7. fejezet

Nyomásgyakorlás a kritikus információs infrastruktúrák támadásán keresztül

A Digital Pearl Harbortól a digitális ökoszisztéma teljes támadásáig

Kovács László

Bevezetés

Digitálissá vált világunk azokra az eszközökre és rendszerekre épül, amelyeket összefoglaló néven kritikus infrastruktúráknak hívunk. Ezekben számos infokommunikációs rendszer található, amelyek szintén kritikusak vagy más szóval létfontosságúak a 21. század társadalmának működéséhez. A kritikus információs infrastruktúrák testesítik meg korunk legjellemzőbb vonását, amikor digitális ökoszisztémáról beszélünk.

A digitális kor és az annak idegrendszereként is felfogható kritikus információs infrastruktúrák az 1970-es évek óta hatalmas fejlődésen mentek keresztül. Ma nyugodtan kijelenthetjük, hogy nincs olyan területe az életünknek, ahol ne lennének jelen, vagy legalább ne lenne hatásuk ezeknek az infrastruktúráknak, illetve azok egyes elemeinek. A digitalizációnak és az információtechnológiai forradalomnak köszönhetően a mai terminológiával élve fizikai vagy hagyományos infrastruktúrák kiegészülnek olyan információs rendszerekkel, eszközökkel és berendezésekkel, amelyek szintén elengedhetetlen részei a mindennapjainknak. Ebből következően ezek az információs infrastruktúrák szintén nélkülözhetetlenek, azaz kritikusak, létfontosságúak. Ráadásul „hagyományos" infrastruktúráink jelentős részében ezek megtalálhatóak, hiszen azok vezérlése vagy irányítása ezeken a nélkülözhetetlenné vált információs rendszereken keresztül valósul meg.

A fentiek azonban nemcsak olyan előnyöket hordoznak magukban, mint például a globális szolgáltatások és azok napi 24 órás elérése, hanem bizony

https://doi.org/10.36250/01079_07

https://orcid.org/0000-0002-6403-0650

hatalmas kihívás elé is állítják magát a társadalmat is, hiszen ezeknek az infrastruktúráknak – lévén létfontosságúak – minden nap minden percében zavartalanul és kielégítő módon kell működniük ahhoz, hogy a társadalom különböző funkciói működjenek.

Az viszont már az 1990-es években világossá vált, hogy az infokommunikációs rendszerek hatalmas ütemű fejlődését azok védelme nem mindig, vagy csak késve tudja követni. Ezek a rendszerek, legyen szó kritikus infrastruktúráról vagy kritikus információs infrastruktúráról, sebezhetőek, sőt önmagukban is számos sérülékenységet hordozhatnak. Ezeket pedig ártó szándékkal – akár előre nem is mindig jelezhető módon és nem megjósolható időben – valakik ki fogják használni.

Anakronisztikus ellentétnek tűnik tehát az a kettősség, amely egyrészt ezen rendszerek létfontosságúvá válásában, másrészt azok támadhatóságában jelentkezik. Ha ezek a rendszerek valóban elengedhetetlenek a mindennapi élet működőképességének fenntartásában, akkor azok működésbeli kiesése nem megengedhető, viszont ennek biztosítása majdhogynem lehetetlen vállalkozásnak tűnik.

Több olyan elképzelt forgatókönyv is született, amely pont a fent említett, a kritikus infrastruktúrákat célzó támadásokat és azok hatásait kívánta megvizsgálni. Ezek közül a Digitális Pearl Harbor *(Digital Pearl Harbor)* a 2000-es évek elején az Amerikai Egyesült Államokban, a Digitális Mohács pedig a 2000-es évek végén Magyarországon született. Mindkét forgatókönyv meglehetősen nagy, de sok esetben vegyes véleményeket kiváltó visszhangot kapott. Jelen fejezetünk arra keresi a választ, hogy a két elképzelt forgatókönyvben is felvázolt támadássorozattal valóban nyomást lehet-e gyakorolni egy országra ma, a 21. század első évtizedeiben.

A kritikus infrastruktúrák és a kritikus információs infrastruktúrák, valamint azok szerepe

Az Európai Unió 2020 végén megjelent új kiberbiztonsági stratégiája egyenesen globális kockázatnak tekinti a kritikus infrastruktúrák rosszindulatú támadását. A stratégia rámutat, hogy az internet decentralizált kialakítású és felépítésű, egyértelműen meghatározható központi szervezet vagy struktúra nélkül, amely hozzájárul a (hálózati) forgalom exponenciális növekedéséhez, miközben viszont állandósultak a rosszindulatú – sok esetben célzott – támadások. Ugyanakkor az internet működése szempontjából olyan kiemelten fontos szolgáltatások,

mint többek között a DNS (*domain name system,* domén név rendszer) vagy az alapvető szolgáltatásokat nyújtó megoldások egyre inkább néhány magáncég tulajdonában koncentrálódnak. Mindez „[…] az európai gazdaságot és társadalmat kiszolgáltatottá teszi olyan zavaró geopolitikai vagy technikai események számára, amelyek érintik az internet lényegét vagy ezek közül egy vagy több társaságot. A világjárvány miatt megnövekedett internethasználat és a változó szokások még inkább rávilágítottak a digitális infrastruktúrától függő ellátási láncok törékenységére."[1]

Természetesen az olyan nemzetközi szervezetek, mint az Európai Unió vagy akár az egyes országok nem 2020-ban vették először górcső alá a kritikus infrastruktúrákat, illetve a kritikus információs infrastruktúrákat, valamint azok védelmének szükségességét.

