüket, esetleg a nyomozás során a fizetési tranzakcióról is található információ.

[130] Rtv. 26-27. §

[131] Rtv. 26. §

2.5. Nemzetközi aspektus

Az internet egy olyan globális, határokat nem ismerő platform, amely nem tartozik állami felügyelet, illetve szabályozás alá. Ezért a kiberbűncselekmények nyomozását tekintve az elkövetők jelentős előnyben vannak az állami hatóságokkal szemben. A kibertér egy olyan, egész bolygót felölelő platform, amelyben nem számítanak az államhatárok, illetve a különböző állami jogi szabályozások. A felhasználók nincsenek helyhez kötve, bármikor, bárhonnan képesek elérni az adott weboldalt, illetve szervezett és fedett módon tudnak egymással kommunikálni.

2004-ben az Európai Unió a tagországok felhasználóinak védelme érdekében – a 460/2004/EK rendelet alapján – létrehozta az Európai Unió Hálózat- és Információbiztonsági Ügynökséget (ENISA – European Union Agency for Network and Information Security). Az ENISA a hálózat- és információbiztonság európai szakértői központja, amely segít az EU-nak és tagországainak abban, hogy jobban fel legyenek készülve az információbiztonsági kihívások felderítésére és kezelésére, illetve megelőzésére, továbbá kapcsolódó koordinációs feladatokat is ellát[132].

A koordinációs együttműködés az Európai Unió intézményeit is érinti. 2012-ben állandó, hálózatbiztonsági vészhelyzeteket elhárító csoportot ún. „CERT-EU”-t hoztak létre, amely az uniós intézmények, ügynökségek és szervek informatikai rendszereinek biztonságáért felel[133]. A bűnügyi szervek együttműködését európai szinten az Europol és az Eurojust koordinálja, előbbi a nyomozó hatóság, utóbbi az ügyészség szintjén. 2013-ban további Európai Uniós együttműködési megállapodások születtek, amelyek tovább segítik a nemzetközi bűnügyi szervek együttműködését. Az Európai Bizottság az Europolon belül 2013. január 1-jével létrehozta a számítástechnikai bűnözés elleni európai központot[134] (European Cybercrime Centre), amelynek feladata az Európai Unió tagállamain belül elkövetett kiberbűncselekmények gyors és hatékony felderítése.

---

[132] az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendelet

[133] Cert-EU https://cert.europa.eu/cert/plainedition/en/cert_about.html, (letöltés ideje: 2017.10.03.)

[134] Európai Unió Sajtóközlemény – Január 11-én megnyílik a számítástechnikai bűnözés elleni európai központ http://europa.eu/rapid/press-release_IP-13-13_hu.htm (letöltés ideje: 2017.10.03.)

Az Európai Unió kiberbiztonsági stratégiájában megfogalmazottak szerint, mind nemzetközi szinten, mind állami és privát szektorban tenni kell a kibertér biztonságáért, ezért az Európai Parlament és a Tanács 2016-ban kiadta a 2016/1148. irányelvet[135]. Ez útmutatást ad a tagállamok számára a minimumkövetelmények teljesítésére, mind az információs rendszerek biztonsági kihívásainak kezelésére, mind információcserére, együttműködésre vonatkozóan. E minimumkövetelmények nem csak a nemzetközi együttműködés kötelességét rögzítik, de minden tagállamnak kötelessége elfogadni egy hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiát. Ez az a dokumentum, amely meghatározza a stratégiai célokat, valamint a biztonság megteremtéséhez és fenntartásához szükséges megfelelő szakpolitikai és szabályozási intézkedéseket az információbiztonság tekintetében[136]. Továbbá minden tagállamnak kötelessége létrehozni egy, vagy több hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes hatóságot[137], illetve számítógép-biztonsági eseményekre reagáló csoportot (CSIRT), amelynek főfeladata a biztonsági események meghatározott eljárással összhangban történő hatékony kezelése[138].

