Kritikus infrastruktúrák védelmének interdiszciplináris megközelítése: a lichterfeldei erőmű elleni támadás esettanulmánya

Absztrakt

A kritikus infrastruktúrák (KI) védelme napjainkban kiemelt jelentőségű biztonságtudományi terület, amely szorosan összefügg a társadalom működésének fenntarthatóságával. Jelen tanulmány a 2026 elején Berlin Lichterfelde kerületében bekövetkezett áramszünetet amelyet egy szélsőbaloldali csoport által végrehajtott szabotázs, a lichterfeldei erőmű elleni támadás idézett elő használja esettanulmányként. A cikk interdiszciplináris megközelítéssel, hálózatelméleti, kockázatmenedzsment, válságkommunikációs és hírszerzési elemzési szempontból vizsgálja az eseményt. Rávilágítunk arra, hogy egy kritikus infrastruktúrát érő támadás milyen rendszerszintű hatásokat okozhat, és hangsúlyozzuk, hogy az ilyen infrastruktúrák védelme csak több tudományterület integrált alkalmazásával lehet hatékony. Az esettanulmány tanulságai alapján ajánlásokat fogalmazunk meg a kritikus infrastruktúrák védelmének fejlesztésére, különös tekintettel a hálózatos sebezhetőségek csökkentésére, a kockázatok proaktív kezelésére, a válsághelyzeti kommunikáció javítására és a hírszerzési előrejelző tevékenységek erősítésére.

Abstract

Interdisciplinary Approach to Critical Infrastructure Protection: A Case Study of the Attack on the Lichterfelde Power Plant. Critical infrastructure protection is a crucial field of security science, closely related to the resilience of societal functions. This study uses the power outage incident in the Lichterfelde district of Berlin in early 2026 caused by a sabotage attack on a power facility by a left-wing extremist group as a case study. The article examines the event from an interdisciplinary perspective, including network theory, risk management, crisis communication, and intelligence analysis aspects. We highlight how an attack on critical infrastructure can lead to systemic impacts and emphasize that protecting such infrastructure effectively requires integrating multiple disciplines. Based on the lessons from the case study, we provide recommendations for improving critical infrastructure protection, with particular focus on reducing network vulnerabilities, proactive risk management, enhancing crisis communication, and strengthening intelligence foresight capabilities.

Bevezetés

A modern társadalom zavartalan működése számtalan egymásra épülő kritikus infrastruktúrától függ, beleértve az energiatermelést és -elosztást, a vízellátást, a közlekedést, a távközlést és az egészségügyi rendszereket (Rinaldi *et al.*, 2001). Ezen rendszerek védelmét, sérülékenységük csökkentését és gyors helyreállításukat célozza a kritikus infrastruktúra-védelem (KI-védelem), amely a biztonságtudomány egy interdiszciplináris területe. A 21. században a fenyegetések köre egyre bővül: a természeti katasztrófák és technológiai balesetek mellett megjelent a

szándékos károkozás, a terrorizmus és a kibertámadások veszélye is (Department of Homeland Security [DHS], 2013). Az Egyesült Államok Nemzeti Infrastruktúravédelmi Terve (National Infrastructure Protection Plan NIPP) már 2013-ban kiemelte, hogy a kritikus infrastruktúrák biztonsága és rezilienciája nemzeti szintű prioritás, és átfogó kockázatkezelési keretrendszert vezetett be ennek érdekében (DHS, 2013). Hasonlóan Európában is erősödik a szabályozás: például az Európai Unió 2022-ben elfogadott új irányelve a létfontosságú entitások rezilienciájáról előírja a rendszeres kockázatértékelést és védelmi tervezést (Šarūnienė *et al.*, 2024).

Az utóbbi évek eseményei rámutattak, hogy a kritikus infrastruktúrák elleni támadások nem pusztán elméleti fenyegetések. 2026 januárjában Berlin jelentős részét napokra sötétségbe borította egy szándékos rongálásból eredő áramszünet, amelynek okát hamarosan egy politikai indíttatású akcióban azonosították (CBS News, 2026; Cook, 2026). A támadás és az azt követő válsághelyzet rávilágított a kritikus infrastruktúrák sebezhetőségére és az ilyen események társadalmi hatásaira. A történtek egyben felhívták a figyelmet arra is, hogy a hagyományos védelmi intézkedések nem elegendőek: a fizikai biztonságon túl szükség van a hálózati rendszerek mélyebb megértésére, a kockázatmenedzsment alaposabb alkalmazására, hatékony válságkommunikációra és proaktív hírszerzési elemzésre (Lewis, 2015; Magee, 2018; Reynolds & Seeger, 2005).

Jelen tanulmány célja, hogy a lichterfeldei erőmű elleni támadást és az annak nyomán kialakult áramszünetet esettanulmányként felhasználva bemutassa a kritikus infrastruktúra-védelem interdiszciplináris elemzésének fontosságát. A következő szakaszokban először összefoglaljuk az esemény körülményeit és közvetlen következményeit. Ezt követően négy különböző nézőpontból vizsgáljuk meg az esetet: (1) hálózatelméleti szempontból, hogyan vezethet egyetlen csomópont kiesése dominóeffektushoz; (2) kockázatmenedzsment szempontból, milyen hiányosságok mutatkoztak a megelőzésben és a felkészülésben; (3) válságkommunikáció szempontból, hogyan kezelték a hatóságok a lakosság tájékoztatását és a pánik elkerülését; (4) hírszerzési elemzés szempontból, mit lehet tudni az elkövetőkről és hogyan lehetne jobban előre jelezni az ilyen fenyegetéseket. Végezetül levonjuk a tanulságokat, és rámutatunk, hogy a kritikus infrastruktúrák védelme csak ezen megközelítések integrált alkalmazásával lehet eredményes.

Esettanulmány: a lichterfeldei erőmű elleni támadás és következményei

2026. január első napjaiban Berlin délnyugati részén, a Steglitz-Zehlendorf kerületben található Lichterfelde erőmű közelében szabotázsakció történt, amelynek következtében a város jelentős részén hosszú ideig tartó áramszünet alakult ki (CBS News, 2026; Cook, 2026). Szombat hajnalban, helyi idő szerint ~6 órakor tűz ütött ki a Teltow-csatorna fölött átívelő kábelhídon, amely több nagyteljesítményű távvezetéket hordozott ezek a vezetékek kulcsszerepet játszottak Berlin villamosenergia-ellátásában (Vassileva, 2026). A keletkezett károk négy délnyugati kerületben köztük Nikolassee, Zehlendorf, Wannsee és Lichterfelde városrészekben mintegy 45 000 háztartást és több ezer üzleti fogyasztót vágtak el az áramszolgáltatástól (Cook, 2026;

Vassileva, 2026). Ez a kiesés a második világháború óta a legsúlyosabb áramszünetnek számított Berlinben (Cook, 2026).

