A KIBERBŰNÖZÉS KÖRNYEZETI HATÁSAI: A KIBERCSALÁSOK ÉS A TISZTA ENERGIA PARADOXONA*

Süvöltős Zsuzsa[1]

A XXI. század két globális rendszerszintű kockázata: a klímaválság és a kiberbűnözés, a kritikus infrastruktúrák digitalizációja révén szorosan összefonódik. Jelen tanulmány a megújuló energiaforrásokra való áttérés (zöld átállás) és a nemzetközi kiberjog kapcsolódási pontjait elemzi, középpontjában a tiszta energia paradoxona áll: miközben a szén-dioxid-kibocsátás csökkentése támogatja a villamosenergia-hálózatok decentralizálását és digitális korszerűsítését, ez a folyamat drasztikusan növeli a kibertámadások kockázatát, a klímafinanszírozás és a kibocsátás-kereskedelem új célpontokat teremt a szervezett kiberbűnözés számára. A tanulmány büntetőjogi szempontból vizsgálja a kritikus infrastruktúrák üzemeltetőinek felelősségét, a nemzetközi kiberjog (különösen a Tallinni Kézikönyv) klímaváltozás által súlyosbított támadások esetén történő alkalmazhatóságát, valamint a zöld gazdaságot érintő adathalász csalások szabályozási hiányosságait.

1. A tiszta energia paradoxona és a kritikus infrastruktúrák jogi védelme

A klímaváltozás és a kiberbiztonsági kockázatok kölcsönhatását tekintve a nemzetközi jog és a biztonságpolitika gyakran elkülönült szabályozási területként kezelte a környezetvédelmi jogot és a kiberbiztonsági szabályozást. A szakirodalom szerint a klímaválság súlyosbodása új kockázati helyzeteket teremt, átalakítja a kiberbűnözési mintázatokat, és felerősítheti a digitális rendszerek rendszerszintű sérülékenységét.[2]

Az extrém meteorológiai jelenségek és környezeti krízishelyzetek nem csupán fizikai megterhelést rónak a kritikus infrastruktúrákra, hanem olyan strukturális és társadalmi anomáliákat idéznek elő, amelyeket a kiberbűnözői csoportok – és az egyes esetekben velük kapcsolatba hozható állami szereplők – célzottan, aránytalan előnyök szerzésére használhatnak fel.[3] A tanulmány e problémakört megragadva, büntetőjogi szempontból vizsgálja a kritikus infrastruktúrák üzemeltetőinek felelősségét, a nemzetközi kiberjog alkalmazhatóságának kérdését, valamint az adathalász csalások szabályozási hiányosságait.

---

* DOI 10.21867/KjK/2026.3.2.

[1] *Dr. Süvöltős Zsuzsa,* bíró

[2] Gruber, Carolyn – Pytlak, Allison (2025): *Cyber and climate threats: Shared risks, resilience, and response strategies.* Stimson Center, 2025. március 4. https://www.stimson.org/2025/cyber-and-climate-threats-shared-risks-resilience-and-response-strategies/ (letöltés dátuma: 2026. október 11.) Ibraheem, Idris Olanrewaju–Bello-Ahmed, Lateefat (2025): Green tech, safe networks: The role of cybersecurity in combating climate change. Discover Internet of Things, Vol. 5., Article 58. https://doi.org/10.1007/s43926-025-00125-5

[3] Gruber–Pytlak (2025): *i.m.*

1.1. A decentralizált hálózatok (Smart Grid) mint jogi sebezhetőségi pontok

A fosszilis tüzelőanyagokról a megújuló energiára való áttérés megköveteli a villamosenergia-hálózat átalakítását. A centralizált, néhány nagy erőművön alapuló rendszert egyre nagyobb részben kiegészíti a decentralizált, intelligens mérőeszközök, IoT-eszközök és a magáncélú mikrohálózatok millióit tömörítő struktúra. Jogi értelemben ez a hálózati demokratizálódás a védelemre szoruló hálózati elemek körét bővíti, a kritikus infrastruktúrává minősítés azonban a jogszabályi feltételektől függ.[4]

A szabályozási probléma gyökere, hogy míg a hagyományos erőművek szigorú nemzetbiztonsági és kiberbiztonsági protokollok hatálya alá estek, a fogyasztói oldalon megjelenő okoseszközök és magánjellegű napelemes inverterek gyártóival és üzemeltetőivel szemben nem támasztanak azonos szintű követelményeket, ami felveti a termékbiztonsági, a termékfelelősségi és az üzemeltetői felelősségi szabályok összehangolásának kérdését arra az esetre, ha egy rosszul védett fogyasztói eszközön keresztül indított támadás veszélyezteti az országos energiahálózat működését.[5]

Erre a közvetlen veszélyre egyebekben a Nemzetközi Energia Ügynökség (IEA) legfrissebb jelentései is rámutatnak, az empirikus adatok szerint a kritikus energetikai infrastruktúrákat érő komplex kibertámadások száma globális szinten exponenciális növekedést mutat.6

Ha például egy állam területéről kiinduló hackercsoport egy klímakatasztrófa okozta hálózati túlterheltséget vagy üzemzavart kihasználva hajt végre támadást egy másik állam intelligens villamosenergia-hálózata ellen, a nemzetközi jogi attribúció – azaz a cselekmény államnak való felróhatósága –

[4] Ibraheem–Bello-Ahmed (2025): i.m. Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv). HL L 333., 2022.12.27., 80–152. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32022L2555 (letöltés dátuma: 2026. október 11.) 2–3. cikk, I. melléklet. Tressler, Judah (2025): *The Clean Energy Paradox: Unmasking Hidden Cyber Threats in Our Green Transition.* LinkedIn Pulse, 2025. május 19. https://www.linkedin.com/pulse/clean-energy-paradox-unmasking-hidden-cyber-threats-our-tressler-92ojc (letöltés dátuma: 2026. október 11.)

[5] Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, továbbá az (EU) 2020/1828 irányelv módosításáról (kiberrezilienciáról szóló rendelet). HL L, 2024/2847, 2024.11.20. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32024R2847 (letöltés dátuma: 2026. október 11.) 13–14. cikk.