Az Európai Unióban már a 2000-es évek elején megkezdődött – nemcsak a gondolkodás, hanem – a kritikus infrastruktúrák védelmével foglalkozó gyakorlati és jogszabályalkotó munka. Az olyan előkészítő munkák után, mint például az EU zöld könyve – hivatalos címén *Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról*[2] –, az unió 2006-ban jelentette meg az úgynevezett kritikusinfrastruktúra-védelem európai programját (*European Programme for Critical Infrastructure Protection,* röviden: EPCIP). Az EPCIP valódi áttörésként értelmezhető, hiszen egységes szerkezetbe foglalta az EU gondolkodását a területen, valamint kötelező érvényű szabályozást jelentett a tagállamok számára.[3]

> „Az EPCIP lefektette a kritikus infrastruktúrák védelmének növelését célzó minden olyan tevékenységnek az általános kereteit, amelyek az EU minden tagországára, valamint minden ágazatra érvényesek. A korábbi irányelvektől eltérően az EPCIP már nemcsak a terrorizmust tekintette fő fenyegetésnek, hanem az egyéb bűncselekményeket, illetve a természeti és ipari katasztrófákat is ide sorolta."[4]

Az európai uniós szabályozási munka, és nem utolsósorban a kritikus infrastruktúrák kitettsége felismerésének eredményeként hazánkban is megkezdődött a terület szabályozása. Az első kézzelfogható hazai szabályozó 2008-ban jelent

[1] JOIN(2020) 18 final. Közös közlemény az Európai Parlamentnek és a Tanácsnak. Az EU kiberbiztonsági stratégiája a digitális évtizedre.

[2] COM(2005) 576. Az Európai Közösségek Bizottsága: *Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról.*

[3] European Commission: *European Programme for Critical Infrastructure Protection* (2006).

[4] Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018. 223.

meg kormányhatározat formájában.[5] Ennek egyik legnagyobb eredménye – azon kívül, hogy megjelent, és ezzel nem csak bizonyította a terület fontosságát, hanem el is kezdődött a védelem szabályozott, nemzeti szinten is koordinált módú szervezése – az volt, hogy számbavette és felsorolta azokat az infrastruktúra-ágazatokat és -alágazatokat, amelyek valóban kritikusnak tekinthetők Magyarország vonatkozásában is.

Hazánkban a kritikusinfrastruktúra-védelem területén az igazi áttörést azonban 2012 hozta meg. Ekkor jelent meg hosszas előkészítő munka után a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, amelyet röviden csak kritikus-infrastruktúra-törvényként vagy a hivatalos címe első két szava alapján rövidítve csak Lrtv.-ként azonosítunk.[6] Meg kell jegyezni, hogy jelen fejezetben is – a törvényi szabályozás által használt létfontosságú rendszerek és rendszerelemek kifejezések mellett – a kritikus infrastruktúra, illetve a kritikus információs infrastruktúra terminológiát használjuk azok elterjedtsége miatt.

Az Lrtv. szerint a kritikus infrastruktúra

> „meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna."[7]

Fontos megemlíteni, hogy a törvény meghatározza az európai értelemben vett kritikus infrastruktúra fogalmát is: „a törvény alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése jelentős hatással lenne – az ágazatokon átnyúló kölcsönös függőségből következő hatásokat is ideértve – legalább két EGT-államra."[8]

E meglehetősen bonyolult megfogalmazás azonban leegyszerűsítve azt takarja, hogy a 21. század társadalmi működése feltételez számos olyan rendszert, amelyek nélkül nem, vagy csak nagyon nehezen tudnánk elképzelni életünket. Ennek megfelelően valóban teljes joggal használhatjuk a *létfontosságú*

[5] 2080/2008. (VI. 30.) Kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.

[6] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

[7] 2012. évi CLXVI. tv. 1. § *f.* pont.

[8] 2012. évi CLXVI. tv. 1. § *c.* pont.

jelzőt, hiszen ezeknek a rendszereknek, vagy akár ezek egyes rendszerelemeinek a folyamatos működése ma már nem csak a kényelem és az életminőség javításában jelentkezik, hanem ezek nélkül gyakorlatilag nem jutnánk hozzá azokhoz a szolgáltatásokhoz, amelyek a mindennapi életünk alapjai. Nagyon leegyszerűsítve: e rendszerek nélkül emberek sokaságának az élete kerülne – akár már rövid időn belül is – veszélybe.

Az említett rendszerek azonban ma már nemcsak fizikai objektumok, hanem nagyon sok esetben információs vagy infokommunikációs rendszerek, amelyek önmagukban vagy az adott kritikus infrastruktúra részeként szintén kritikusak, azaz működésük létfontosságú a társadalom egésze szempontjából. Az említett hazai kritikusinfrastruktúra-védelmi törvény végrehajtási rendeleteként kiadott kormányrendelet meghatározza a kritikus információs rendszer és létesítmény fogalmát is: „a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek.”[9] Ez a meghatározás nagyon jól összefoglalja, hogy ma már nemcsak a hagyományos értelemben vett infrastruktúrák, hanem az ezek vezérlését, működését ellátó információs rendszerek közül önmagában is nagyon sok kritikus infrastruktúrának minősül. A jogszabály 10 fő ágazatot – energia, közlekedés, agrárgazdaság, egészségügy, társadalombiztosítás, pénzügy, infokommunikációs technológiák, víz, honvédelem, közbiztonság-védelem – és több mint 30 alágazatot határoz meg kritikus infrastruktúraként.[10]

A kritikus információs infrastruktúrák európai szabályozásában 2016-ban született meg az úgynevezett NIS direktíva azzal a legfontosabb feladattal, hogy olyan egységes követelményrendszert határozzon meg, amely az összes európai uniós tagországban garantálhatja azt, hogy a hálózati és információs rendszerek egyformán biztonságosak legyenek.[11] Legalábbis elvileg. Ugyanis a NIS megalkotását pont az a felismerés indukálta, hogy az EU tagországainak információs rendszerei eltérő fejlettségűek, és eltérő biztonsági állapotban vannak. Ugyanakkor ezek a rendszerek a hálózatokon keresztül összeköttetésben

[9] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról. 1. § 3. pont.

[10] 1. melléklet a 2012. évi CLXVI. törvényhez.