A támadásért felelősséget vállaló csoport egy magát *Vulkangruppe* néven azonosító szélsőbaloldali anarchista kollektíva volt, amely az elmúlt másfél évtizedben már több hasonló akciót hajtott végre Németországban (CBS News, 2026; Cook, 2026). A csoport egy online közzétett nyilatkozatban azt állította, hogy sikerrel „szabotáltak" egy gáztüzelésű erőművet Lichterfelde térségében, tiltakozásul a fosszilis energiafelhasználás, a klímaváltozás és a társadalmi egyenlőtlenségek ellen (CBS News, 2026; Cook, 2026). A közleményük provokatív címet viselt: *„Elzárni az uralkodók energiáját"*, utalva arra, hogy szándékosan jómódú negyedeket céloztak, hogy „kikapcsolják az elektromos ellátást a vezető osztálynál" (CBS News, 2026). Ugyanakkor a csoport bocsánatot is kért azoktól a szegényebb lakosoktól, akiket a kimaradás akaratlanul sújtott, jelezve, hogy nem ők voltak a célpontok (CBS News, 2026). A támadók ideológiai üzenete szerint az akció „szükséges lépés" volt a fosszilisenergia-függőség és a nagy energiaigényű adatközpontok (melyek az ő narratívájukban a megfigyelést és a klímaváltozást súlyosbítják) elleni tiltakozásul (CBS News, 2026).

A szabotázs következményei gyorsan túlmutattak a támadók által megjelölt célcsoporton. Az áramszünet miatt számos létfontosságú szolgáltatás akadozott: a távfűtési hálózat bizonyos részei leálltak, mivel a fűtőerőmű ugyan fizikailag nem sérült, de a fűtőközeg keringetéséhez szükséges szivattyúk áram híján nem működtek (Vassileva, 2026). Több kórház és idősotthon vészhelyzeti üzemmódba kényszerült; néhány bentlakót át kellett szállítani, mivel az épületek nem tudták biztosítani a szükséges áramellátást az orvosi berendezésekhez (Cook, 2026). A közlekedésben is fennakadások voltak: egyes helyi vasúti és városi közlekedési vonalak leálltak, a közúti közlekedést pedig kieső jelzőlámpák nehezítették (CBS News, 2026). A telekommunikációs hálózat sérülékenysége is megmutatkozott, mivel bizonyos mobiltelefonos cellák és átjátszók áram hiányában lekapcsolódtak, így a mobilhálózat részlegesen összeomlott a szóban forgó kerületekben (CBS News, 2026). Ez nemcsak a lakosság kommunikációját érintette, de egyes segélyhívó számok is átmenetileg elérhetetlenné váltak (Cook, 2026). A hideg téli időjárás közepette több ezer ember maradt fűtés nélkül; a hatóságok sportcsarnokokat és közösségi létesítményeket nyitottak meg ideiglenes melegedőhelyekként, uszodákat pedig fürdési és tisztálkodási lehetőség biztosítására (Cook, 2026). A rendőrség hangosbemondókkal felszerelt járőrautókkal járta az utcákat, hogy tájékoztassa a lakosokat a helyzetről és a szükséges teendőkről, figyelembe véve, hogy sok háztartásban a rádió, televízió és internet híján más információforrás nem volt (CBS News, 2026).

A városvezetés és a kormányzat reakciója gyors és határozott volt. Kai Wegner, Berlin főpolgármestere a történteket élesen elítélte, „abszolút elfogadhatatlan" terrorcselekménynek nevezve az infrastruktúra elleni támadást, amely szerinte emberéleteket veszélyeztetett (CBS News, 2026; Cook, 2026). Hangsúlyozta, hogy ezek „nem csínytevések, hanem professzionális bűnözők akciói", amelyek a város lakosságának legsebezhetőbb tagjait például lélegeztetőgépre szoruló betegeket, kisgyermekes családokat is veszélybe sodorták (CBS News, 2026). Wegner a tettesek felelősségre vonását sürgette, és arra figyelmeztetett, hogy az energiainfrastruktúra elleni támadások óriási terhet rónak a segélyszolgálatokra (CBS News, 2026). Berlin belügyi szenátora, Iris Spranger kiemelte, hogy a villamosenergia-hálózatra vonatkozó részletes

információk nyilvánossága aggályos szerinte „az elektromos hálózatunk részletei nem valók a nyilvánosság elé”, mivel a jogszabályi átláthatósági követelmények akaratlanul is megkönnyíthetik a szélsőségesek dolgát (Cook, 2026). A német Szövetségi Főügyészség közben átvette a nyomozást, jelezve az ügy kiemelt súlyát (Cook, 2026). A hatóságok rámutattak, hogy a Vulkangruppe név alatt (vagy ahhoz hasonló elnevezéssel) működő szélsőbaloldali sejt(ek) 2011 óta folytatnak szabotázskampányt, amelynek során energia-, vasúti és távközlési infrastruktúrák ellen követtek el több tucat támadást, milliós károkat okozva (CBS News, 2026; Cook, 2026). 2018-ban például egy tűzeset több ezer háztartás áramellátását vágta el, 2024 márciusában pedig a csoport magára vállalta egy nagyfeszültségű távvezeték felgyújtását, amely a berlin-brandenburgi Tesla Gigafactory üzemét látta el energiával a termelést ideiglenesen le kellett állítani az üzemben (CBS News, 2026). 2025 szeptemberében Berlin délkeleti részén történt egy hasonló, több mint 60 órás áramszünettel járó támadás, amelyet bár nem vállalták nyíltan a hatóságok széles körben a Vulkangruppe tevékenységének tulajdonítottak (CBS News, 2026; Cook, 2026).