[6] International Energy Agency (2024): *Electricity 2024: Analysis and forecast to 2026.* Paris, IEA. https://iea.blob.core.windows.net/assets/6b2fd954-2017-408e-bf08-952fdd62118a/Electricity2024-Analysisandforecastto2026.pdf (letöltés dátuma: 2026. október 11.) International Energy Agency (2025): *Energy and AI.* AI and energy security. Paris, IEA. https://www.iea.org/reports/energy-and-ai/ai-and-energy-security (letöltés dátuma: 2026. október 11.) „Cyberattacks per week per energy organisation, 2020–2024" ábra.

de facto ellehetetlenülhet a digitális nyomok sérülékenysége és manipulálhatósága miatt.[7]

1.2. Kibercsalások a zöld gazdaságban

A zöld gazdaságot érintő kibercsalások és a transznacionális bűnszervezetek működési mechanizmusainak feltárása során a Nemzetközi Szervezett Bűnözés Elleni Globális Kezdeményezés (Global Initiative Against Transnational Organized Crime) legfrissebb kutatási eredményei, szakpolitikai jelentései, valamint empirikus adatai jelentenek kiindulópontot annak megértéséhez, miként használja ki a szervezett bűnözés a környezeti krízisek és a zöld átállás szabályozási réseit a kibertérben.[8]

A klímaválság enyhítésére létrehozott pénzügyi alapok és a szén-dioxid kvóták (karbonkreditek) kereskedelmi rendszerei a kiberbűnözők elsődleges célpontjaivá válhatnak, a felügyeleti mechanizmusok pedig strukturális hiányosságokat mutatnak.[9]

A bűnszervezetek kifinomult adathalász (phishing) kampányokkal, hamis zöld befektetési platformokkal és identitáslopással (identity theft) milliárdos összegeket vonnak el a tényleges klímavédelmi projektektől, amely körülmény jogi szempontból felveti a pénzügyi felügyeleti szervek és a platformüzemeltetők mögöttes felelősségét a nem megfelelő ügyfél-átvilágítási (KYC – Know Your Customer) protokollok miatt.[10]

A zöld gazdaságot érintő, kifinomult pénzügyi csalásoknak nagyon jó gyakorlati példája a Zephyr Energy PLC (2026) ellen elkövetett kibertámadás.[11] A technológiavezérelt, tiszta energiaprojektekre is fókuszáló brit vállalat egyik amerikai leányvállalatát egy úgynevezett üzleti e-mail kompromittálásra (BEC)

---

[7] International Law Commission (2001): Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. Yearbook of the International Law Commission, 2001, Vol. II., Part Two. https://legal.un.org/ilc/texts/instruments/English/commentaries/9_6_2001.pdf (Letöltés dátuma: 2026. október 11.) 4., 8. és 11. cikk. Egyesült Nemzetek Szervezete (1945): Az Egyesült Nemzetek Alapokmánya. https://www.un.org/en/about-us/un-charter/full-text (letöltés dátuma: 2026. október 11.) 2. cikk (4) bekezdés. Schmitt, Michael N. (szerk.) (2017): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge, Cambridge University Press. https://ccdcoe.org/research/tallinn-manual/ (letöltés dátuma: 2026. október 11.) 69. és 71. szabály.

[8] Macbeath, Alastair (2025): *A climate of criminality: The organized crime–climate change nexus.* Global Initiative Against Transnational Organized Crime, 2025. november 14. https://globalinitiative.net/analysis/a-climate-of-criminality/ (letöltés dátuma: 2026. október 11.)

[9] INTERPOL (2013): *Guide to Carbon Trading Crime.* Lyon, INTERPOL, 2013. június. https://www.interpol.int/content/download/5172/file/Guide%20to%20Carbon%20Trading%20Crime.pdf (letöltés dátuma: 2026. október 11.) a kibocsátás-kereskedelmi piacok és a kereskedelmi bűncselekmények áttekintése.

[10] INTERPOL (2013): i.m. az áfacsalásról és a pénzmosásról szóló részek. Aguirre, B. E.–Lane, David (2019): Fraud in disaster: Rethinking the phases. International Journal of Disaster Risk Reduction, Vol. 39., Article 101232. https://doi.org/10.1016/j.ijdrr.2019.101232

[11] Zephyr Energy plc (2026): *Cybersecurity incident.* RNS Number: 7163Z, 2026. április 9. https://data.fca.org.uk/artefacts/NSM/RNS/7a1bddd4-4ebc-40c3-9d32-841ebf646163.html (letöltés dátuma: 2026. október 11.)

épülő támadás érte. A kiberbűnözők észrevétlenül beépültek a cég belső kommunikációjába, majd egy rutinszerű, külső alvállalkozónak szánt utalás során manipulálták a számlázási folyamatot, és a banki adatok módosításával jogosulatlanul egy hacker által ellenőrzött számlára irányították át az összeget.

Az incidens közvetlen következményeként a vállalatot mintegy 700.000 font kár érte. Bár a Zephyr Energy bevett gyakorlatként alkalmazta az iparági védelmi sztenderdeket, a támadás rávilágított arra, hogy a hagyományos biztonsági rendszerek önmagukban már nem nyújtanak teljes körű védelmet. A cég a hatóságok bevonása mellett azonnal szigorúbb ellenőrzési szinteket épített be a kifizetési munkafolyamataiba, a történtek pedig példaként szolgálnak arra, hogyan képes egyetlen adathalászattal kombinált manipuláció súlyos anyagi veszteséget okozni a modern energiaszektor szereplőinek.[12]

Hasonlóak a Maire Tecnimont-ügy büntetőjogi tanulságai. Az energiaszektort célzó adathalászati és fizetés-átirányítási csalások nem csupán vállalatirányítási, hanem súlyos büntetőjogi kérdéseket is felvetnek, amit a Maire Tecnimont esete szemléltet a leginkább. Ebben az ügyben a kínai hackerek a vállalat olaszországi vezérigazgatójának kiadva magukat (CEO fraud) vették rá az indiai leányvállalat pénzügyi vezetőit - fiktív kínai cégfelvásárlásra hivatkozva – 18,5 millió dollár átutalására.[13] A csalás büntetőjogi relevanciáját az adja, hogy a nyomozó hatóságoknak és az ügyészségnek a klasszikus csalási tényállások mellett a számítástechnikai rendszer és adatok elleni bűncselekmények, a pénzmosás, valamint a nemzetközi bűnszervezetben való részvétel vádját is bizonyítaniuk kellett a digitális nyomok alapján. Végül vádemelésre nem került sor, polgári peres úton próbálja a szaudi leányvállalat a brit NatWest bankkal szemben érvényesíteni a vagyoni igényét, amely kártérítés iránti eljárás jelenleg is folyamatban van a Londoni Felsőbíróság Kereskedelmi Bíróságán.