Az állami hatóságoknak szükséges volt létrehozni egy új nyilvántartási rendszert, amelyben a különböző büntetőítéletekről szóló információk cseréje egységes és gyors formában történik, továbbá útmutatást ad a jogalkalmazásban.

E szükségleteket tekintve bűnügyi nyilvántartást hoztak létre a hatóságok részére, nevezetesen az Európai Bűnügyi Nyilvántartási Információs Rendszert (ECRIS). A nyilvántartás, a büntetőjogi felelősséget megállapító ítéletekre vonatkozó gyors adatcserét teszi lehetővé az államok között. A 2016-os fejlesztéseknek hála, az ECRIS nem csupán az Unión belüli állampolgárokra, hanem harmadik ország állampolgárai vonatkozóan is tárol adatot.[139].

---

[135] Az Európai Parlament és a Tanács 2016/1148. irányelve, a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

[136] uo. 7. cikk

[137] uo. 8. cikk

[138] uo. 9. cikk

[139] ECRIS – European Criminal Records Information System http://ec.europa.eu/justice/criminal/european-e-justice/ecris/index_en.htm
(letöltés ideje: 2017.10.03.)

2.6. Ransomware – Kell-e fizetni a zsarolóvírusnak?

Miután a helyi és hálózati meghajtókat megfertőzte a ransomware, felmerül a kérdés, érdemes-e kifizetni a 900 $ értékű dekódolást és bízni az egyszerű megoldásban, vagy célszerű-e más megoldásokat keresni.

A Symantech, internetbiztonsággal foglalkozó cég javaslatai alapján a fizetés abszolút nem célravezető. A Bitcoin elutalása ugyanis nem jelent biztosítékot arra, hogy a ransomware dekódolja saját magát. Ez eredhet szándékos beállításból, vagy programozási hibából is. Továbbá a fizetéssel az áldozatok jelzik a kiberbűnözők számára, hogy egy kiváló módszert találtak a pénzszerzésre, bátorítóan hat további támadások indítására, illetve tőkét biztosíthatnak számukra a további fejlesztésekre[140].

3. A magánszektor és önkormányzati szereplők helyzetkezelésbe történő bevonásának lehetőségei

A kialakult helyzetet elsősorban az erre rendelt, illetve a különleges jogrend által felhatalmazott hivatásos állományú szervek számolják fel, a helyzet összetettsége miatt ez valószínűleg meghaladja az állomány kapacitását, így érdemes mérlegelni azt, hogy más, önkormányzati- és magánszereplők bevonásával hogyan lehetne tehermentesíteni őket, illetve a lakosság ellátását több ponton-több módon biztosítani.

Jelen alfejezetben elsősorban ajánlásokat szeretnénk megfogalmazni, amelyek a hatékony elhárítást, a további problémák eszkalálódását ellensúlyozhatják.

3.1. A Polgárőrség és a Fővárosi Önkormányzati Rendészet bevonása

Tekintettel arra, hogy a Rendőrség állományának a helyszíni biztosítás, a felderítés és a különleges jogrendben foglalt feladatainak teljesítése miatt már nem jut elég kapacitása arra, hogy a lakosság körében pontos felmérést készítsen arra vonatkozóan, hogy mindenki hozzájut-e a szükséges ivóvízmennyiséghez, célszerű egyéb szerveket bevonni a helyzet

[140]Ransomware removal and protection with Symantec Endpoint Protection https://support.symantec.com/en_US/article.HOWTO124710.html (letöltés ideje 2017.10.03.)

kezelésébe. Erre a Polgárőrség és a Fővárosi Önkormányzati Rendészet tökéletesen alkalmas lehet, hiszen kerületi szintű járőrözések során fel tudják azt mérni, hol tartózkodnak olyan idős, beteg személyek vagy kiskorú gyermekek, továbbá hajléktalanok, akik akadályoztatva vannak abban, hogy az ivóvizet biztosító pontokra eljussanak. Az önkormányzati rendészek gépjárműveikkel és alapos helyismeretükkel segíthetik az ivóvíz hatékonyabb szétosztását, illetve a mentőszolgálatot tájékoztathatják olyan súlyos betegek tartózkodási helyéről is, akik valamilyen oknál fogva nem tudtak egészségügyi intézményekbe eljutni.