A lichterfeldei esemény rávilágított Berlin kritikus infrastruktúráinak sebezhetőségére, és felerősítette a követelést a védelmi intézkedések javítására. A német energiaipari szövetség (BDEW) vezérigazgatója, Kerstin Andreae a támadás kapcsán hangsúlyozta, hogy erősíteni kell az életfontosságú létesítmények fizikai és kiberbiztonsági védelmét, mivel a mostani eset is azt mutatja, hogy a támadók kis erőfeszítéssel is súlyos és messzeható következményeket tudnak előidézni egy erősen összekapcsolt urbánus infrastruktúrában (Vassileva, 2026). Andreae utalt a készülő német *Kritikus Infrastruktúrák Átfogó Védelméről szóló törvényre* (KRITIS törvény), amely először foglalja egységes jogi keretbe a kritikus létesítmények védelmét, igazodva az EU új NIS2 kiberbiztonsági irányelvéhez (Vassileva, 2026). Ugyanakkor figyelmeztetett, hogy a jelenlegi jogszabályok által előírt túlzott átláthatóság például a hálózati adatok és geolokációs információk közzététele éppen hogy alááshatja a biztonságot, mert „ezáltal gyakorlatilag tálcán kínáljuk a kritikus infrastruktúráink térképét a nyilvánosság számára” (Vassileva, 2026). A politikai és szakmai nyilatkozatok egyaránt egy interdiszciplináris megközelítés szükségességét sugallták: nem elég a fizikai védelem, párhuzamosan gondoskodni kell a megfelelő redundáns hálózati struktúrákról, a kockázatok folyamatos felméréséről, a lakosság felkészítéséről és tájékoztatásáról, valamint az elhárító szervek közötti információmegosztásról is.

A következőkben részletesen megvizsgáljuk a fenti szempontokat, hogy feltárjuk, miként járultak hozzá a történések alakulásához, és milyen tanulságok vonhatók le a kritikus infrastruktúrák jövőbeni védelme érdekében.

Hálózatelméleti szemlélet: a rendszerszintű sebezhetőség

A lichterfeldei támadás rámutatott a kritikus infrastruktúrák hálózatos jellegére és sebezhetőségére. A villamosenergia-ellátó rendszer tipikusan egymással összekapcsolt alállomások, vezetékek és erőművek összetett hálózata, amelyben egyetlen csomópont vagy kapcsolat kiesése is disproporcionális hatást gyakorolhat az egész rendszerre (Albert *et al.*, 2004). Jelen esetben a támadók pontosan egy ilyen kritikus pontot a Teltow-csatorna feletti kábelhidat és az azon futó vezetékeket célozták meg. Ennek következtében több elosztó alállomás egyszerre vált elérhetetlenné az átviteli hálózat számára (Cook, 2026), ami

dominóelvet indukált: az áramszolgáltatás széles körben megszűnt a hálózatban downstream irányban. A hálózatelmélet ezt a jelenséget “cascading failure”-nek, vagyis kaszkádszerű hibaterjedésnek nevezi, amikor egy adott elem meghibásodása tovagyűrűző hatást indít el a rendszerben (Rinaldi *et al.*, 2001). Az interdependens infrastruktúrák (pl. energiától függő távközlés, közlekedés, vízellátás) esetében pedig a fizikai hálózat meghibásodása más szektorok szolgáltatásait is magával ránthatja, ahogy azt Berlinben is láthattuk.

Hálózatelemzési kutatások kimutatták, hogy a komplex infrastruktúrahálózatok általában bizonyos fokig *robosztusak* a véletlenszerű hibákkal szemben, ugyanakkor célzott támadások esetén sérülékenyek, ha azok a hálózat magas fokú centralitású csomópontjait érik (Albert *et al.*, 2004). A jelen eset is ezt támasztja alá: a támadás nem véletlenszerűen érte a hálózatot, hanem láthatóan egy előre azonosított szűk keresztmetszetet (kritikus érpontot) céloztak. Az eredmény egy olyan *strukturális sérülés* volt, amely a hálózat jelentős részének működését megbénította. A hálózatelméleti megközelítés rávilágít arra, hogy a kritikus infrastruktúra-hálózatokban azonosítani kell az ilyen kulcselemeket például nagyelosztó központok, egyedi fontosságú távvezetékek, transzformátorok –, mert ezek fokozott védelemre vagy redundáns megoldásokra szorulnak (Rinaldi *et al.*, 2001; Lewis, 2015). Ideális esetben a rendszer tervezésekor törekedni kell a redundanciára, hogy egyetlen pont meghibásodása ne okozhasson ekkora kiesést. Jelen támadás rámutatott, hogy a szóban forgó berlini hálózatrész redundanciája nem volt megfelelő: egy kábelhíd kiesése négy kerületet sötétített el.

Az eset azt is példázza, hogy a hálózatok közötti kölcsönös függések (interdependenciák) tovább súlyosbíthatják a károkat. Mivel a villamos energia egy másik kritikus infrastruktúra a távfűtés működésének előfeltétele, az áramszünet maga után vonta a fűtési szolgáltatás akadozását is (Vassileva, 2026). Hasonlóképpen, az elektromos hálózat kiesése megbénította a telekommunikációs hálózat egy részét, valamint a közlekedési lámpák működését. Ez tipikus példája annak, amit a szakirodalom rendszerszintű kockázatnak vagy *szupraadditív hatásnak* nevez: a kár mértéke nem egyszerűen az egyes alrendszerek kiesésének összege, hanem annál több, mert a párhuzamosan fellépő zavarok egymást erősítik (Rinaldi *et al.*, 2001). Ahogy Rinaldi és munkatársai (2001) hangsúlyozzák, a kritikus infrastruktúrák védelmének tervezésekor elengedhetetlen ezen kölcsönhatások figyelembevétele, különben a védelem tervezői alulbecsülhetik egy-egy támadás potenciális következményeit.

A hálózatelméleti elemzés tehát két fő tanulsággal szolgál a lichterfeldei eset kapcsán: egyrészt szükséges a kritikus csomópontok és élek azonosítása és védelme (műszaki és fizikai biztonsági intézkedésekkel egyaránt); másrészt fontos a rendszerszintű, hálózatok közötti kapcsolatok megértése, hogy a vészhelyzeti tervezés során számításba vegyük a dominóeffektust. E megfontolások az alábbi kockázatmenedzsment elemzésben is visszaköszönnek majd.

Kockázatmenedzsment és felkészülés hiányosságai

A kritikus infrastruktúrák védelmének sarokköve a kockázatmenedzsment megközelítés, melynek célja, hogy azonosítsa a potenciális fenyegetéseket, felmérje a sebezhetőségeket, és ezek ismeretében csökkentse a várható következmények súlyosságát (DHS, 2013). A lichterfeldei

támadás tükrében érdemes megvizsgálni, milyen kockázatkezelési tanulságok adódnak, azaz mire mutat rá ez az incidens a megelőző tervezés és felkészülés terén.