Az ilyen típusú elkövetéseknél a vádhatóságok világszerte komoly bizonyítási nehézségekkel küzdenek, mivel az elkövetők gyakran fejlett anonimizáló technológiákat használnak, a büntetőjogi felelősség megállapítása érdekében a hangsúly a pénzáramlás követésére és a pénzmosás elleni fellépésre helyeződik át, a strómanok és a „pénzügyi öszvérek” (money mules) hálózatának felszámolása mellett. Az eset rávilágít arra is, hogy a hagyományos csalási tényállásokban rögzített jogi keretek önmagukban elégtelenek, a modern

[12] Zephyr Energy (2026): i.m.

[13] Reuters (2019): *Chinese group swindles $18.5 million from Indian arm of Italian company – Economic Times.* 2019. január 10. https://uk.marketscreener.com/quote/stock/MAIRE-S-P-A-13369769/news/Maire-Tecnimont-Chinese-group-swindles-18-5-million-from-Indian-arm-of-Italian-company-Economic-27846733/ (letöltés dátuma: 2026. október 11.)

kiber-manipulációknál az elkövetői szándék bizonyításához elengedhetetlen a komplex igazságügyi szakértői bizonyítás.[14]

1.3. Adatmanipuláció és „fantom" karbonkreditek generálása. A C-Quest Capital-ügy

A karbonkreditek piacának egyik legveszélyesebb kiber-bűnügyi aspektusa a projektek digitális mérési és jelentéstételi rendszereinek (MRV) szándékos manipulálása.

A C-Quest Capital, a világ egyik legnagyobb önkéntes karbonkredit-fejlesztő vállalata ellen indított eljárás rávilágított arra, hogyan lehet az informatikai rendszereket hamis adatokkal feltölteni.15 Ebben az esetben az elkövetők éveken át módszeresen manipulálták a kibocsátáscsökkentési szoftverek bemeneti adatait, fiktív vagy nem működő zöld projekteket (pl. el sem helyezett energiatakarékos eszközöket) rögzítve a digitális adatbázisokban.[16]

Ezzel a kiber-manipulációval a szervezet több millió olyan „fantom" karbonkreditet (VCU) generált a hivatalos online regiszterekben, amelyek mögött semmilyen valós környezetvédelmi teljesítmény nem állt. A csalás révén a cégvezetés egy 250 millió dollár értékű befektetési kötelezettségvállalást szerzett meg jogtalanul, amelyből a visszaélés feltárásáig ténylegesen 170 millió dollárnyi tőkét hívtak le és realizáltak. Büntetőjogi szempontból az eset rávilágított, hogy a zöldpiaci kiberbűnözés nem feltétlenül külső hackertámadást jelent, a belső hozzáféréssel rendelkező elkövetők által végrehajtott adatmanipuláció és számítástechnikai csalás - szemben a hagyományos csalással - közvetlenül veszélyezteti a nemzetközi kibocsátás-kereskedelmi rendszerek integritását.[17]

---

[14] Europol (2025): *Steal, deal and repeat: How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment (IOCTA) 2025.* Luxembourg, Publications Office of the European Union. DOI: 10.2813/4926508. https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data (letöltés dátuma: 2026. október 11.) United Nations Office on Drugs and Crime (2013): *Comprehensive Study on Cybercrime.* Draft, 2013. február. Vienna, United Nations. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (letöltés dátuma: 2026. október 11.) a digitális bizonyítékok és a nemzetközi együttműködés fejezetei.

[15] U.S. Securities and Exchange Commission (2024): *In the Matter of CQC Impact Investors LLC.* Order Instituting Cease-and-Desist Proceedings, Making Findings, and Imposing a Cease-and-Desist Order. Securities Act Release No. 11315; Exchange Act Release No. 101232; Administrative Proceeding File No. 3-22224, 2024. október 2. https://www.sec.gov/files/litigation/admin/2024/33-11315.pdf (Letöltés dátuma: 2026. október 11.) III. rész, 1–5. pont. U.S. Department of Justice, U.S. Attorney's Office, Southern District of New York (2024): *U.S. Attorney Announces Criminal Charges in Multi-Year Fraud Scheme in the Market for Carbon Credits.* 2024. október 2. https://www.justice.gov/usao-sdny/pr/us-attorney-announces-criminal-charges-multi-year-fraud-scheme-market-carbon-credits (letöltés dátuma: 2026. október 11.)

[16] SEC (2024): i.m. III. rész, 13–17. pont.

[17] SEC (2024): *i.m*. III. rész, 18. pont és 2. lábjegyzet. U.S. Department of Justice (2024): *i.m.*

1.4. Zöld állami támogatások és adathalász kampányok (Energy Subsidy Phishing)

Míg a karbonkrediteknél a nagyvállalati szektor, addig a zöld támogatások területén a lakosság és a kisvállalkozások válnak a kibertámadások közvetlen célpontjaivá, kihasználva a kormányzati energiakorszerűsítési programok (pl. hőszivattyú- vagy napelemtámogatások) népszerűségét. A nemzetközi hatóságok, mint az ausztrál Scamwatch vagy a brit Citizens Advice által feltárt esetek kiberbűnügyi szempontból azonos sémát követnek, amikor a bűnszervezetek a hivatalos minisztériumi vagy hatósági oldalakat szinte tökéletesen másoló, klónozott weboldalakat és adathalász e-mail kampányokat indítanak.[18]

A fenntarthatósági narratívát eszközként használva (green halo effektus) a gyanútlan igénylőket arra késztetik, hogy az állami támogatás elnyerése érdekében adják meg érzékeny személyes adataikat, bankszámla-hozzáféréseiket vagy fizessenek be előre adminisztrációs díjakat. Csak az Egyesült Királyságban egyetlen év alatt több mint 5 millió állampolgárt céloztak meg ilyen típusú kibercsalásokkal.