[11] 2016/1148. Az Európai Parlament és a Tanács (EU) irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

állnak egymással, így az egyik tagország hiába rendelkezik megfelelő biztonsági szintű információs rendszerrel, ha egy másik ország kevésbé biztonságos rendszerén keresztül az támadhatóvá válik. A NIS nagy előrelépés lehet abban, hogy a tagországok egyformán értékeljék a hálózati és információs rendszerek biztonságát, legyen – többé-kevésbé – homogén és egységes stratégiájuk ezek megvédésére, illetve a biztonságuk folyamatos fejlesztésére. A NIS meghatározza azokat a legfontosabb kritikus információs infrastruktúrákat, amelyek védelme az egész unióban a lehető legmagasabb szinten meg kell hogy valósuljon. Ezek az infrastruktúrák, illetve ágazatok – nem meglepő módon – sok esetben egybeesnek a hazai kritikusinfrastruktúra-ágazatokkal. Ezek az ágazatok: az energia, a közlekedés, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, az ivóvízellátás és -elosztás, valamint a digitális infrastruktúra. A felsorolásból jól látszik, hogy ezek mindegyike olyan szolgáltatás, illetve rendszer, amely határokon átnyúlik, és úgy hálózza be a tagországok mindegyikét, hogy gyakorlatilag az összes EU-országot összeköti egymással. Ezek esetében a(z) – határokon átnyúló – interdependencia, illetve az ágazatok jellegéből adódó gazdasági és társadalmi működés függősége nem szorul magyarázatra. Ennek megfelelően a közös elvek mentén történő egységes, a biztonság magas szintjének megvalósulására irányuló szabályozás szükségessége teljes mértékben indokolt. A probléma azonban a szabályozás betartásának az ellenőrzésében van, hiszen abból a szempontból nagyon liberális ez a szabályozás.

Ugyanakkor azt ma már világosan lehet látni, hogy az egyes kritikus információs infrastruktúrákon belül is vannak olyan rendszerek, rendszerelemek vagy akár szolgáltatások, amelyek nélkül maga az adott rendszer sem lenne képes működni. Az internet esetében ilyen szolgáltatás például a DNS-szolgáltatás. A doménnévrendszer-szolgáltatás nélkül rövid ideig még működik az interneten elérhető szolgáltatások egy része, de hiányában hamar érezhető szolgáltatáskiesés lép fel, hosszabb idő után pedig már nagyon nehézkesen vagy egyáltalán nem érhetők el a szolgáltatások. A DNS-rendszer támadására, illetve annak kísérletére több alkalommal volt példa, az egyik legsikeresebb támadás 2016 októberében következett be az Egyesült Államokban. Ekkor a Dyn nevű keleti parti DNS-szolgáltató szervereit érte olyan DDoS-támadás (*distributed denial of service,* elosztott túlterheléses támadás), amely miatt a cég szolgáltatásai leálltak. Jól felépített támadássorozat volt több hullámban, amelyben több tízezer, egyes elemzések szerint akár százezer[12] IoT- (*Internet of Things,* a dolgok internete)

[12] Trend Micro: Operation Pawn Storm: Fast Facts and the Latest Developments (2016. január 16.).

eszköz vett részt, amelyek túlnyomó részben Mirai *malware*-rel fertőződtek meg korábban. A bekövetkezett szolgáltatáskiesés messze túlmutatott az Egyesült Államok határain,[13] mert számos Ázsia irányába menő IP-cím-tartománynév feloldása is ezeken a megtámadott szervereken keresztül valósult meg, így azok a szolgáltatások is elérhetetlenné váltak.[14]

Az egyes kritikus információs infrastruktúrákon belül meglévő függőségre a DNS mellett másik például a felhőszolgáltatások adódnak. Azok a felhőszolgáltatások, amelyek a nagy közösségi platformoknak nyújtanak létfontosságú háttértámogatást, szintén kritikusak. Az ezekben a szolgáltatásokban bekövetkező rendszer- vagy működéskiesés súlyos, akár globális kihatással lehet azokra a rendszerekre, amelyeket emberek (felhasználók) milliói naponta használnak. A szolgáltatáskiesés banalitására, illetve ezeknek a rendszereknek a ma már nélkülözhetetlen voltára az egyik legjobb példa az az eset, amely 2021. május közepén történt. A Fastly felhőszolgáltató cég, amely többek között az Amazonnak, a Redditnek és számos online folyóiratnak, hírportálnak, közösségimédia-felületnek is szolgáltat háttérmegoldásokat, egyik ügyfele megváltoztatta a szolgáltatási beállításait. Az új beállítás teljesen legitim módon történt, azonban annak nem várt hatása lett. A beállítás olyan hibát *(bug)* generált, amely következtében a Fastly ügyfeleinek 85%-a hibát tapasztalt az általa igénybe vett folyamatokban, és a szolgáltatásai leálltak.[15] A működéskiesés, bár nagyon rövid ideig – csak egy órán keresztül – tartott, jól rávilágít arra, hogy ma már az internetes szolgáltatások mögött is kritikus infrastruktúrák – legyenek azok informatikai eszközök és rendszerek vagy informatikai szolgáltatások – működnek, amelyek kiesése akár világméretű hatással jár.

Támadások a kritikus rendszerek ellen: elképzelt támadások és az azokból levonható következtetések

A 2000-es évek elején több olyan elméleti forgatókönyv is született, amely azt volt hivatott felmérni, hogy az egyre komplexebbé váló infrastruktúrák egyes elemeinek támadása milyen közvetlen vagy nem várt közvetett hatással

[13] Lily Hay Newman: What We Know About Friday's Massive East Coast Internet Outage. *Wired.com,* 2016. október 21.

[14] Kovács (2018): i. m. 92.