A kockázatmenedzsment folyamatának klasszikus lépései közé tartozik a kockázatértékelés, amely tipikusan a *fenyegetés, sebezhetőség és következmény* hármasának elemzésére épül (DHS, 2013; Magee, 2018). Jelen esetben a fenyegetés egy ismert szélsőséges csoport részéről érkezett, amelynek infrastruktúra-ellenes akciói több mint egy évtizedre vezethetők vissza (CBS News, 2026). A német hatóságok birtokában voltak olyan hírszerzési és elhárítási információk, amelyek szerint a Vulkangruppe és hasonló anarchista sejtjei aktívak a térségben, és rendszeresen hajtanak végre szabotázsokat (Cook, 2026). Felmerül a kérdés, hogy a fenyegetésvalószínűség megfelelően lett-e értékelve vajon a kritikus infrastruktúra üzemeltetők és a hatóságok számoltak-e egy ilyen jellegű támadás realitásával? A kockázatelemzés második eleme, a sebezhetőség kapcsán látható, hogy a szóban forgó kábelhíd és vezetékek védelme nem volt kellően megoldva: a támadók viszonylag kis ráfordítással (feltehetően gyújtószer használatával) komoly károkat tudtak okozni (CBS News, 2026). Ez arra utal, hogy a fizikai védelem (pl. megfigyelő rendszerek, őrzés, behatolásjelzés) és a mérnöki védelem (pl. tűzálló burkolat, automatikus eloltó rendszerek) terén hiányosság állt fenn ennél a létesítménynél. Végül a következmények súlyosságát azaz, hogy egy sikeres támadás milyen mértékű szolgáltatáskiesést és társadalmi zavarokat okozhat talán szintén alábecsülték a tervezés során. Berlin esetében lehetséges, hogy a hálózati redundancia nem felelt meg a „N-1 kritériumnak" (az elvárásnak, hogy bármely egyetlen elem kiesése ne okozzon szolgáltatás-kimaradást). A kockázatmenedzsment nézőpontjából mindez azt jelenti, hogy a kockázatcsökkentő intézkedések nem bizonyultak kellően hatékonynak: a fenyegetés realitását és a sebezhetőség mértékét alulbecsülhették, így a bekövetkező kár nagysága meghaladta az elfogadható szintet.

Fontos megjegyezni, hogy a kritikus infrastruktúrák kockázatkezelése nem pusztán műszaki kérdés, hanem szabályozási és szervezési feladat is. A németországi reakció beleértve a KRITIS törvénytervezetet arra utal, hogy a döntéshozók felismerték: átfogóbb, *rendszerszintű kockázatkezelési tervezésre* van szükség (Vassileva, 2026). Ennek része egy olyan kereszt-szektoriális szemlélet, amely egyszerre veszi figyelembe az energia, közlekedés, távközlés, vízellátás stb. területek közötti kölcsönös függőségeket (Šarūnienė *et al.*, 2024). A friss kutatások szerint a több szektoron átívelő, *multi-hazard* (többféle veszélyforrást egyszerre kezelő) kockázatértékelési módszerek képesek csak megragadni a mai komplex fenyegetési környezetet (Šarūnienė *et al.*, 2024). Ez azt jelenti, hogy a kockázatelemzésbe be kell építeni olyan forgatókönyveket is, mint például szándékos fizikai támadás kombinálva kibertámadással vagy természeti csapással hiszen a valóságban az ilyen események akár egymást erősítve is jelentkezhetnek.

A proaktív kockázatkezelés fontos eleme a megelőző biztonsági intézkedések bevezetése mellett az is, hogy felkészülünk a legrosszabb esetre. Berlin példája azt mutatja, hogy bár történt vészhelyzeti tervezés (pl. aggregátorok, mobil generátorok bevetése, szükségmenedékek nyitása), a helyreállítás így is több napot vett igénybe (Cook, 2026). Ez felveti a kérdést, hogy a helyreállítási tervek és gyakorlatok elégségesek voltak-e. A kockázatmenedzsment körforgásának utolsó fázisa a tanulságok levonása és a visszacsatolás: a bekövetkezett incidenst alaposan ki kell értékelni, és ennek alapján frissíteni a kockázatkezelési terveket (DHS, 2013).

Jelen esetben például nyilvánvalóvá vált, hogy nagy szükség van a fizikai biztonság fokozására (pl. kritikus csomópontok jobb őrzése, védelme), a hálózati redundancia növelésére (alternatív vezetési útvonalak kialakítása), valamint a krízistervek továbbfejlesztésére (gyorsabb helyreállítási képességek kiépítésére).

Összességében a lichterfeldei támadás kockázatmenedzsment szempontból azt az üzenetet hordozza, hogy a hagyományos tervezésben rejlő hiányosságokat egy integrált, interdiszciplináris megközelítéssel kell orvosolni. Ide tartozik a *fenyegetésértékelésben* a hírszerzési inputok hatékony felhasználása, a *sebezhetőség csökkentésében* a mérnöki és technológiai innovációk alkalmazása, valamint a *következménykezelésben* a válságkommunikáció és vészhelyzeti elhárítás módszereinek előtérbe helyezése. Ezek közül a következő szakaszokban a válságkommunikáció és a hírszerzés szerepét emeljük ki részletesebben.

Válságkommunikáció: a lakosság tájékoztatása és a pánik megelőzése

Egy kritikus infrastruktúrát érintő katasztrófa vagy támadás esetén legyen az áramszünet, ivóvíz-szennyezés vagy éppen kiberrendszerek leállása a válságkommunikáció kulcsfontosságú szerepet játszik a károk mérséklésében és a társadalmi rend fenntartásában. A válságkommunikáció lényege, hogy a hatóságok gyorsan, pontosan és megnyugtató módon tájékoztassák az érintett lakosságot a helyzetről, az elérhető segítségről és a várható fejleményekről (Reynolds & Seeger, 2005). Kutatások igazolják, hogy az időben és hitelesen közvetített információ csökkenti a bizonytalanságot és a pánikot, növeli a lakosság együttműködését, és javítja a krízishelyzetek kezelésének hatékonyságát (Reynolds & Seeger, 2005; Pérez Moreira *et al.*, 2024).

A lichterfeldei áramszünet során Berlin városvezetése több kommunikációs csatornát is igénybe vett, igazodva a lehetőségekhez. Mivel az áramszünet miatt sok háztartásban nem működtek a szokásos információs eszközök (TV, internet, rádió töltő hiányában), a hatóságok innovatív megoldásokhoz folyamodtak: a rendőrség hangosbemondókon keresztül adott tájékoztatást a lakosoknak közvetlenül az utcákon (CBS News, 2026). Emellett a kormányzat és a közműszolgáltató cég (Stromnetz Berlin) folyamatosan informálta a médiát és a közösségi platformokon keresztül a nyilvánosságot a helyreállítás előrehaladtáról és arról, hogy várhatóan mikorra tér vissza az áramszolgáltatás (Cook, 2026). A rendszeresen frissített hírek például, hogy a szolgáltató ideiglenes megkerülő vezetéket épített ki, és mely területeken sikerült már helyreállítani a hálózatot segítettek a lakosság bizalmának fenntartásában, mert azt mutatták, hogy a helyzet kézben van tartva, és zajlik a megoldás (Cook, 2026). Fontos volt hangsúlyozni, hogy a hatóságok mindent megtesznek: például a tűzoltók és műszaki szakemberek éjjel-nappal dolgoztak a károk elhárításán, mobil aggregátorokat telepítettek kritikus létesítményekhez (kórházakhoz), és a teljes ellátás helyreállítását csütörtök délutánra ígérték (Cook, 2026).