Büntetőjogi szempontból ezek az esetek a számítástechnikai rendszer útján elkövetett csalás mellett a tömeges személyes adattal való visszaélés és identitáslopás minősített eseteit valósítják meg, ahol a digitális infrastruktúra biztosítja az elkövetők névtelenségét.[19]

Fentieken túl ezek a zöld gazdaságot érintő digitális visszaélések makrogazdasági szinten is megjelennek, amit az Európai Unió történetének egyik legnagyobb csalássorozata, a hírhedt „Carbon Prince" ügy is bizonyított, amelyben a bűnszervezet egy határokon átnyúló áfa-karusszel csalás során több száz millió eurós kárt okozott.[20] A bűncselekmény kifejezett kiber-vonatkozását az adta, hogy a karbonkvóta, amely egy tisztán digitális, immateriális vagyoni értékű jog, ezért a tranzakciók végrehajtásához nem volt szükség külön fizikai árura. A csalók adathalász kampányokkal és közvetlen kibertámadásokkal törték fel a nemzeti karbon-regisztereket, hogy legálisan működő vállalatok

[18] Australian Competition and Consumer Commission / Scamwatch (2011): *Continue to beware of scam solar offers.* 2011. szeptember 21. https://www.scamwatch.gov.au/about-us/news-and-alerts/continue-to-beware-of-scam-solar-offers (Letöltés dátuma: 2026. október 11.) Citizens Advice (2021): *19 million targeted by a green scam – here are five top tips on staying safe when making your home more energy efficient.* 2021. december 6. https://www.citizensadvice.org.uk/about-us/media-centre/press-releases/19-million-targeted-by-a-green-scam-here-are-five-top-tips-on-staying-safe-when-making-your-home-more-energy-efficient/ (letöltés dátuma: 2026. október 11.)

[19] Citizens Advice (2021): i.m. a 2021. évi felmérés eredményei. 2012. évi C. törvény a Büntető Törvénykönyvről, 219., 373., 375. és 422–423. §.

[20] Europol (2009): *Carbon Credit fraud causes more than 5 billion euros damage for European Taxpayer.* 2009. december 9. https://www.europol.europa.eu/media-press/newsroom/news/carbon-credit-fraud-causes-more-5-billion-euros-damage-for-european-taxpayer (Letöltés dátuma: 2026. október 11.) INTERPOL (2013): *i.m.* az áfa-karusszelről szóló rész.

számláiról kvótákat lopjanak el, majd azokat internetkapcsolaton keresztül, másodpercek alatt mossák tisztára a digitális tőzsdéken.[21]

A kiberbűnözői manipulációk végül olyan mértékű piaci anomáliákat és biztonsági kockázatokat okoztak, hogy az Európai Bizottság kénytelen volt ideiglenesen teljesen befagyasztani a teljes európai karbonkereskedelmet a rendszerszintű informatikai sebezhetőségek miatt.[22]

2. A klíma-kiber incidensek és tanulságaik

2.1. A texasi elektromos hálózat (ERCOT) válsága mint elvi modell

A 2021-es texasi energiaválság során a kritikus események láncreakciószerűen követték egymást, amelynek következtében a villamosenergia-hálózat mindössze 4 perc 37 másodpercre volt a teljes összeomlástól, amely az állam egész területén hónapokig tartó áramkimaradást okozhatott volna.[23] Az eset szerint 2021 februárjában egy rendkívüli sarkvidéki vihar - a „Sarki Örvény" (Winter Storm Uri) - érte el Texas államot, ahol a hőmérséklet évtizedek óta nem látott szintre süllyedt. Mivel Texasban a fűtés túlnyomórészt elektromos árammal működik, a lakosság egyszerre kapcsolta be a fűtőtesteket. A villamosenergia-kereslet rekordmagasságba, 67 gigawatt fölé ugrott, ami messze meghaladta a texasi hálózatirányító kapacitását.[24]

A fagy miatt a gázkitermelő kutak fejénél befagyott a kitermelt víz, így a gáz nem tudott áramlani a vezetékekben, a szélturbinák egy része eljegesedett és leállt, sőt, még az egyik atomerőmű is lekapcsolt egy megfagyott érzékelő miatt. Amikor a hálózat gyengülni kezdett, az elosztók lekapcsolták az áramot bizonyos körzetekben, ugyanakkor a kaotikus nyilvántartás miatt véletlenül olyan gázkompresszor-állomásoktól is elvették az áramot, amelyek a gázt pumpálták volna az erőművekbe. Ezzel az áramhiány gázhiányt okozott, a gázhiány pedig még nagyobb áramhiányt és így a hálózat kapacitásának közel 40-50%-a kiesett.[25]

Hogy megmentsék a hálózatot a fizikai megsemmisüléstől, az ERCOT az utolsó pillanatban, 4 perc 37 másodperccel a kritikus időhatár előtt elrendelte a

[21] INTERPOL (2013): i.m. a kvótalopásról és az adathalászatról szóló részek.

[22] European Commission (2011): *Update on transitional measure for EU ETS registries: Austria and Poland to resume operations on 7 March.* 2011. március 4. https://climate.ec.europa.eu/news-other-reads/news/update-transitional-measure-eu-ets-registries-austria-and-poland-resume-operations-7-march-2011-03-04_en (letöltés dátuma: 2026. október 11.)

[23] Federal Energy Regulatory Commission–North American Electric Reliability Corporation–Regional Entities (2021): *The February 2021 Cold Weather Outages in Texas and the South Central United States.* 2021. november. https://ferc.gov/sites/default/files/2021-11/cold%20weather%20report_%20november%202021.pdf (Letöltés dátuma: 2026. október 11.) az ERCOT frekvenciaeséséről és a terheléskorlátozásról szóló rész.

[24] FERC–NERC–Regional Entities (2021): *i.m.*

[25] FERC–NERC–Regional Entities (2021): *i.m*. a termelőegység-kiesések és a földgáz–villamos energia kölcsönfüggőség elemzése.

tömeges, kényszerített fogyasztói lekapcsolásokat, egész városrészeket és megyéket kapcsoltak le napokra teljesen a hálózatról.[26]

A hivatalos adatok szerint több mint 4,5 millió otthon és vállalkozás maradt áram, fűtés és ivóvíz nélkül[27], a hivatalos adatok szerint legalább 246 ember fagyott meg a saját otthonában, vagy halt meg szén-monoxid-mérgezésben, miközben az autójukkal vagy aggregátorokkal próbáltak fűteni[28], a gazdasági kár pedig elérte a 195–295 milliárd dollárt.[29]

Rengeteg energiakereskedő társaság hivatkozott a „vis maior" elvére, mondván, hogy az extrém időjárás miatt nem tudtak áramot szállítani. A bíróságoknak azt kellett mérlegelniük, hogy egy előrejelzett téli vihar valóban „kiszámíthatatlan" volt-e.

Az ERCOT-válság büntetőjogi szempontból levonható tanulsága a modern jogtörténet egyik legnagyobb paradoxonát és elvi vitáját eredményezte. Bár a katasztrófa több száz ember halálát és óriási anyagi kárt okozott, a klasszikus értelemben vett, magánszemélyek vagy vállalatok elleni közvetlen büntetőjogi elítélések elmaradtak, de az eset rávilágított arra, hogyan válik maga a jogrendszer a rendszerszintű felelősségrevonás akadályává, valamint arra is, hogy a jövőben a klímaváltozás miatti extrém időjárás egyre kevésbé fogadható el automatikus kimentési okként a szerződéses kötelezettségek alól.