[15] Jane Wakefield: One Fastly Customer Triggered Internet Meltdown. *BBC News,* 2021. június 9.

járna. Ezek közül a szcenáriók közül az egyik legnagyobb hatású forgatókönyv 2002-ben az amerikai Naval War College és a Gartner cég együttműködésében, ipari szereplők bevonásával készült. Egy úgynevezett hadijáték alkalmával azt vizsgálták, hogy a kibertérben elkövetett terrortámadások mennyiben és milyen mértékben lennének hatással az Egyesült Államok gazdaságára és politikai vezetésére. A több mint 80 fő bevonásával lezajlott hadijáték szereplőit, akik között voltak különböző informatikai szolgáltatók, illetve olyan kritikusinfrastruktúra-üzemeltetők is, mint például villamosenergia-ellátás, kommunikációs rendszerek vagy internetszolgáltatás, több csapatra osztották. Az egyik csoport, a támadó, azaz Red Team az Egyesült Államok kulcsfontosságú rendszerei elleni kibertámadásokat szimulált. A támadások az előre kiválasztott négy kritikusinfrastruktúra-ágazat – a telekommunikáció, az internet és a számítógép-hálózati szolgáltatások, a villamosenergia-ellátás, valamint a pénzügyi szektor – ellen irányultak. A négy ágazatot négy különválasztott kiberterrorista-csoportot szimuláló csapat támadta különböző kibertéri eszközökkel, egy ötödik csoport pedig a négy támadó csapat akcióit koordinálta. A szimulált kiberterrorista-csoportok dedikáltan államnál kisebb csoportokat jelentettek, és az államok feltételezhető erőforrásainál kevesebb lehetőséggel rendelkeztek. A kevesebb mint 50 millió dollár költségvetéssel megvalósított – hangsúlyosan – kibertámadások mellett, korlátozott fizikai támadások szimulált kivitelezésére volt csak mód. Mind a négy támadó csoport csak 8-8 fizikai támadásra kapott lehetőséget, ezzel ösztönözve azt, hogy ezek célpontjait úgy válasszák ki, hogy az azokkal párhuzamosan elkövetett kibertámadások egymás hatásait felerősítsék. A kivitelezés minden kritikusinfrastruktúra-szektorban stratégiai tervezéssel kezdődött, majd következett a felderítés, amely során meghatározták a legfontosabb célpontokat és azok támadásának célszerű és hatékony módját. Az ezeket a fázisokat követő támadások szimulációja során azt vizsgálták, hogy azok mennyire hatékonyak, illetve az okozott károkat mennyi időn belül tudja a célpont felszámolni.

A Digitális Pearl Harbor, a szimulált, kritikus infrastruktúrákat ért kibertámadások forgatókönyve számos érdekes és fontos tanulsággal járt. A villamosenergia-ellátás vonatkozásában az a megállapítás született, hogy egyes kibertámadásokkal nem okozható nagy méretű szolgáltatáskiesés, azok csak szigetszerűen következnek be.[16] Az ipari SCADA-k (*supervisory control and data acquisition,*

[16] Eric Purchase – French Caldwell: Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack. In Malek Manu – Ghosh Sumit – Edward A. Stohr (szerk.): *Guarding Your Business: A Management Approach to Security.* Boston, Spinger, 2004. 49.

felügyeleti, irányító- és adatgyűjtő rendszerek) esetében is hasonló megállapítás született, azaz azok az esetek többségében – ne felejtsük el, hogy ekkor még csak 2002-t írtunk! – nem csatlakoznak az internethez, azaz azok támadása nem elhanyagolható veszélyforrás, de azokkal sok esetben szintén csak szigetszerűen bekövetkező rendszerkiesések okozhatók.[17] Ugyanakkor a pénzügyi szektor kiváló célpontja lehet a kibertámadásoknak, ugyanis ezekkel előidézhető a közvetlen károkon túl az adott ország kormányába vetett bizalom megrendülése. Az internet és az IT-szektor támadása már egészen más eredményt mutatott. Bár ezeket is nehéz támadni, mert ezekhez megfelelő szakértelem szükséges, azonban az interneten a terrorcsoportok hatékonyabban tudnak rejtőzködni akár az akcióik szervezésekor, akár az egymással történő kommunikációjuk alatt.

A Digitális Pearl Harbor legnagyobb tanulsága az, hogy a kritikus infrastruktúrák komplex és összehangolt akciókkal eredményesen támadhatók, és bár a különböző ágazatokban eltérő mértékű kár okozható, azok összekapcsoltsága révén a jól megválasztott célpontok támadása ágazatokon átnyúló, súlyos károkat képes okozni. A végső konklúzió tehát az, hogy a felvázolt veszélyek nagyon is reálisak.

Ezt erősíti az a tény is, hogy a 2000-es évek óta eltelt időszak alatt az IoT-eszközök elterjedése robbanásszerű volt, ugyanakkor biztonságuk ezt a fejlődést nem követte. Az IoT-eszközökön keresztül viszont számos olyan támadás indítható, amely már az OT-n (*operational technology,* működési technológia) keresztül fejti ki hatásait, sokszor a fizikai térben. Ezt nagyban segíti az IoT- és az OT-eszközök nagy fokú konvergenciája, amely leginkább a SCADA, az ICS (*industrial control system,* ipari irányítási rendszer), illetve az RTU-k (*remote terminal unit,* távoli irányítási egység) összekapcsoltságában jelentkezik.[18]

A Digitális Pearl Harbor szcenárió sok kritikát is kapott, amely elsősorban a kissé hatásvadász címéből eredt, mégis pont ez az, amely felhívja a figyelmet még ma is a kritikus infrastruktúrák területének fontosságára, nemcsak a mindennapi civil életünkben, hanem akár a hadseregek vonatkozásában is:

> „[k]ritikusai ellenére a Pearl Harbor-analógia kitart, mert hasznos keretet ad arra, hogy a kibertértől való függőség hogyan generál sebezhetőségeket, amelyeket az ellenségek kihasználhatnak. […] Figyelmeztetés arra nézve is, hogy az Egyesült Államok és szövetségesei jelenlegi taktikai háborús képességének nagy része attól függ, hogy

[17] Purchase–Caldwell (2004): i. m. 50.

[18] Anna Ribeiro: Protecting Critical Infrastructure Supply Chain Security From Cyber Attacks. *Industrial Cyber,* 2021. május 6.