A Polgárőrség és a Fővárosi Önkormányzati Rendészet fent említett feladata közé érdemes beépíteni az állatmenhelyek látogatását is, hiszen nem csak az emberek, az állatok is tömegesen betegedhetnek meg, és a jelentős számú elhullásuk ismételten egy járványügyi kockázat lehet, ezért ezen szervezetek számára is biztosítani kell a tiszta ivóvizet, illetve célszerű fokozottabban figyelni, szükség szerint begyűjteni a kóbor állatokat, ami gátat szabhat a fertőzések további terjedésének.

3.2. A Szolgáltató informatikai rendszerének izolálása, a károk helyreállítása

A támadást észlelve a Szolgáltató – bejelentési kötelezettségeinek eleget téve[141] – azonnal megkezdi a károk felmérését és a rendszer izolációját a GovCERT szakmai koordinációjával. A Szolgáltató megfertőzött rendszerének teljes hálózati leválasztása szükséges, ami után párhuzamosan meg kell kezdeni az azonnali biztonsági mentésből való visszaállítást és rendszerelemzést. Ez a lépés feltárja, milyen mélységben érintette a kibertámadás a rendszereket, így csökkentve a lefedetlen időszakot. A biztonsági mentés helyreállítása előtt mindenféleképpen meg kell vizsgálni, hogy fertőzött állomány került-e eltárolásra, ezáltal elkerülhető a visszafertőzés veszélye.

Javasoljuk egy független internetkapcsolat biztosítását (akár önálló modemmel rendelkező mobil internet) is, amelyhez a felhasználói hozzáférést korlátozni kell, tehát csak meghatározott vezetői szinten túl lehet azt kapcsolattartásra használni. A dolgozók internethasználatát az izoláció során korlátozni kell, amely elejét veheti a vírusok további terjesztésének, illetve a belső, bizalmas információk kiszivárogtatásának egyaránt.

[141] A GovCert 7/24 órás ügyelete, az Országos Vízügyi Főigazgatóság, illetve a BM Ügyelet felé.

A Szolgáltató azon rendszereinél, ahol még nincs a támadásnak nyoma, szintén célszerű egy rendszerelemzést végrehajtani megelőzésképpen, biztonsági intézkedésként. Ha nem található vírus, a biztonsági mentéseket haladéktalanul meg kell kezdeni, valamint azok külső, hálózatról leválasztott meghajtókon való tárolásával, duplikálásával az adatokat biztosítani. Erre a célra bár különösen költséges, de a legalkalmasabb a szalagos mentőegység lehet, amelyeket fokozott figyelemmel és körültekintéssel kell tárolni, valamint kezelni.

3.3. A médiaszolgáltatókra háruló feladat

Azon túl, hogy terrorveszélyhelyzet lehetővé teszi azt, hogy a Kormány ellenőrizheti az internet-, levél-, és postaforgalmat, valamint az állami médiát kötelezheti a kormányzati állásfoglalások kiadására, a pánikhelyzet kialakulásában nagy szerepe van a bulvársajtó és a médiaszolgáltatók egyéni felelősségének is.

A támadások vezető hírként fognak szerepelni és az idő előrehaladtával egyre több és több adat fog napvilágot látni az eseményekről, mert a lakosság folyamatos információs igényét a gyors cikkmegjelentetésekkel szeretnék kielégíteni. Ez a támadás harmadik lépésének, az álhírek terjesztésének és a dezinformációs műveleteknek kedvez.

Az állami médián keresztül közölt állásfoglalásokon, a sajtótájékoztatók tartásán túl érdemes lenne fontolóra venni azt, hogy a közösségi oldalakat is fel lehet használni, mint a hivatalos, megbízható hírek minél nagyobb közönséghez történő eljuttatási fórumát, hiszen mind a BM OKF, mind az ORFK rendelkezik Facebook oldallal, amelyen a hírek – felhasználói megosztások által – gyorsan, de mégis hiteles formában terjedhetnek.