A Texasi Legfelsőbb Bíróság 2023-ban kimondta, hogy az ERCOT – bár formálisan magánjogi szervezet – állami feladatot lát el, ezért szuverén mentességet élvez az időjárás okozta károk megtérítésére irányulóan indított polgári jogi perekben. Ez a polgári jogi döntés tehát a vezetők büntetőjogi felelősségét nem zárta ki, de annak megállapítására mégsem került sor, mivel a jogszabályok az extrém hidegre való felkészülést kötelezően nem írták elő, a mulasztás nem minősült kötelezettségszegésnek, így büntetőjogi felelősség sem volt megállapítható.A következmények az igazgatótanács egyes tagjainak lemondásában és a vezérigazgató távozásában realizálódtak.[30]

Bár a 2021-es texasi téli fagyok okozta hálózati összeomlás elsősorban infrastrukturális és meteorológiai okokra volt visszavezethető, a jogi és

[26] FERC–NERC–Regional Entities (2021*): i.m.* a frekvenciaesés és a terheléskorlátozás elemzése.
[27] FERC–NERC–Regional Entities (2021): *i.m.*
[28] Texas Department of State Health Services (2021): *February 2021 Winter Storm-Related Deaths – Texas.* 2021. december 31. https://www.dshs.texas.gov/sites/default/files/commprep/disasterepi/surveillance/SMOC_FebWinterStorm_MortalitySurvReport_12-30-21.pdf (Letöltés dátuma: 2026. október 11.) pp. 2–3., 7., 3. táblázat.
[29] The Perryman Group (2021): *Preliminary Estimates of Economic Costs of the February 2021 Texas Winter Storm.* 2021. február 25. https://www.perrymangroup.com/media/uploads/brief/perryman-preliminary-estimates-of-economic-costs-of-the-february-2021-texas-winter-storm-02-25-21.pdf (letöltés dátuma: 2026. október 11.) pp. 1–2.
[30] FERC–NERC–Regional Entities (2021): i.m. a téliesítési követelményekről és ajánlásokról szóló részek. Electric Reliability Council of Texas (2021): *Notice of Electric Reliability Council of Texas, Inc. Regarding Corporate Governance Status and Expected Vacancy of Chief Executive Officer Position.* Public Utility Commission of Texas, Project No. 51878, 2021. március 10. https://www.ercot.com/files/docs/2021/03/10/51878_Notice_ERCOT_Corporate_Governance_Status_Expected_CEO_Vacancy.pdf (letöltés dátuma: 2026. október 11.) pp. 1–3.

kiberbiztonsági szakértők - köztük a Guy Carpenter és az Industrial Cyber elemzői - azóta ezt az esetet használják alapmodellként az összetett „klíma-kiber" katasztrófák szimulációjára.[31]

2.2. Kibertámadások az energiaszektorban: trendek és adatok

Az energetikai szektor veszélyeztetettségéről szóló nemzetközi adatok szerint az utóbbi időben az egy hétre jutó támadások drasztikus növekedése figyelhető meg: A Nemzetközi Energia Ügynökség (IEA) hivatalos adatbázisa és a Check Point Cyber Security Report elemzései kimutatták, hogy az energiaszektor szervezeteit érő kibertámadások száma a 2020 és 2024 közötti időszakban folyamatosan és meredeken emelkedett.

Az energetikai vállalatok mára a kiberbűnözők egyik legfőbb célpontjává váltak, mivel a támadások közel 20%-a a létfontosságú közszolgáltatások és a közigazgatás ellen irányult.[32]

A zöld átállás biztonsági réseinek elemzése során a holland kutatók és a Holland Nemzeti Kiberbiztonsági Központ átfogó vizsgálata kimutatta, hogy 35 európai országban több mint 8500 olyan adminisztratív és hálózatirányítási rendszer működik a szél- és napenergia-ágazatban, amely közvetlen nyilvános internetes eléréssel rendelkezik, így a globális hálózat felől védtelenül hozzáférhető. A valós szabotázs-kockázatokat tekintve a kutatók becslése szerint ebből körülbelül 181 megújulóenergia-telephelyen a nem megfelelő konfiguráció miatt a hackerek számára technikailag lehetséges lett volna a turbinák és inverterek feletti irányítás átvétele, ami súlyos veszélyt jelent.[33]

A Dragos OT Report ipari kiberbiztonsági kutatásai az inverterek és akkumulátoros tárolók sebezhetőségével összefüggésben arra is rávilágítottak, hogy a hálózati akkumulátoros energiatároló rendszerekben tömegesen

---

[31] Guy Carpenter (2025): *Climate change x cyber: An intertwining risk.* https://gcstage65.www.guycarp.net/insights/2025/09/climate-change-x-cyber-an-intertwining-risk.html (Letöltés dátuma: 2026. október 11.) Ribeiro, Anna (2026): *Why industrial cybersecurity must evolve as climate disruption and digitalization reshape critical infrastructure.* Industrial Cyber, 2026. március 15. https://industrialcyber.co/features/why-industrial-cybersecurity-must-evolve-as-climate-disruption-and-digitalization-reshape-critical-infrastructure/ (letöltés dátuma: 2026. október 11.)

[32] IEA (2025): i.m. „Cyberattacks per week per energy organisation, 2020–2024" ábra. Check Point Software Technologies (2025): *The State of Cyber Security 2025.* 13th Annual Edition. https://www.checkpoint.com/resources/items/report-cyber-security-report-2025 (letöltés dátuma: 2026. október 11.) p. 33., 3. ábra.