A berlini válságkommunikációs gyakorlat jónéhány bevett elvet követett, amelyek megfelelnek a nemzetközi legjobb gyakorlatnak. Az egyik ilyen elv a transzparencia és őszinteség: a hatóságok nem titkolták el a probléma súlyosságát (például nyíltan kimondták, hogy a második világháború utáni idők leghosszabb áramszünetéről van szó), ugyanakkor igyekeztek keretet adni a

helyzetnek azzal, hogy határidőt szabtak a megoldásra (Reynolds & Seeger, 2005). Egy másik fontos elv a lakosság segítése az alkalmazkodásban: ennek jegyében nyitották meg a melegedőközpontokat, biztosítottak vízvételi és fürdési lehetőséget, és adtak tanácsokat (pl. takarékoskodjanak a mobiltelefon akkumulátorával, keressék fel a rászoruló szomszédokat) ezekről pedig kommunikáltak is, hogy minden érintett értesüljön (Cook, 2026). Harmadrészt, a kommunikációnak empatikusnak kell lennie: a városvezetők elismerték a helyzet nehézségeit és kifejezték együttérzésüket a lakosokkal, miközben biztosították őket arról, hogy az elkövetőket keresik és felelősségre vonják (CBS News, 2026; Cook, 2026).

Érdemes kitérni a technológiai kihívásokra is: egy áramszünet során a hagyományos tömegtájékoztatási csatornák egy része kieshet, ezért redundáns kommunikációs tervekre van szükség. A Berlinben látott hangosbemondós módszer kreatív példája annak, hogyan lehet eljuttatni az információt olyan körülmények között, amikor a modern infrastruktúra egy része nem elérhető. A jövőre nézve a válságkommunikációs tervekben számolni kell azzal, hogy "low-tech" eszközöket is alkalmazzanak, például közösségi riasztórendszereket, szórólapokat, személyes tájékoztatást igénybe véve. Mindemellett a hatóságoknak a közösségi médiát is figyelniük és használniuk kell: a krízis idején ugyanis gyorsan terjedhetnek pletykák és álhírek. A Berlinben történtekkel kapcsolatban is megjelent néhány összeesküvés-elmélet és téves információ az online térben, de a hivatalos szervek igyekeztek gyorsan cáfolni és korrigálni ezeket, ami szintén a hatékony válságkommunikáció része.

A berlini áramszünet tapasztalatai megerősítik, hogy a válságkommunikáció hatása kézzelfogható: a lakosság körében nem tört ki pánik, sikerült elkerülni a komolyabb közrendet sértő incidenseket, és az emberek együttműködtek az utasítások betartásában (pl. energiatakarékosság, közlekedési korlátozások elfogadása). Amint azt Pérez Moreira és kollégái (2024) tanulmánya is alátámasztja: az elektromos hálózat meghibásodásainál az eredményes kríziskommunikáció közvetlenül hozzájárul a közösség rezilienciájához, mivel elősegíti, hogy az emberek megfelelően reagáljanak, és kihasználja a rendelkezésre álló alternatív erőforrásokat (pl. aggregátorok, megújuló energiaforrások, szomszédsági segítségnyújtás). Így a válságkommunikáció nem csupán „puha tényező", hanem a kritikus infrastruktúrák védelmének integráns része, amely a műszaki intézkedésekkel párhuzamosan fejleszthető és gyakorolható.

Hírszerzési és biztonsági elemzés: a megelőzés és elhárítás szerepe

A kritikus infrastruktúrákat fenyegető szándékos támadások különösen a terrorizmus és a szervezett szabotázsakciók elleni védelem fontos pillére a hírszerzés és az elhárítás. Az ilyen fenyegetésekre való felkészülésben kulcsszerepet játszik az, hogy a biztonsági szolgálatok és a rendvédelmi szervek időben információkat gyűjtsenek és elemezzenek a potenciális elkövetőkről, terveikről és képességeikről (Magee, 2018). Az intelligencia elemzésének célja, hogy még a támadások bekövetkezése előtt figyelmeztető jeleket azonosítson, feltérképezze a fenyegetések hálózatát, és megossza az információkat azokkal, akik meg tudják tenni a szükséges védelmi lépéseket (Department of Homeland Security, 2015, idézi Magee, 2018).

A lichterfeldei eset rávilágít arra, hogy még egy fejlett nagyvárosban is előfordulhat: a támadók tervei a cselekmény elkövetéséig rejtve maradnak a hatóságok előtt. Bár a Vulkangruppe

tevékenységi köre ismert volt a német alkotmányvédelmi hivatal (BfV) számára hiszen a csoportot és szimpatizánsi hálózatát már évek óta megfigyelés alatt tartották, és tisztában voltak vele, hogy évente több millió eurós kárt okoznak infrastrukturális szabotázsakciókkal (Cook, 2026) –, konkrétan ezt a támadást mégsem sikerült megelőzni. Felmerül a kérdés, hogy lehetett-e olyan előjel (pl. kommunikáció az elkövetők között, gyanús terepszemle a helyszínen, online fenyegetés), amit észre lehetett volna venni és riasztást kiadni. Az ilyen utólagos kérdések gyakoriak egy-egy támadás után, és arra mutatnak, hogy a hírszerzési folyamatnak vannak korlátai, illetve hogy szükség van a tanulságok levonására (pl. jövőben figyelni az energia-infrastruktúrát kritizáló szélsőséges fórumokat, blogbejegyzéseket).