Összegzés

A fenti helyzetet, valamint megoldási dimenziókat látva megállapítást nyert az, hogy bár Magyarország terrorfenyegetettsége alacsonyabb, mint más, nyugat-európai országoké[142], egy ilyen típusú támadás kivitelezésének valószínűsége – részint a viszonylag „könnyű" kivitelezésnek, részint pedig az informatikai támadási lehetőségek sebezhetőségekből eredő térnyerésének köszönhetően – nem elhanyagolható.

A XXI. század információs társadalmában látnunk kell a mindennapos életvitelünket veszélyeztető tényezőket. Számolnunk kell az emberi tényezővel mind az elkövetők, mind az elszenvedők vonatkozásában. A kibertérben rejlő lehetőségek ártó szándékú felhasználása a modern kor egyik legnagyobb kihívásává fogja kinőni magát. Ennek ellensúlyozása érdekében – ahogy a felvázolt eseménysorozat is mutatja – nem csak az állami szféra, a beavatkozó, elhárító és nyomozó hatóságok felkészültségét kell a lehető legmagasabb szintre fejleszteni, hanem a hétköznapi emberek gondolkodásmódját is. A tudatosítás, az „informatikai önvédelmi képesség" kialakítása és fokozása kiemelt célként kell, hogy szerepeljen az olyan stratégiai szintű dokumentumokban például, mint Magyarország Kiberbiztonsági Stratégiája. Mind állami, mind magánszektor vonatkozásában erősíteni – ha szükséges, akkor kötelezni – kell az informatikai tudatosító kampányok során az eszközök napi használatából fakadó veszélyekre vonatkozó ismereteket. Az emberi hiszékenység, a tájékozatlanság csökkentésére irányuló kezdeményezések útján el kell érni, hogy a következő években csökkenjen a szcenárióban bemutatott helyzetek kivitelezhetősége.

Természetesen a szerzők is tisztában vannak azzal, hogy nem egy-egy tudatosító előadás hozza meg az eredményt, éppen ezért olyan egyszerű, közérthető, kis anyagi vonzattal járó informatika biztonsági oktatási koncepciót ajánlunk mind az állami, mind a magánszektor számára, amelyek egyszerűen beépíthetők minden munkatárs napi rutinjába és amelyeket a magánéletükben is sikerrel és könnyedén alkalmazhatnak. Ezt azért tartjuk fontosnak, mert – ahogyan a tanulmányunkból is kiderült – az ártó szándékú fél sem munkaidőben fogja támadni a célpontot, úgy, mint az adott szervezethez vagy céghez tartozó kollégát, hanem az

[142] A brit külügy 2017 májusában készült fenyegetettség felmérése alapján. http://www.telegraph.co.uk/travel/maps-and-graphics/Mapped-Terror-threat-around-the-world/ (letöltés ideje: 2017.10.10.)

egyénhez, a magánemberhez próbál minél közelebb kerülni, hogy aztán azt kiismerve fel tudja használni céljai eléréséhez.

Célszerűnek tartjuk azt is, hogy a munkavállalókat a kötelező dolgozói oktatásokon túl véletlenszerűen ellenőrizzék akár az IT biztonsági osztályhoz tartozó kollégák, akár a felettesek, annak tekintetében, hogy a megtévesztésre mennyire hajlamosak, illetve mennyire fogékonyak akár a jelen tanulmányban ismertetett social engineering technikák tekintetében.