> képesek-e tájékozódni, és biztonságossá tenni azt a kiberteret, ahol erőik és fegyverrendszereik összekapcsolódnak, és azok vezetése megtörténik."[19]

A Digitális Pearl Harborhoz hasonló, de magyarországi forgatókönyv született 2009-ben Digitális Mohács címmel. Az analógia, azaz az országok egy nevezetes, de annál inkább tragikus történelmi eseményének mint hívónévnek a választása korántsem a véletlen műve. A Digitális Mohács forgatókönyv fő célja az volt, hogy felhívja a figyelmet arra a tényre, amelyet a Digitális Pearl Harbor esetében már láthattunk, nevezetesen, hogy a kritikus infrastruktúrák és ezen belül is a kritikus információs infrastruktúrák támadhatók, aminek következményei beláthatatlanok. A Digitális Mohács egy elképzelt támadássorozat egyes elemeit mutatja be, majd azok hazánk gazdasági és politikai életére gyakorolt hatásait elemzi. A történet pénzügyi manipulációt sejtető megtévesztő médiaművelettel indul, majd ezt követi annak vizsgálata, hogy a pénzügyi rendszer mennyire támadható a kibertérből. Ezzel a fázissal párhuzamosan az internet támadhatósága is vizsgálat tárgya volt. A szcenárió egy következő támadási fázist feltételezve azt is megvizsgálta, hogy a közlekedési infrastruktúra különböző vezérlőrendszerei hogyan reagálnának, illetve milyen következményei lennének egy-egy kibertérből érkező támadásnak. Ugyanakkor a támadási sorozat befejező, ámde legnagyobb kárt okozó fázisa az energiaszektor, ezen belül is a villamosenergia vezérlőrendszereinek a támadása volt.

A Digitális Mohács forgatókönyv rendkívül egyszerűen kivitelezhető, de hatásaiban messze az egyes ágazatokon túlnyúló támadássorozatot vázolt fel. Az ezek elemzéséből levont legfőbb következtetés olyan megállapításokat tett, amelyek a védelem közös felelősségében és az állami szinten koordinált védekezés szükségességében összegezhetőek. A tanulmány mindezt így foglalta össze:

> „[t]ermészetesen a különböző infrastruktúrákat üzemeltetők bizonyos szintig fel vannak készülve az esetleges támadásokra, illetve ezek kezelésére. Abban az esetben azonban, ha az ország több kritikus információs infrastruktúráját éri egyszerre, párhuzamosan komplex – tehát egy időben jelentkező informatikai és fizikai – támadás is, akkor koordináció hiányában nem biztosítható megfelelő szintű védelem. Mindezeknek megfelelően a védelem területén egy átfogó – a kritikus információs infrastruktúrák komplex védelmére vonatkozó – védelmi stratégia kidolgozása az első lépés, amelyet meg kell tenni."[20]

[19] Emily O. Goldman – Michael Warner: Why a Digital Pearl Harbor Makes Sense … and Is Possible. In George Perkovich – Ariel E. Levite (szerk.): *Understanding Cyber Conflict. 14 Analogies.* Washington (DC), Georgetown University Press, 2017. 147.

[20] Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3. (2010), 1. 56.

Támadások a kritikus rendszerek ellen: a nyomásgyakorlás módszerei és az azokból levonható következtetések

Az kétségtelen módon kiderül a fenti, elméletben felállított szcenáriókból – azaz a Digitális Pearl Harbor, illetve a Digitális Mohács forgatókönyvből, majd az azokból levonható következtetésekből –, hogy a kritikus információs infrastruktúrákon keresztül egy fejlett digitális ökoszisztémával rendelkező országra jelentős nyomás gyakorolható ezeken a rendszereken keresztül. Ez a nyomásgyakorlás, függetlenül annak céljától, amely lehet politikai, gazdasági, társadalmi vagy akár katonai, minden valószínűséggel több fázisból áll. A fázisok közül az első és a legtöbb időt igénybe vevő az információszerzés, valamint a megszerzett adatok és információk feldolgozása, illetve kiértékelése, majd ezt követi a tervezés és a célmeghatározás, a támadás végrehajtása, végül pedig a hatáselemzés.

Annak vizsgálatára, hogy valóban működik-e egy adott ország vonatkozásában a nyomásgyakorlás a kritikus infrastruktúrákon, illetve a kritikus információs infrastruktúrákon keresztül, az egyik kínálkozó módszer, ha felidézünk néhány, az elmúlt időszakban a kritikus infrastruktúrát ért támadást.

2020 áprilisában az egyébként súlyos vízellátási problémákkal küzdő Izrael vízszolgáltatását érték támadások. Az egyik támadás mezőgazdasági vízszivattyúkat célzott Galilea felső részén, ahol azok leállását sikerült elérni, míg egy másik az ország közepén lévő ivóvízellátási rendszereket támadta a kibertérből. Az ország vízügyi hatósága megerősítette a támadások tényét, de közleményük szerint Izrael vízrendszerében nem történt jelentős kár. A hivatalos források nem erősítették meg, de hírügynökségek Iránt sejtették a támadások hátterében. Ugyanakkor ezek a nem hivatalos források a támadások más dimenzióit is felvázolták, amely szerint Irán nemcsak a vízszivattyúk leállítását célozta, hanem az ivóvízrendszer klórszintjének emelését is el akarta érni. Abban az esetben, ha a támadásnak ez a szakasza bekövetkezett volna, akkor emberek százait betegíthette volna meg a magas klórkoncentráció.[21] Ugyanakkor az izraeli Nemzeti Kiberügyi Igazgatóság akkori vezetője, Yigal Unna egy hivatalos nyilatkozatában, bár név szerint nem említette Iránt, azt elmondta, hogy a támadások nemcsak az ivóvíz klórszintjének emelésére, hanem a klór mellett más vegyi anyagok bejuttatására is kísérletet tettek. Nyilatkozatában Unna a kibertéri támadások

[21] Times of Israel: Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps. *Times of Israel,* 2020. július 17.