A hírszerzési elemzés terén létezik egy megközelítés, amelyet Aden Magee (2018) a kritikus infrastruktúra-védelem kapcsán hangsúlyoz: az *"intelligence targeting"*, azaz a célzott hírszerzési célkiválasztás szemlélete. Ennek lényege, hogy a védelmi tervezők az ellenfél szemével nézve is elemezzék a saját infrastruktúráikat. A katonai és terrorista tervezők ugyanis módszeresen feltérképezik az ellenséges kritikus infrastruktúrákat, keresve azokat a kritikus csomópontokat és gyenge pontokat, amelyek megtámadásával aránytalanul nagy hatást érhetnek el (Magee, 2018). Ezzel szemben figyelmeztet Magee a békeidőben működő infrastruktúra-menedzserek olykor megelégszenek egy *belső nézőpontú* kockázatelemzéssel, ami a saját rendszerük megerősítésére fókuszál, de nem számol egy kreatív és elszánt támadó stratégiájával (Magee, 2018). A lichterfeldei kábelhíd esete is ezt példázza: valószínű, hogy az üzemeltető inkább az erőmű területének védelmére koncentrált ("inside the wire" szemlélet), míg a támadók a kerítésen kívüli, nyilvános területen futó kábelhidat választották célnak kihasználva a védelmi logika vakfoltját. Az ilyen helyzetek elkerülésére a szakértők azt javasolják, hogy a kritikus infrastruktúrák védelmét tervező csoportokban kapjanak helyet hírszerzői/red-teaming szakértők, akik célzottan azonosítják azokat a sérülékenységeket, amiket egy ellenséges gondolkodású fél kihasználhat (Magee, 2018). A *red teaming* módszerrel amelynek során a védelmi oldalt játszó szakemberek az ellenfél fejével gondolkodva próbálnak "támadási" terveket készíteni felszínre hozhatók az olyan gyenge pontok is, amelyek egy hagyományos mérnöki szemlélet elől rejtve maradhatnak (Magee, 2018).

A hírszerzés és információmegosztás területén a lichterfeldei támadás egyik tanulsága, hogy erősíteni kell a kommunikációt az infrastruktúra-üzemeltetők és a biztonsági szervek között. Ha például a hálózat üzemeltetői tisztában lettek volna azzal, hogy szélsőséges csoportok érdeklődhetnek a hálózat bizonyos pontjai iránt netán kaptak volna előre jelzést a hatóságoktól fokozott fenyegetésről –, talán jobban felkészülhettek volna (pl. ideiglenes járőrözés, extra kamerafigyelés bevezetésével). Az Egyesült Államokban már a 2000-es évek elején kialakult egy modell a kritikus infrastruktúra fenyegetés-információk megosztására, amelyben az érintett magánszektorbeli partnerek és az állami hírszerző szervek együttműködnek (DHS, 2013). Ezt a modellt Európában is igyekeznek erősíteni, például az EU új reziliencia-irányelve és a NIS2 kiberbiztonsági irányelv is előír bizonyos információmegosztási kötelezettségeket a szolgáltatók és hatóságok között (Šarūnienė *et al.*, 2024; Vassileva, 2026). Természetesen ezeknek az együttműködéseknek megvannak a kihívásai: bizalmi kérdések, az érzékeny adatok védelme, a reagálás késlekedése stb. de a lichterfeldei incidens valószínűleg lendületet adott a német hatóságoknak is, hogy javítsák az ilyen partnerségeket.

Végül fontos kiemelni, hogy a hírszerzés nem csak a megelőzést szolgálja, hanem a reagálást és felderítést is. A támadást követően a begyűjtött információk (például a helyszínről, tanúktól, online térben közzétett vállalások) segítettek gyorsan azonosítani az elkövetői kört (Cook, 2026). A digitalizált világban a szélsőséges csoportok gyakran vállalják tetteiket az interneten, ahogy a Vulkangruppe is tette ezt a fajta nyilvános információt a hírszerzés "nyílt forrású" komponense (OSINT) keretében lehet hasznosítani. A hatékony hírszerzés tehát többrétegű: magában foglalja az emberi forrásokat (HUMINT), a műszaki megfigyelést (SIGINT) és az nyílt információk elemzését, melyek együttesen adhatnak teljes képet egy fenyegetésről (Lowenthal, 2017). Az így szerzett ismeretek birtokában a kritikus infrastruktúrák védelme hatékonyabban szervezhető meg, hiszen a védekezés a legvalószínűbb és legveszélyesebb forgatókönyvekre koncentrálhat.

Összefoglalva, a lichterfeldei eset hírszerzési tanulságai közé sorolhatjuk: (1) a támadó gondolkodásmód beépítésének szükségességét a védelmi tervezésbe (*"gondolkodj úgy, mint az ellenség"* elv alkalmazása); (2) a jobb együttműködést és információcserét az állami biztonsági szervek és az infrastruktúra-tulajdonosok között; (3) a fenyegetés-elemzés folyamatos finomítását a változó extremista taktikák fényében. Ezek a szempontok is azt erősítik, hogy a kritikus infrastruktúra-védelem nem szorítható egyetlen szakterület keretei közé a hírszerzési és biztonsági elemzés éppolyan fontos összetevője, mint a mérnöki lépések vagy a válságkezelés.

Az interdiszciplináris megközelítés szükségessége a kritikus infrastruktúra-védelemben

Az előző szakaszok külön-külön megvilágították, hogy a kritikus infrastruktúrák védelmének egyes aspektusai hálózati tervezés, kockázatmenedzsment, válságkommunikáció, hírszerzés mind saját szakmai mélységgel és tudásbázissal rendelkeznek. A lichterfeldei erőmű elleni támadás ugyanakkor egyértelműen megmutatta, hogy ezek a területek szorosan összefonódnak egy válsághelyzet során. Éppen ezért a hatékony védekezés és reagálás csak akkor valósulhat meg, ha az említett diszciplínák szakértői együttműködnek, és integrált szemlélettel közelítenek a problémához (Rinaldi *et al.*, 2001; Reynolds & Seeger, 2005; Magee, 2018).

Az interdiszciplináris megközelítés jelentőségét több érv is alátámasztja:

- Holisztikus kockázatfelismerés: Minden szakterület más lencsén keresztül azonosít kockázatokat. A mérnökök a műszaki hibákra és fizikai sérülékenységekre koncentrálnak, a biztonsági szakértők a fenyegető szándékra, a kommunikációs szakemberek a társadalmi reakciókra, míg a hálózatkutatók a rendszerstruktúra gyenge pontjaira. Csak ezen nézőpontok együttes figyelembevételével kaphatunk teljes képet a valós kockázatokról (DHS, 2013; Šarūnienė *et al.*, 2024).

- Megelőzés és felkészülés integrálása: Az egyes diszciplínák együttműködése biztosítja, hogy a megelőző intézkedések egymást erősítsék, ne pedig párhuzamosan, elszigetelten létezzenek. Például egy technikai hálózatbiztonsági fejlesztés (mint a redundáns kábelkapacitás kiépítése) csak akkor éri el célját, ha azt a hírszerzési elemzések is priorizálják (ti. valóban kritikus pont védelmét szolgálja), és ha a lakosság is értesül róla

(pl. áramkimaradás esetére tudják, mit tegyenek) vagyis a műszaki, hírszerzési és kommunikációs szál összeér (Lewis, 2015; Pérez Moreira *et al.*, 2024).