A levezetett feltételezés alapján áttekintettük a beavatkozó és nyomozati szervek reagáló-képességét biztosító jogszabályi környezetet is. Ez alapján megállapítottuk, hogy a különleges jogrend általi felhatalmazások érvényesítésével és a rendkívüli intézkedések bevezetésével a lakosság alapellátásának biztosítása megoldottnak tűnik, ugyanakkor számolni kell azzal, hogy egy ilyen komplex támadás meghaladhatja az erre rendelt erők képességeit. Különösen igaz lehet ez abban az esetben, amikor az általános rendőrségi feladatok ellátására létrehozott szerv eleve rendkívüli leterheltségnek van kitéve a tömeges bevándorlás okozta válsághelyzetből fakadó, folyamatosan végrehajtandó feladatok által. Mindez jelentősen befolyásolhatja az ilyen mértékű támadás kezelésével járó, elsősorban a közrend fenntartása érdekében előirányzott erőátcsoportosítási lehetőségeket, tekintettel arra, hogy a közbiztonság garantálása – a határvédelmi és a terrorcselekménnyel kapcsolatos feladatok mellett is – alaprendeltetésből fakadó kötelezettség az egész ország területére vonatkozóan.

A jogszabályi környezet elemzése során felmerült, hogy az ivóvíz-ellátás szabotálása miatt kialakuló helyzet következményeinek kezelésére az Alaptörvény veszélyhelyzeti tényállásának kihirdetése lehet a válasz, annak érdekében, hogy a gyors és hatékony döntéshozatal, illetve az azonnali intézkedések bevezetése megvalósítható legyen. Ugyanakkor a „klasszikus” terrorcselekmények (robbantások) elkövetése automatikusan feltételezi az Alaptörvény terrorveszélyhelyzeti tényállásának kihirdetését. Ahogy az a kialakult krízis kezelésének dimenziói c. fejezetben említésre került, fennáll a lehetősége, hogy a helyzetet két különleges jogrendi állapotra jellemző közigazgatási eszközökkel kezelik. Érdemes lenne emiatt megvizsgálni az ehhez hasonló, sajátos körülmények között szerveződő döntés-előkészítő és döntéshozó mechanizmust, valamint a rendvédelmi szervek hatáskör-telepítésének és az így kialakulható kollíziók feloldásának jogi és gyakorlati megoldásait, a párhuzamok és duplikációk elkerülése érdekében. Szintén a jogszabályi környezet vizsgálata közben állapítottuk meg, hogy a jelenlegi szabályozás szerint a KKB

ülésein résztvevők közvetetten rendelkeznek a terrorelhárítással kapcsolatos információkkal (belügyminiszter, országos rendőrfőkapitány, polgári nemzetbiztonsági szolgálatok főigazgatói). A pontos és szükség esetén részletekbe menő információk rendelkezésre állása érdekében megfontolandónak tartjuk terrorveszélyhelyzet kihirdetett időszakában legalább a TEK főigazgatójának jelenlétét jogszabályi úton is biztosítani.

Tanulmányunk forgatókönyvének döntő tényezőjeként azonosítottuk a pánik kialakulását, amelynek elsődleges táptalaját az álhírek, valamint a nem megbízható, ellenőrizetlen forrásból származó információk adják. A folyamatos, hivatalos forrásokból származó lakosságtájékoztatás megakadályozhatja ezt, valamint az ebből fakadó tömeges atrocitásokat, amely összességében az elkövetők végső célkitűzéseként aposztrofálható: a belső rend, a közbizalomba vetett hit megingatása. Meglátásunk szerint ennek felelősségét a médiaszolgáltatóknak is kell magukra vállalni és – bár a minél többet olvasott cikkek és eladott lapszámok jelentik bevételük fő forrását, amelyet a figyelemfelkeltő cikkekkel lehet elérni – mérlegelniük azt, hogy ebben a rendkívüli helyzetben a tényszerű, lényegre törő, a lakosság számára hiteles tények közlését helyezzék előtérbe.

Összességében megállapítottuk, hogy a hatályos jogszabályi környezet és a hatóságok rendelkezésére álló képességek alapján a feltételezett támadás következményeinek kezelése – feszített tempóban, a nemzetgazdaság tartalékainak igénybe vétele mellett, a magánszektor bizonyos mértékű bevonásával – eredményesen kezelhető. Bár az önkormányzati rendészeti szervek, valamint a rendőrség közti együttműködésre az elmúlt évek során egyre több példát látunk, véleményünk során a jövőben célszerű lenne hasonló gyakorlatokba belevonni őket is.