fizikai térben megnyilvánuló hatásait vetítette előre: „[v]alami olyasminek lehetünk tanúi, aminek célja a valós élet, és nem az informatika vagy az adatok károsítása."[22]

2020 decemberében egy másik, első ránézésre nem a kritikus infrastruktúrákkal összefüggő támadásra derült fény. 2020. december 8-án a FireEye amerikai kiberbiztonsági vállalat egyik hivatalos blogjában beszámolt egy, a cég rendszereit ért szofisztikált támadásról. A bejegyzés szerint a FireEye cég kormányzati szereplők biztonsági tesztelésére is használt szoftvereit lopták el a támadók. A cég vizsgálatai kiderítették, hogy elsőként nem is az ő, hanem az egyik szoftverkomponensüket gyártó cég, a SolarWinds rendszereibe hatoltak be hónapokkal korábban, és ott kém-, valamint egyéb rosszindulatú programokat helyeztek el. A SolarWinds a FireEye-on kívül közel 18 ezer további vállalatnak és szervezetnek szállított szoftvereket. Az elemzések azt mutatták, hogy a SolarWinds érintett szoftvereibe azok gyári frissítésén keresztül hatolhattak be a támadók még 2020 áprilisában. A SolarWinds által gyártott szoftvereken keresztül bekövetkezett támadások érintették többek között az Egyesült Államok olyan szoftverfejlesztő és IT-szolgáltató vállalatait, mint például a Cisco, az Intel, az NVIDIA, a Deloitte, az SAP, a Check Point, illetve a szövetségi kormányzat szervezeteit, mint például a Védelmi Minisztérium, a Belbiztonsági Minisztérium, az Államkincstár, illetve a NASA. Az Egyesült Államokon kívül világszerte számos ország kormányzati rendszere szintén érintett volt a támadásban, amelynek egyik bizonyítható célja az adatlopás volt.[23] A fenti felsorolásból is látható, hogy a SolarWinds-támadás néven elhíresült akciósorozat érintette az infokommunikációs ágazat mellett a pénzügyi szektort, de a közigazgatást is mint kritikusinfrastruktúra-ágazatot. A SolarWinds-ügy világszerte hatalmas visszhangot váltott ki, hiszen nagyon jól rávilágított a beszállítói lánc – angol terminológiával élve: *supply chain* – biztonságának kérdéseire. A támadás hátterében szakértők Oroszországot sejtik.[24]

Egy másik eset, a Colonial Pipeline esete szintén nagyon jól mutatja a kibertérből érkező támadások fizikai térben kifejtett hatását, amely ráadásul egy olyan kritikus infrastruktúra esetében jelentkezett, amely a világ legerősebb

[22] Associated Press – Times of Israel: 'Cyber Winter Is Coming,' Warns Israel Cyber Chief After Attack on Water Systems. *Times of Israel,* 2020. május 8.

[23] Christina Zhao: SolarWinds, Probably Hacked by Russia, Serves White House, Pentagon, NASA. *Newsweek,* 2020. december 14.

[24] David E. Sanger: After Russian Cyberattack, Looking for Answers and Debating Retaliation. *The New York Times,* 2021. február 23.

országában okozott számottevő fennakadásokat és károkat. A Colonial Pipeline az Egyesült Államok egyik legnagyobb üzemanyag-szállító csőhálózata, amely az USA keleti partja mentén, Houstontól az észak-keleti New Jersey-ig fut, közel 9000 km hosszúságban. A keleti part napi üzemanyag-mennyiségének 45%-a ezen a hálózaton jut el az elosztókig, a benzinkutakig, illetve a felhasználókig. 2021 áprilisában nem hivatalos információk szerint egy orosz, de nem állami kötődésű kiberbűnözői csoport, a DarkSide megtámadta a csőhálózatot üzemeltető vállalat informatikai rendszereit, amelyekben *ransomware*-t helyezett el. A támadás sikerességét mutatja, hogy a vállalat kénytelen volt leállítani a teljes irányítórendszert, elkerülendő a zsaroló vírus további eszkalációját. Ugyanakkor ez azt okozta, hogy számos államban, így Észak-Karolinában, illetve Georgiában a benzinkutak nem jutottak üzemanyaghoz, azok kifogytak, súlyos ellátási problémát okozva ezzel az egyébként is nagyban a közúti közlekedési infrastruktúrára alapozott szállításban és közlekedésben. A cég döntése az volt, hogy kifizetik a támadók által bitcoinban kért „váltságdíjat", amelyért cserébe megkapták a zsaroló vírus által titkosított adatok feloldásához szükséges kódokat. Ugyanakkor ez még nem jelentette automatikusan a rendszerek működésének azonnali helyreállíthatóságát, hiszen az egy ilyen nagyságú és komplexitású infrastruktúra esetében több napot is igénybe vehet. A támadó csoport, azaz a DarkSide az eset után közleményt adott ki, amelyben leszögezte, hogy nem politikai, geopolitikai vagy egyéb céljai voltak a támadással, hanem egyszerűen csak pénzszerzés volt a motiváció. Ez nagyon jól rávilágít arra a tényre, hogy a kritikus infrastruktúrák támadásának következményei függetlenek a támadások mögött lévő motivációtól.[25]

Mindemellett nemcsak a kritikus infrastruktúra jól látható elemeit érheti támadás, hanem az olyan, a háttérben működő rendszereket, illetve azok egyes elemeit is, mint például az élelmiszeripar. Ennek egyik példája a Brazília legnagyobb húsfeldolgozó vállalatát ért – nem meglepő, szintén *ransomware*-támadás 2021 tavaszán. A JBS nemcsak Brazília, hanem a világ egyik legnagyobb húsfeldolgozó és húsellátó cége is egyben, amely több mint 15 országban végzi tevékenységét közel 150 ezer alkalmazottal. A vállalat rendszereit ért támadás következtében „a vállalat számítógépes rendszerei megbénultak, az Ausztráliában, Kanadában és az Egyesült Államokban működő üzemeik közül pedig több

[25] BBC News: Colonial Pipeline Boss Confirms $4.4M Ransom Payment. *BBC News,* 2021a. május 19.

leállt".[26] Ez komoly húsellátási problémákat okozott az említett országokban, illetve azok környezetében regionálisan.[27]

A fenti, kritikus infrastruktúrák és kritikus információs infrastruktúrák ellen elkövetett, a kibertéren keresztül megvalósított támadásokból levonható az a következtetés, hogy egy adott országra, illetve akár nagyobb földrajzi régióra is nagy nyomás gyakorolható. A támadások következményeikben és hatásaikban eltérőek, de azok már jóval túlmutatnak a kibertéren, hiszen sok esetben a fizikai térben megnyilvánuló hatásokkal járnak. Ez abszolút jelentős nyomást gyakorol az adott országra.