[33] Modat (2026): *Modat research shows more than 8,500 exposed systems in Europe's wind and solar parks.* 2026. október 6. https://modat.io/blog/modat-research-exposed-systems-wind-and-solar/ (letöltés dátuma: 2026. október 11.) van den Berg, Stephanie–Sterling, Toby (2026): *Thousands of European wind and solar power systems exposed online, Dutch researchers say.* Reuters, 2026. október 6. https://www.reuters.com/technology/thousands-european-wind-solar-power-systems-exposed-online-dutch-researchers-say-2026-10-06/ (Letöltés dátuma: 2026. október 11.) Shanghai Metals Market (2026): *[SMM PV Flash] Nearly 8,000 European Solar Systems Found Exposed Online, Raising Cybersecurity Concerns.* 2026. október 8. https://news.metal.com/newscontent/104145195-smm-pv-flash-nearly-8000-european-solar-systems-found-exposed-online-raising-cybersecurity-concerns (letöltés dátuma: 2026. október 11.)

találhatók olyan hitelesítési hibák és a rendszerparancsok jogosulatlan futtatását lehetővé tévő biztonsági rések, amelyek révén a támadók közvetlenül manipulálhatják a hálózatra kapcsolt nagy teljesítményű áramátalakító invertereket, veszélyeztetve a hálózat feszültségstabilitását.[34]

Az informatikai eszköz felhasználásával elkövetett bűncselekmények közvetlen gazdasági károkat okoznak a hazai gazdasági szektorban is, a gazdasági és bűnügyi statisztikákban rögzített esetek mutatják a veszély nagyságát. A reprezentatív hazai piaci felmérések és kiberbiztonsági jelentések szerint tízből kilenc magyar nagyvállalatot (90%) ért már kibertámadás. Bár a vizsgált hazai cégek 75 százaléka, a nagyvállalatoknak pedig a 97 százaléka alkalmaz valamilyen összetettebb kibervédelmi megoldást, a kutatások szerint a legnagyobb problémát a „hamis biztonságérzet" jelenti, mivel a védelmi rendszerek sokszor nincsenek felkészítve a komplex, összetett fenyegetésekre.[35]

A magyarországi vállalati adatokból kirajzolódó sérülékenység és a jelentős pénzügyi károk rávilágítanak arra, hogy a hagyományos, reaktív védelmi vonalak már nemzeti szinten sem elegendőek a komplex fenyegetésekkel szemben.[36]

A fenti esetekből is megállapítható, hogy a hagyományos, reaktív rendszerek csupán a már bekövetkezett eseményekre reagálnak vagy ismert támadási mintákat keresnek, ezzel szemben a modern, proaktív megközelítés már a fenyegetések kialakulásának fázisában, valós időben avatkozik be. Ebben a folyamatban az MI kulcsszerepe a hálózati anomáliák intelligens felismerése és szétválasztása azzal, hogy a mesterséges intelligencia képes rendkívül magas, 93–96%-os pontossággal megkülönböztetni a külső, természetes környezeti hatások (például az időjárás okozta feszültségingadozások) által kiváltott hálózati zavarokat a tényleges, rosszindulatú kibertámadásoktól. Ez minimalizálja a téves riasztásokat és lehetővé teszi, hogy a védelmi rendszerek azonnal és célzottan reagáljanak a valódi veszélyekre, biztosítva a kritikus energetikai infrastruktúra folyamatos és biztonságos működését.[37]

Ezt a technológiai váltást és az MI hatékonyságát a legújabb tudományos modellek eredményei és a Smart Grid szimulációk is alátámasztják38, azt, hogy az okosmérők és alállomások elleni sikeres támadások a puszta áramkimaradáson túl magának a rendszernek az összeomlását és az inverterek fizikai meghibásodását is előidézhetik, emiatt a hálózatok fizikai integritásának

[34] Dragos (2026): *Dragos OT Cybersecurity Report: Adversaries Increase Real-World Impact, Map Control Loops Across Industrial Infrastructure.* 2026. február 17. https://www.dragos.com/resources/press-release/dragos-2026-year-in-review-new-ot-threats-ransomware (Letöltés dátuma: 2026. október 11.) a BESS-sebezhetőségekről szóló rész.

[35] One Solutions (2026): *A biztonság illúziója.* https://www.one.hu/static/documents/kozep-nagyvallalatok/One-Solutions_A_biztonsag_illuzioja_ebook.pdf (letöltés dátuma: 2026. október 11.)

[36] One Solutions (2026): *i.m.*

[37] Ibraheem–Bello-Ahmed (2025): *i.m*;. IEA (2025): i.m. „AI and cybersecurity: a two-way street" rész.

[38] Farooq, A.–Shahid, K.–Olsen, R. L. (2024): Securing the green grid: A data anomaly detection method for mitigating cyberattacks on smart meter measurements. International Journal of Critical Infrastructure Protection, Vol. 46., Article 100694. https://doi.org/10.1016/j.ijcip.2024.100694

megőrzése és a katasztrofális láncreakciók elkerülése érdekében elengedhetetlenné válik a hagyományos védelmi vonalak szabályozásának újragondolása.

3. Jogi felelősségi keretek: nemzetközi kiberjog és magyar büntetőjogi vonatkozások a környezeti válságok tükrében

Az Európai Unió a NIS 2 irányelvvel (Network and Information Security Directive) igyekezett választ adni erre a kihívásra, kiterjesztve a kötelezetti kört a megújulóenergia-ágazat szereplőire is. Az irányelv szigorú kockázatkezelési és incidens-bejelentési kötelezettségeket ír elő, azonban a klímaváltozás kontextusában a kockázatértékelésnek kombinált veszélyhelyzeteket is értékelnie kell, így például arra, hogy egy hőhullám miatti hálózati túlterheltség idején elkövetett zsarolóprogramos (ransomware) támadás milyen jogi következményekkel jár az üzemeltetőre nézve, amennyiben nem rendelkezett fizikailag leválasztott védelmi rendszerekkel.[39]

3.1. A Tallinni Kézikönyv relevanciája

A nemzetközi szokásjog alkalmazása a kibertérben továbbra is vitatott, de a Tallinni Kézikönyv iránymutatásai alapul szolgálnak a digitális konfliktusok jogi megítéléséhez. Ha egy állam által támogatott hackercsoport egy klímakatasztrófa, pl. egy hurrikán alatt támadja meg a célország energiahálózatát, a nemzetközi jogi attribúció, a támadás államhoz köthetősége rendkívül nehézzé válik, mivel a támadók elfedhetik tevékenységüket a természeti csapás okozta „hálózati zajban”.[40]

Ezzel összefüggésben kulcskérdés, hogy a nemzetközi humanitárius jog szempontjából az energetikai infrastruktúra és a vízművek elleni, környezeti krízis idején végrehajtott kibertámadások megsértik-e az erőszak alkalmazásának tilalmát az ENSZ Alapokmányának 2. cikk (4) bekezdése értelmében, különösen, ha a támadás közvetve humanitárius katasztrófához vezet.[41]

A nemzetközi jogban elfogadott konszenzus szerint a fizikai rombolás hiánya (pl. ha nem robban fel az erőmű, csak szoftveresen lekapcsolják) nem zárja ki az ENSZ Alapokmány 51. cikke szerinti önvédelmi jog megállapíthatóságát, amennyiben a támadás hatásának súlyossága (pl. a fűtés és vízművek hiánya miatti tömeges halálozás) eléri a kinetikus fegyverek pusztítási szintjét.[42]