Irodalomjegyzék

Nemzetközi szabályozók

1. Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságának és a Régiók Bizottságának – Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52013JC0001 (letöltés ideje: 2017.10.03.)
2. 460/2004/EK rendelet az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:HU:HTML (letöltés ideje: 2017.10.03.)
3. Az Európai Parlament és a Tanács 2016/1148. Irányelve, a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről http://ec.europa.eu/justice/criminal/european-e-justice/ecris/index_en.htm (letöltés ideje: 2017.10.03.)

Jogszabályok

4. Magyarország Alaptörvénye
5. 1994. évi XXXIV. törvény a Rendőrségről
6. 1995. évi CXXV. törvény a Nemzetbiztonsági Szolgálatokról
7. 1998. évi XIX. törvény a büntetőeljárásról
8. 1999. évi LIV. törvény az Európai Unió bűnüldözési információs rendszere és a Nemzetközi Bűnügyi Rendőrség Szervezete keretében megvalósuló együttműködésről és információcseréről
9. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

10. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
11. 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról
12. 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről
13. 33/2011. (XII. 2.) BM utasítás a Belügyminisztérium és a belügyminiszter irányítása alá tartozó szervek ügyeleti szolgálatai által teljesítendő tájékoztatási kötelezettség rendjéről, valamint a Kormányügyelet működéséről
14. 30/2012. (V. 8.) HM utasítás a Magyar Honvédség készenléte fenntartásának és fokozásának rendjéről
15. A Katasztrófavédelmi Koordinációs Tárcaközi Bizottság 1/2016. (IV.29.) határozata a Katasztrófavédelmi Koordinációs Tárcaközi Bizottság ügyrendjének és a Katasztrófavédelmi Koordinációs Tárcaközi Bizottság Nemzeti Veszélyhelyzet-kezelési Központ ügyrendjének elfogadásáról.

Tanulmányok

16. BAÁN Mihály, BORS István, CSIFFÁRY Tamás, HÁRI László, KOCSIS Lajos, szerk. SZENTES László: Magyarország védelmi igazgatása a közigazgatás új környezetében. Zrínyi Kiadó, Budapest, 2014.
17. Cisco 2017 Midyear Cybersecurity Report. Published July 2017. https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1456403/Cisco_2017_Midyear_Cybersecurity_Report.pdf?elqTrackId=f6ccd8439e9945639096a9846044695a&elqaid=5897&elqat=2 (letöltés ideje: 2017.10.07.)
18. DARUKA Norbert: A bűnös célú/terror jellegű robbantások és az ellenük való védekezés lehetőségei, különös tekintettel a tűzszerész feladatok ellátására. Doktori (PhD) értekezés, http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2014/daruka_norbert.pdf (letöltés ideje: 2017.08.26.)

19. Keep Security The Most Common Passwords of 2016.
https://keepersecurity.com/public/Most-Common-Passwords-of-2016-Keeper-Security-Study.pdf
(letöltés ideje: 2017.10.05.)

20. KOVÁCS László–KRASZNAY Csaba: A digital Mohács - IN: Nemzet és Biztonság: Biztonságpolitikai szemle (Spec. Issue Winter) pp. 49-59
http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf
(letöltés ideje: 2017.09.30.)

21. KOVÁCS László–SIPOS Marianna: A Stuxnet és ami mögötte van – Tények és a cyberháború hajnala. IN: Hadmérnök V. Évfolyam 4. szám pp. 163-172. (2010.)
http://hadmernok.hu/2010_4_kovacs_sipos.pdf
(letöltés ideje: 2017.10.07.)