- Reagálóképesség és rugalmasság: Válsághelyzetben azonnali döntésekre van szükség, és ilyenkor az interdiszciplináris csapatok jobban teljesítenek. Ha egy válságkezelő törzsben ott ül az üzemeltetési mérnök, a kommunikációs vezető, a rendőrség/elhárítás képviselője és a hálózatelemző, akkor a döntéshozók minden fontos információ birtokában hozhatnak intézkedéseket. Ez a fajta közös helyzetértékelés és döntéstámogatás sokkal hatékonyabb, mintha utólag, külön-külön próbálnák összeilleszteni a képet (Reynolds & Seeger, 2005).

- Tanulás és adaptáció: Az interdiszciplináris megközelítés elősegíti a folyamatos fejlődést, mivel a különböző területek tanulnak egymástól. Egy incidens utáni felülvizsgálatnál például a hálózati szakemberek megérthetik a hírszerzőktől, hogy az ellenséges szereplők milyen logika mentén választanak célpontot, míg a hírszerzők tanulhatnak a mérnököktől a rendszer műszaki korlátairól. Ezáltal a következő iterációban már közös tudásbázissal rendelkeznek, ami finomítja a védelmi stratégiákat (Magee, 2018; Rinaldi *et al*., 2001).

A lichterfeldei támadás esetében felfedezhető, hogy ahol megvolt az interdiszciplináris összefogás csírája, ott jobban működött a védekezés. Ilyen például a válságstáb felállítása, amelyben a műszaki hibajavítást végző Stromnetz Berlin együtt dolgozott Berlin város polgári védelmi vezetésével és a rendőrséggel ennek köszönhetően sikerült koordináltan megszervezni az aggregátorok telepítését, a lakosság evakuálását egyes intézményekből és a kommunikációt. Ugyanakkor azok a területek, ahol nem volt meg az integráció (pl. a hírszerzés és a megelőző fizikai védelem között), sérülékenynek bizonyultak.

Összességében kijelenthetjük, hogy a kritikus infrastruktúrák védelme természeténél fogva interdiszciplináris kihívás (Lewis, 2015). A fizikai infrastruktúra, a kiber-infrastruktúra, az emberi tényező és a környezeti hatások mind befolyásolják a biztonságot. Az ehhez értő szakemberek eltérő háttérrel rendelkeznek mérnökök, informatikusok, közgazdászok, szociológusok, biztonságpolitikai elemzők, kommunikációs szakértők stb. és a siker záloga az, hogy közös nyelvet és együttműködési keretet alakítsanak ki. Az interdiszciplináris szemlélet nemcsak a védelem tervezésekor, hanem az oktatásban és kutatásban is fontos: a biztonságtudományi képzéseknek és a kutatóprogramoknak integrálniuk kell a különböző területeket, hogy a jövő szakemberei már eleve holisztikus látásmóddal rendelkezzenek (Rinaldi *et al*., 2001).

Következtetések

A Lichterfeldei erőmű elleni támadás és az annak nyomán kialakult többnapos áramszünet egyértelmű figyelmeztetésként szolgál arra, hogy a modern, összekapcsolt társadalmakban a kritikus infrastruktúrák védelme mennyire összetett és sokrétű feladat. A tanulmányban bemutatott eset rávilágított arra, hogy egyetlen, viszonylag egyszerű módszerrel végrehajtott szabotázsakció (kábelgyújtogatás) is súlyos zavarokat okozhat, ha az infrastruktúra rendszerjellegét kihasználva a támadás egy gyenge pontot ér el. Láttuk, hogy a keletkezett károk nem csak az energiaszektort, hanem dominóhatásként számos más létfontosságú szolgáltatást is érintettek bizonyítva a kritikus infrastruktúrák közötti kölcsönös függések jelentőségét.

Az esettanulmány elemzése során több nézőpontból megvizsgáltuk a történteket, és mindegyik perspektíva saját tanulsággal szolgált. Hálózatelméleti oldalról kiemeltük a rendszer- és hálózat szemlélet fontosságát a sebezhetőségek felismerésében: a kritikus csomópontok védelme és a redundancia biztosítása alapvető feladat. Kockázatmenedzsmenti szempontból rámutattunk, hogy a fenyegetések, sebezhetőségek és potenciális következmények szisztematikus értékelése nélkülözhetetlen és a berlini eset fényében e folyamat hiányosságai hozzájárultak a válság kialakulásához. Válságkommunikációs nézőpontból láthattuk, hogy a hatóságok megfelelő tájékoztatása és a lakosság bevonása mennyire kritikus a pánik megelőzésében és a társadalmi nyugalom fenntartásában, valamint hogy a kommunikáció hiánya vagy késedelme tovább súlyosbíthatná a helyzetet. Végül a hírszerzési elemzés rávilágított arra, hogy az ilyen támadások megelőzésében és felderítésében mennyire kulcsfontosságú a proaktív információgyűjtés, az ellenfél szemszögének átvétele és a biztonsági együttműködések erősítése.

A legfőbb következtetés, amely a fenti elemzésekből adódik, az az, hogy a kritikus infrastruktúrák védelme csak interdiszciplináris megközelítéssel lehet eredményes. Nem elegendő pusztán a technikai intézkedésekre hagyatkozni, ahogy az sem járható út, hogy csak a rendvédelmi/hírszerzői aspektusra fókuszáljunk, vagy éppenséggel kizárólag a válság utókezelésére. Minden komponensre szükség van, és azoknak egymást kiegészítve kell működniük. A Lichterfeldei támadás tanulságai alapján az alábbi ajánlások fogalmazhatók meg a jövőre nézve:

1. Hálózatbiztonsági fejlesztések: Azonosítani kell a kritikus infrastruktúra-hálózatok legsebezhetőbb pontjait, és *célzott védelmi beruházásokat* kell eszközölni (pl. fizikai védelem, redundáns útvonalak, tartalék rendszerek kiépítése) ezekre a pontokra (Albert *et al.*, 2004; Rinaldi *et al*., 2001).

2. Kockázatkezelési tervezés és gyakorlatok: Rendszeres kockázatfelméréseket kell végezni, beleértve a legújabb fenyegetési trendeket (pl. politikai szélsőséges csoportok aktivitását), és ennek alapján frissíteni a védelmi stratégiákat. Évente több szektort átívelő gyakorlatok szükségesek, amelyek tesztelik a vészhelyzeti reagálást és az együttműködést a különböző szervek között (DHS, 2013; Šarūnienė *et al*., 2024).

3. Válságkommunikációs protokollok: Kidolgozott tervekre van szükség arra az esetre, ha a hagyományos kommunikációs csatornák kiesnek. Ennek része a lakosság előzetes felkészítése (pl. tudják, hol találnak információt áramszünet esetén, milyen készleteket halmozzanak fel), valamint a sokcsatornás kommunikáció biztosítása vészhelyzetben (Reynolds & Seeger, 2005; Pérez Moreira *et al*., 2024).