Ilyen volt a zöld infrastruktúra elleni, válsághelyzetekkel összehangolt kibertámadások legfontosabb nemzetközi precedense, a Viasat műholdas

[39] (EU) 2022/2555 irányelv. 2–3., 20–23. cikk, I. melléklet.
[40] Schmitt (2017): *i.m.,* International Law Commission (2001): *i.m*. 8. és 11. cikk.
[41] ENSZ Alapokmány. 2. cikk (4) bekezdés. Schmitt (2017): i.m. 69. szabály.
[42] ENSZ Alapokmány. 51. cikk. Schmitt (2017): i.m. 71. szabály.

hálózat elleni kibercsapás, amely során a támadók egy kártékony szoftverrel megbénították a kommunikációt, a káosz okozta digitális zaj pedig sikeresen elfedte az elkövetők nyomait. A támadás dominóeffektusként azonnal átgyűrűzött a megújuló energia szektorba is, mivel Németországban több mint 5800 szélturbina távvezérlése és monitorozása állt le teljesen, kritikus stabilitási kockázat elé állítva az európai energiahálózatot.[43]

Azt, hogy az ilyen jellegű kiberszabotázsok már nem csupán elméleti problémák, azt a Nemzetközi Büntetőbíróság (ICC) legújabb joggyakorlata is bizonyítja.

Az ICC hivatalos eljárások keretében tette nyilvánvalóvá, hogy az energia- és közműhálózatok szoftveres bénítása a Római Statútum alapján háborús bűncselekménynek minősülhet, amennyiben az a civil lakosság aránytalan és súlyos szenvedését idézi elő.[44]

3.2. A kellő gondosság elve a klíma-kiber kontextusban

A nemzetközi jogban a kellő gondosság-elve (due diligence) írja elő, hogy az államok nem engedhetik meg, sőt kötelesek megakadályozni, hogy más államok a területüket sértő, jogellenes cselekményekre használják. A kellő gondosság kibertérbeli alkalmazásának egyik szakirodalmi értelmezése szerint az adott államnak az ismert, más államok jogait súlyosan sértő tevékenységek megszüntetésére észszerűen rendelkezésére álló intézkedéseket kell megtennie.[45]

Felmerül a kérdés, hogy a zöld átállás során a fejlődő országokban telepített transznacionális megújuló projektek esetében melyik államot terheli a jogi felelősség, ha a területén működő zöld infrastruktúráról indítanak globális kibercsalás sorozatot vagy ellátási lánc elleni támadást.[46]

A kellő gondosság elve a vállalati vezetők felelősségét a polgári jogi felelősségen túl is érintheti, hiszen a fenntarthatósági átvilágításról szóló (EU) 2024/1760 irányelv (CSDDD) és a NIS 2 irányelv a szakirodalom szerint együttesen rögzíti a vállaltok digitális gondossági kötelezettségének elvét (digital duty of care). Ennek értelmében a környezetvédelmi adatok, az emissziós rendszerek vagy a karbonkredit-nyilvántartások informatikai védelmének elhanyagolása nem pusztán mulasztás, hanem a büntetőjogi

[43] Viasat (2022): *KA-SAT Network cyber attack overview.* 2022. március 30. https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/ (Letöltés dátuma: 2026. október 11.) Sheahan, Maria–Steitz, Christoph–Rinke, Andreas (2022): *Satellite outage knocks out thousands of Enercon's wind turbines.* Reuters, 2022. február 28. https://finance.yahoo.com/news/1-satellite-outage-knocks-control-152923545.html (Letöltés dátuma: 2026. október 11.)

[44] International Criminal Court, Office of the Prosecutor (2025): *Policy on Cyber-Enabled Crimes under the Rome Statute.* 2025. december 3. https://www.icc-cpi.int/news/policy-cyber-enabled-crimes-under-rome-statute (Letöltés dátuma: 2026. október 11.)

[45] Schmitt (2017): *i.m.* 6–7. szabály.

[46] International Law Commission (2001): *i.m.* 4–11. cikk.

felelősség megállapítását is megalapozhatja, ha az adott tényállás gondatlan alakzata is büntetendő.[47]

A nemzetközi büntetőjogi szakirodalom szerint a szoftveres sebezhetőségek tudatos figyelmen kívül hagyása a büntetőjogban az eshetőleges szándék vagy a tudatos gondatlanság körébe eshet. A külföldi tanulmányok hangsúlyozzák, hogy a klímavédelmi vagy környezetirányítási adatok digitális manipulálása, illetve az adathalászattal vagy hackeléssel szerzett hozzáférések révén a zöld csalások kimerítik a gazdasági és környezeti bűncselekmények törvényi tényállását, ilyen módon a gondossági kötelezettség megszegése adminisztratív-irányítási mulasztásból közvetlen büntetőjogi felelősséget keletkeztető tényezővé léphet elő.[48]

3.3. A magyar büntető anyagi jogi szabályozás

A magyar jogalkotás a kiberbűnözés és az információs társadalom kihívásaira a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) keretein belül ad szisztematikus választ, az Európai Unió NIS 2 irányelvét Magyarország a kiberbiztonságról szóló 2024. évi LXIX. törvénnyel ültette a hazai jogrendbe.

A kriminológiai szakirodalom a kiberbűncselekményeket alapvetően két nagy kategóriára osztja.[49] Tisztán informatikai ún. kiberfüggő bűncselekmények (cyber-dependent) azok, amelyek informatikai rendszer nélkül nem követhetők el, és jellemzően az információs rendszert vagy adatot támadják (pl. zsarolóvírus, jogosulatlan belépés)[50], míg a számítógép felhasználásával elkövetett vagy ún. kibertámogatott bűncselekmények (cyber-enabled) azok a hagyományos bűncselekmények, amelyeknek az elkövetését az információs rendszer megkönnyíti vagy hatékonyabbá teszi.[51]

Az információs rendszerek elleni deliktumok, amelyeket a Btk. XLIII. fejezete önállóan rendel büntetni, ezek a 422.§ szerinti tiltott adatszerzés bűncselekménye, a 423. § szerinti információs rendszer vagy adat megsértése (pl. jogosulatlan belépés, adatmódosítás, DDoS támadások), valamint a 424. § szerinti, információs rendszer védelmét biztosító technikai intézkedés kijátszása.