A nyomásgyakorlást módszereiben és eszközeiben két csoportra oszthatjuk: közvetlen és közvetett eszközökre. A közvetlen eszközök közé tartozhat például a kritikus rendszerek bénítása. Ebben az esetben az olyan rendszerek támadása vagy működésének befolyásolása a cél, amelyek számos más létfontosságú rendszerre hatnak. Ilyen az energiaszektor és annak rendszerei. Nyilvánvalóan a villamosenergia-rendszer fizikai átviteli hálózatai (például az áramvezetékek) és azok akár fizikai támadása okozhatja a legnagyobb károkat. Főleg úgy, hogy ezek a rendszerek nem védettek, sok esetben nem is lehetnek teljesen védettek a fizikai támadásokkal szemben. Ennek több oka van, de az okokat itt is alapvetően a kockázatokkal arányos védelemben kell keresni. Azaz ezek esetében – elsősorban azok földrajzi kiterjedtsége miatt – nem éri meg olyan szintű fizikai védelmet kiépíteni, amely ezen rendszerek egyes elemeinek esetleges fizikai rombolása ellen nyújtanának maximális védelmet.

A nyomásgyakorlás közvetett eszközei lehetnek például a közigazgatási rendszerek működésének akadályozására irányuló akciók. Ezek a támadások, illetve a működés akadályozása ebben az esetben is információgyűjtéssel kezdődik. Az információgyűjtés az adott közigazgatási rendszer technikai információi (például alkalmazott hálózati megoldások, szoftverek, hardverek, illetve ezek birtokában az azokban meglévő és kihasználható sérülékenységek) mellett a rendszereket üzemeltető személyekről, illetve az ezeket a szolgáltatásokat használó közigazgatási dolgozókról szóló információk összegyűjtésével, azok elemzésével és értékelésével kezdődik. Itt már látható módon összekapcsolódik az üzemeltetői és felhasználói állomány biztonságtudatos – akár magánéletében is megvalósított – internet- és infokommunikációseszköz-használata, vagy a másik véglet: a biztonságtudatosság hiánya. A célzott támadások (például a *spear*

[26] BBC News: JBS: Cyber-Attack Hits World's Largest Meat Supplier. *BBC News,* 2021b. június 2.
[27] BBC News (2021b): i. m.

phishing) túlnyomó többsége a közösségimédia-platformok használata során megadott, majd a támadók által összegyűjtött és akár éveken keresztül szisztematikusan elemzett és értékelt információk felhasználására épül. Ugyanakkor az így megszerzett információk a *social engineering* támadások első fázisában is kiválóan használhatóak, hiszen a megtévesztésre vagy akár a humán zsarolásra épülő támadás megindításához ezek az információk elengedhetetlenek. Az így megszerzett információk birtokában a közigazgatási rendszerek támadása már viszonylag egyszerűen kivitelezhető. Sok esetben ehhez még ezeknek a rendszereknek a nem átgondolt és nem megfelelően megvalósított, illetve fenntartott biztonsági állapota is hozzájárul hatásnövelőként. A közigazgatási rendszerek szisztematikus támadása a fentiekben is említett, az állammal szembeni bizalom megbontásán túl súlyos ellátási, szervezési és nem utolsósorban közbiztonsági következményekkel járhat.

Összefoglalás

A fentiekben bemutatott, a kritikus infrastruktúrák támadhatóságát felvázolni hivatott szcenáriók esetében a használt Digitális Pearl Harbor vagy Digitális Mohács kifejezés mint metafora valószínűleg nem jó, figyelmeztetnek szakértők.[28] Ugyanakkor ennek oka nem az, hogy a kritikus infrastruktúrák nincsenek veszélynek kitéve, és azokban nem következhet be mohácsi tragédia, hanem az, hogy bár a veszély nagyon is reális, de nagy valószínűséggel nem egy támadás, hanem a kritikus infrastruktúrák, illetve kritikus információs infrastruktúrák elleni támadások jól összehangolt sorozata fogja csak előidézni azt, amit ezeknek a metaforaként használt történelmi eseményeknek a révén be szeretnénk mutatni, illetve amire a figyelmet ezek fel szeretnék hívni.

A fentiek alapján nem kétséges, hogy a kritikus infrastruktúrák területén jelentkező veszélyek valósak. A kérdés inkább az, hogy a felvázolt komplex támadások hogyan épülnek fel, és mely infrastruktúrák vagy azok mely elemei ellen fognak irányulni. Egy másik óriási kérdés, hogy hogyan lehet megvédeni ezeket a rendszereket, hiszen sok esetben önmagukban a védelmet jelentő biztonsági rendszerek is kritikus infrastruktúrának minősülhetnek, tovább bonyolítva a kérdést.

[28] Sharon Weinberger: Cyber Pearl Harbor: Why Hasn't a Mega Attack Happened? *BBC,* 2013. augusztus 20.