22. William Powel: The Anarchist Cookbook, Barricade Books Inc. (1971.)
https://uniteyouthdublin.files.wordpress.com/2015/01/anarchist-cookbook-william-powell.pdf
(letöltés ideje: 2017.08.22)

Internetes források

23. http://vizmuvek.hu/files/public/Fovarosi_vizmuvek/tarsasagi_informaciok/FVM_Eves_Jel_HUN.pdf
(letöltés ideje: 2017.08.12.)

24. http://okoenergia.hu/vizfogyasztasi-statisztika/
(letöltés ideje: 2017.10.05.)

25. http://www.orientpress.hu/cikk/2017-08-02_a-fovaros-kuzd-a-hoseggel
(letöltés ideje: 2017.10.05)

26. https://www.budapestinfo.hu/hu/szallashely-statisztika---minden-mutato-emelkedett-2017-elso-feleveben-budapesten-is
(letöltés ideje: 2017.08.26)

27. http://vizmuvek.hu/jubileum/
(letöltés ideje: 2017.08.22.)
28. https://sg.hu/cikkek/it-tech/96470/lecsereli-informatikai-halozatat-a-fovarosi-vizmuvek
(letöltés ideje: 2017.08.22.)
29. http://www.information-age.com/risks-facing-industrial-control-systems-reach-all-time-high-123467315/
(letöltés ideje: 2017.10.07.)
30. http://invenioit.com/security/ransomware-statistics-2016/
(letöltés ideje: 2017.10.09.)
31. http://budapest.hu/Documents/varosfejlesztesi_koncepcio_2011dec/11_Kozmuvek_jav.pdf
(letöltés ideje: 2017.10.08.)
32. Epidemiológiai Információs Hetilap (2006. 23. szám pp. 291-296.) http://epa.oszk.hu/00300/00398/00208/pdf/00208.pdf
(letöltés ideje: 2017.10.07.)
33. http://metros.hu/vonal/jellemzok_m2.html
(letöltés ideje: 2017.10.01.)
34. http://hvg.hu/itthon/20160926_Hidegverrel_lepett_at_aldozatain_a_robbanto (letöltés ideje: 2017.10.01.)
35. http://metros.hu/vonal/jellemzok_m3.html
(letöltés ideje: 2017.10.01.)
36. https://azelin.files.wordpress.com/2010/06/aqap-inspire-magazine-volume-1-uncorrupted.pdf
(letöltés ideje: 2017.08.27)
37. http://hvg.hu/itthon/20161205_baleset_miatt_nem_jar_a_2es_metro
(letöltés ideje: 2017.08.12.)
38. http://www.thehindu.com/news/national/what-is-not-in-my-name-all-about/article19194499.ece
(letöltés ideje: 2017.10.07.)
39. http://neih.gov.hu/locky
(letöltés ideje: 2017. 10. 03.)

40. http://www.kozterulet-felugyelet.hu/sites/default/files/kepek/kozutkezeloi_kamerak_lista_.pdf
(letöltés ideje: 2017.10.04.)
41. http://jihadology.net/category/inspire-magazine/
(letöltés ideje: 2017.10.08.)
42. http://jihadology.net/
(letöltés ideje: 2017.10.08.)
43. https://clarionproject.org/docs/islamic-state-dabiq-magazine-issue-7-from-hypocrisy-to-apostasy.pdf
(letöltés ideje: 2017.10.08.)
44. https://clarionproject.org/factsheets-files/Rumiyah-ISIS-Magazine-1st-issue.pdf (letöltés ideje: 2017.10.08.)
45. https://www.mrcoin.eu/hu/atm
(letöltés ideje: 2017.10.03.)
46. https://cert.europa.eu/cert/plainedition/en/cert_about.html
(letöltés ideje: 2017.10.03)
47. http://europa.eu/rapid/press-release_IP-13-13_hu.htm
(letöltés ideje: 2017.10.03.)
48. https://support.symantec.com/en_US/article.HOWTO124710.html
(letöltés ideje: 2017.10.03.)
49. http://www.telegraph.co.uk/travel/maps-and-graphics/Mapped-Terror-threat-around-the-world/
(letöltés ideje: 2017.10.10.)