4. Hírszerzési és elhárítási integráció: Erősíteni kell a kapcsolatot az infrastruktúra üzemeltetők és a hírszerző/elhárító szervek között. Információmegosztó fórumokat, közös elemző munkacsoportokat célszerű létrehozni, ahol *konkrét fenyegetési információk* cserélnek gazdát, beleértve a kibertérben zajló potenciális előkészületeket is (Magee, 2018).

5. Interdiszciplináris együttműködés és oktatás: Létre kell hozni olyan *koordinációs testületeket* (akár helyi, regionális, országos szinten), amelyek összehozzák a különböző

szakterületek képviselőit a kritikus infrastruktúra-védelem témakörében. Emellett támogatni kell az olyan oktatási programokat és kutatásokat, amelyek hidat képeznek a műszaki tudományok, a társadalomtudományok és a biztonsági tanulmányok között a KI-védelem területén (Rinaldi *et al*., 2001).

A lichterfeldei eset szerencsére nem járt halálos áldozatokkal, de *költséges figyelmeztetés* volt mind a döntéshozók, mind a szakemberek számára. Ahogy Berlin polgármestere fogalmazott: "ez nem csíny, hanem terrorizmus" azaz komoly fenyegetés, amire komoly választ kell adni (CBS News, 2026). A válasznak pedig a jelen tanulmány érvelése szerint komplexnek és sokoldalúnak kell lennie. A kritikus infrastruktúrák a modern élet gerincét alkotják; védelmük ezért nem bízható egyetlen tudományágra vagy intézményre. Csak az *összefogás*, a tudások és erőforrások egyesítése révén érhető el az a biztonsági szint és reziliencia, ami garantálhatja, hogy egy hasonló támadás a jövőben ne okozhasson ekkora fennakadást, vagy ha be is következik, a következmények kezelhetőbbek legyenek. A Lichterfeldei esemény tanulságai tehát messze túlmutatnak Berlin határain: globális üzenetként szolgálnak minden ország számára, hogy a kritikus infrastruktúrák védelme közös ügy, és csak interdiszciplináris megközelítéssel lehet eredményes.

Irodalomjegyzék

Albert, R., Albert, I., & Nakarado, G. L. (2004). Structural vulnerability of the North American power grid. *Physical Review E, 69*(2), 025103.

CBS News. (2026, January 5). *Berlin mayor calls left-wing arson attack behind massive power outage terrorism that endangers lives*. CBS News. https://www.cbsnews.com/news/berlin-power-outage-vulkangruppe-left-wing-arson-attack-called-terrorism/

Cook, E. (2026, January 7). *Berlin plunged into darkness after left-wing attack: What we know*. Newsweek. https://www.newsweek.com/berlin-electricity-grid-darkness-left-wing-attack-11320980

Department of Homeland Security. (2013). *NIPP 2013: Partnering for critical infrastructure security and resilience*. Washington, DC: DHS.

Lewis, T. G. (2015). *Critical infrastructure protection in homeland security: Defending a networked nation* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Magee, A. (2018, November 18). Perspective: An intelligence targeting approach to critical infrastructure protection. *Homeland Security Today*. https://www.hstoday.us/subject-matter-areas/intelligence/perspective-an-intelligence-targeting-approach-to-critical-infrastructure-protection/

Pérez Moreira, D. U., Guerra Sánchez, K. I., Buenaño Moyano, L. F., & Tasán Cruz, D. (2024). Impact of crisis communication on electrical failure management during natural disasters: The role of renewables in system resilience. *Journal of International Crisis and Risk Communication Research, 7*(S6), 1432–1440.

Reynolds, B., & Seeger, M. W. (2005). Crisis and emergency risk communication as an integrative model. *Journal of Health Communication, 10*(1), 43–55.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine, 21*(6), 11–25.

Šarūnienė, I., Martišauskas, L., Krikštolaitis, R., Augutis, J., & Setola, R. (2024). Risk assessment of critical infrastructures: A methodology based on criticality of infrastructure elements. *Reliability Engineering & System Safety, 243*, 109797.

Vassileva, A. (2026, January 7). *Berlin power outage puts focus on critical infrastructure security*. Renewables Now. https://renewablesnow.com/news/berlin-power-outage-puts-focus-on-critical-infrastructure-security-1287594/

#	Hivatkozás (röviden)	Típus	Link
1	Albert, R., Albert, I., & Nakarado, G. L. (2004). *Structural vulnerability of the North American power grid.*	Tudományos cikk (Physical Review E)	(APS Links)
2	CBS News (2026). *Berlin mayor calls left-wing arson attack behind massive power outage terrorism that endangers lives.*	Hírportál cikk	(CBS News)
3	Cook, E. (2026). *Berlin plunged into darkness after left-wing attack: What we know*. Newsweek.	Hírmagazin cikk	(Newsweek)
4	Department of Homeland Security. (2013). *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience.*	Nemzeti infrastruktúravédelmi terv (jelentés)	(NIST)
5	Lewis, T. G. (Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation).	Szakkönyv (Wiley)	(Wiley)
6	Magee, A. (2018). *Perspective: An intelligence targeting approach to critical infrastructure protection.* Homeland Security Today.	Szakcikk / elemzés	(HSToday)
7	Pérez Moreira, D. U. et al. (2024). *Impact of crisis communication on electrical failure management during natural disasters…*	Szakcikk	**file:///C:/Users/kocsi/Downloads/5.pdf**
8	Reynolds, B., & Seeger, M. W. (2005). *Crisis and emergency risk communication as an integrative model.*	Tudományos cikk (Journal of Health Communication)	(Europe PMC)

#	Hivatkozás (röviden)	Típus	Link
9	Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). *Identifying, understanding, and analyzing critical infrastructure interdependencies.*	Tudományos cikk (IEEE Control Systems Magazine)	(OSTI)
10	Šarūnienė, I. et al. (2024). *Risk assessment of critical infrastructures: A methodology based on criticality of infrastructure elements.*	Tudományos cikk (Reliability Engineering & System Safety)	(ScienceDirect)
11	Vassileva, A. (2026). *Berlin power outage puts focus on critical infrastructure security.* Renewables Now.	Szakmai hír/elemzés	(Renewables Now)

Dr. Bérczi László PhD Tűzoltó dandártábornok

Igazságügyi szakértő

Belügyminisztérium

Kocsis Zoltán Iparbiztonsági szakértő

az ECIP Kft tulajdonosa,

a Pannon Egyetem Mérnöki Kar Fenntarthatósági Megoldások Kutatólaboratórium oktatója