Azt azonban ki kell jelenteni, hogy a kritikus infrastruktúrák és különösen a kritikus információs infrastruktúrák egymással való – sok esetben mármár átláthatatlan és gyakorlatilag feltérképezhetetlen – kapcsolata, valamint azok interdependenciája, azaz egymástól való függősége azt is jelenti, hogy egy adott ország kritikus infrastruktúráját vagy kritikus információs infrastruktúráját ért bármilyen támadás kihatással van egy vagy több másik kritikus infrastruktúra vagy kritikusinformációsinfrastruktúra-elem működésére. Ugyanakkor ezek a hatások a földrajzi határokon átívelő módon jelentkeznek. Mindezekre a legjobb a példa a fentiekben említett SolarWinds-ügy, ahol már a beszállítói lánc biztonsága is komolyan érintett, de ugyanilyen jó példa a Dyn DNS-szolgáltató esete az infrastruktúrákon belül meglévő alrendszerek kritikusságára.

Csak két példa, amely rávilágít arra, hogy a fejezet címéből eredő kérdésekre adott válaszok rendkívül komplexek. A kibertámadásokkal a kritikus infrastruktúrákban okozható károk dominóeffektust hoznak létre, amely jóval a kibertér határain kívül is jelentkezik. Ezek a támadások a fizikai térben is éreztetik hatásukat, felerősítve a – jelen fejezet címében szintén megfogalmazott kvázi hipotézist, azaz a – nyomásgyakorlást egy adott országra.

A kritikus infrastruktúrák védelme nem pusztán szabályozási és nem pusztán technikai kérdés. A védelemnek dinamikusnak kell lennie, amely a felkészüléstől a közel valós idejű incidenskezelésen át a kutatás-fejlesztésig kell hogy tartson.

Mindezeken túl a védelem megvalósítása össztársadalmi tevékenységet igényel. Ahogy az amerikai Kibervédelmi Parancsnokság korábbi vezetője megfogalmazta: „[…] teljes mértékben tisztában vagyok azzal, hogy a kiberbiztonság nemzetbiztonsági kérdés, és olyan összkormányzati megközelítést igényel, amely nemcsak a kormányt, a minisztériumokat, a különböző ügynökségeket, hanem a magánszektort és a nemzetközi partnereinket is összefogja."[29]

[29] Committee on Armed Services United States Senate: United States Cyber Command Washington, D.C., 2018. február 17.

Irodalomjegyzék

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

2016/1148. Az Európai Parlament és a Tanács (EU) irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. Brüsszel, 2016.

2080/2008. (VI. 30.) Kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

Associated Press – Times of Israel: 'Cyber Winter Is Coming,' Warns Israel Cyber Chief After Attack on Water Systems. *Times of Israel,* 2020. május 8. Online: www.timesofisrael.com/israeli-cyber-chief-attack-on-water-systems-a-changing-point-in-cyber-warfare/

BBC News: Colonial Pipeline Boss Confirms $4.4M Ransom Payment. *BBC News,* 2021a. május 19. Online: www.bbc.com/news/business-57178503

BBC News: JBS: Cyber-Attack Hits World's Largest Meat Supplier. *BBC News,* 2021b. június 2. Online: www.bbc.com/news/world-us-canada-57318965

COM(2005) 576. Az Európai Közösségek Bizottsága: Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról. Brüsszel, 2005. november 17. COM(2005) 576 végleges.

Committee on Armed Services United States Senate: *United States Cyber Command.* Washington, D.C. 2018. február 17. Online: www.armed-services.senate.gov/imo/media/doc/18-17_02-27-18.pdf

European Commission: *European Programme for Critical Infrastructure Protection.* Brüsszel, 2006.

Goldman, O. Emily – Michael Warner: Why a Digital Pearl Harbor Makes Sense … and Is Possible. In George Perkovich – Ariel E. Levite (szerk.): *Understanding Cyber Conflict. 14 Analogies.* Washington (DC), Georgetown University Press, 2017. 147–157. Online: https://carnegieendowment.org/2017/10/16/why-digital-pearl-harbor-makes-sense-.-.-.-and-is-possible-pub-73405

JOIN(2020) 18 final. Közös közlemény az Európai Parlamentnek és a Tanácsnak Az EU kiberbiztonsági stratégiája a digitális évtizedre. Brüsszel, 2020. december 16.

Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3. (2010), 1. 44–56. Online: www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf

Newman, Lily Hay: What We Know About Friday's Massive East Coast Internet Outage. *Wired.com,* 2016. október 21. Online: www.wired.com/2016/10/internet-outage-ddos-dns-dyn

Purchase, Erik – French Caldwell: Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack. In Sumit Ghosh – Manu Malek – Edward A. Stohr (szerk.): *Guarding Your Business: A Management Approach to Security.* Boston, Spinger, 2004. 47–64. Online: https://doi.org/10.1007/0-306-48638-5_4

Ribeiro, Anna: Protecting Critical Infrastructure Supply Chain Security From Cyber Attacks. *Industrial Cyber,* 2021. május 6. Online: https://industrialcyber.co/article/protecting-critical-infrastructure-supply-chain-security-from-cyber-attacks/

Sanger, E. David: After Russian Cyberattack, Looking for Answers and Debating Retaliation. *The New York Times,* 2021. február 23. Online: www.nytimes.com/2021/02/23/us/politics/solarwinds-hack-senate-intelligence-russia.html

Times of Israel: Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps. *Times of Israel,* 2020. július 17. Online: www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/

Trend Micro: Operation Pawn Storm: Fast Facts and the Latest Developments (2016. január 16.). Online: www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-pawn-storm-fast-facts

Wakefield, Jane: One Fastly customer triggered internet meltdown. *BBC News,* 2021. június 9. Online: www.bbc.com/news/technology-57413224

Weinberger, Sharon: Cyber Pearl Harbor: Why Hasn't a Mega Attack Happened? *BBC,* 2013. augusztus 20. Online: www.bbc.com/future/article/20130820-cyber-pearl-harbor-a-real-fear

Zhao, Christina: SolarWinds, Probably Hacked by Russia, Serves White House, Pentagon, NASA. *Newsweek,* 2020. december 14. Online: www.newsweek.com/solar-winds-probably-hacked-russia-serves-white-house-pentagon-nasa-1554447