Ugyanakkor a gazdasági és vagyon elleni kiberbűncselekmények – köztük a zöld gazdaságot és a mindennapi pénzügyeket leginkább veszélyeztető

[47] Az Európai Parlament és a Tanács (EU) 2024/1760 irányelve (2024. június 13.) a fenntarthatósággal kapcsolatos vállalati átvilágításról, valamint az (EU) 2019/1937 irányelv és az (EU) 2023/2859 rendelet módosításáról. HL L, 2024/1760, 2024.7.5. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32024L1760 (Letöltés dátuma: 2026. október 11.) (EU) 2022/2555 irányelv. 20–21. cikk. Btk. 4. és 8. §.

[48] Btk. 4., 8., 241., 323. és 375. §.

[49] Mezei Kitti (2020): A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre. *Állam- és Jogtudomány, 61*. évf., 4. sz., 65–81., 68–69.

[50] Mezei (2020): *i.m.* 68–69.

[51] Mezei (2020): *i.m.* 68–69.

adathalász csalások – a konkrét elkövetési módtól függően a 373. §-ban meghatározott csalás, a 375. §-ban rögzített információs rendszer felhasználásával elkövetett csalás, illetve más tényállás szerinti minősítést is megalapozhatnak, mint káreredménnyel járó, materiális bűncselekmények.

Megjegyzendő, hogy bár a Btk. „Környezet és a természet elleni bűncselekmények" XXIII. fejezete nem tartalmaz nevesített kiber-tényállást, a kritikus infrastruktúrák, pl. okos energiahálózatok elleni informatikai szabotázs a 323. §-ban szereplő közérdekű üzem működésének megzavarása szerint is büntetendő, amely környezeti katasztrófához vezetve súlyosabban minősülhet.

A klíma-kiber kontextusban – így különösen az intelligens villamosenergia-hálózatok sérelmére elkövetett informatikai szabotázsakciók esetén – a hatályos magyar anyagi büntetőjog alapján elsősorban a közérdekű üzem működésének megzavarása, valamint az információs rendszer vagy adat megsértése tényállásának megállapíthatósága merül fel, anyagi vagy alaki bűnhalmazatban.

Az információs rendszer vagy adat megsértése a kibertámadások központi tényállása, amely esetében a törvény három magatartást különít el, így a védelmi intézkedés megsértésével vagy kijátszásával történő jogosulatlan belépést (illetve a jogosultság kereteit túllépő bentmaradást), valamint az információs rendszer működésének jogosulatlan akadályozását és a rendszerben lévő adat jogosulatlan megváltoztatását, törlését vagy hozzáférhetetlenné tételét. A védett jogi tárgy ebben az esetben az információs rendszerek és az adatok bizalmassága, sértetlensége és rendelkezésre állása.
Megállapítható, hogy a klíma-kiber aspektusból főként a második bűncselekményi csoport bír relevanciával, a zsarolóvírus általi titkosítás az adat hozzáférhetetlenné tétele (pl. egy naperőmű-hálózat vagy vízmű adatai esetében), a szolgáltatásmegtagadásos támadás pedig a rendszer működésének akadályozása révén.

A törvény súlyosabban (2–8 évig terjedő szabadságvesztéssel) rendeli büntetni, ha az elkövetés közérdekű üzem ellen irányul, ami az energiahálózatok elleni támadásoknál külön minősítő körülmény és kiemelten bünteti, ha a támadás stratégiai célpontot ér.

A Btk. 459. § (1) bek. 21. pontja szerinti közérdekű üzemnek minősül többek között a közművek, az elektronikus hírközlő hálózatok, a közösségi közlekedési üzem és az energiaellátás is, amelyek működésének megzavarása a közbiztonság elleni bűncselekmények közé tartozik. A tényállás a működés jelentős mértékű megzavarását kívánja meg, ezért az adatok elleni támadás önmagában nem elegendő a megvalósulásához. Így amennyiben a kibertámadás ténylegesen megszakítja az áramszolgáltatást (például hőhullám vagy fagy idején), a 323.§ szerinti bűntett is megállapítható, feltéve, hogy a zavar jelentős mértékű. A büntetés alapesetben 1-5 évig, csoportosan, bűnszövetségben vagy különösen nagy kárt okozva 2-8 évig, fegyveresen, felfegyverkezve vagy különösen jelentős kárt okozva 5-10 évig terjedő szabadságvesztéssel büntetendő.

A gondatlan elkövetést az (5) bekezdés rendeli büntetni 3 évig terjedő, míg különösen nagy vagy azt meghaladó kárt okozása esetén 1-5 évig terjedő szabadságvesztéssel.

A fentieken túl a zöld pénzügyi bűncselekmények esetében releváns lehet a Btk. 373. § szerinti csalás és a Btk. 375. § szerinti információs rendszer felhasználásával elkövetett csalás is, amely az első tényállás esetében a tévedésbe ejtéssel vagy tévedésben tartással megvalósuló vagyoni haszonszerzést szankcionálja, míg ezzel szemben a másik az információs rendszerben tárolt, kezelt, feldolgozott adat vagy a rendszer működésének jogtalan befolyásolására épül, és nem igényli a tévedésbe ejtő magatartást. Az üzleti e-mail-kompromittálás és a CEO fraud esetén a pénzügyi vezető félrevezetése a 373. §, a bankszámla-adatok manipulálása pedig a 375. § szerint minősülhet a konkrét elkövetési magatartástól függően.

3.4. A NIS 2 irányelv és a büntetőjogi szankciók viszonya

A szabályozási környezet elemzése során elengedhetetlen a preventív jellegű európai uniós kiberbiztonsági normák és a megtorló funkciójú nemzeti büntetőjog dogmatikai elhatárolása.

A nemzetközi és hazai szakirodalomban megjelenő álláspontok szerint a NIS 2 által megkövetelt magas szintű adminisztratív védelem bevezetése közvetlenül befolyásolja a büntetőjogi felelősségre vonás megalapozottságát és irányát.[52]

A NIS 2 irányelv (illetve az azt átültető hazai kiberbiztonsági törvény) és a Btk. viszonya a klasszikus közigazgatási szakpolitikai jog és a büntető anyagi jog komplementer, egymást kiegészítő kapcsolatára épül,[53] ugyanakkor a két norma alapvetően eltér a szabályozás jellege, a felelősségre vonás alanya, valamint a jogkövetkezmények tekintetében.

A Kibertv. a szervezetekre és vezetőikre ex ante kockázatkezelési, incidensbejelentési és auditálási kötelezettségeket állapít meg, és ezek megszegését közigazgatási bírsággal szankcionálja, esetükben a felügyeletet a Szabályozott Tevékenységek Felügyeleti Hatósága látja el, míg az irányelv az alapvető fontosságú szervezetekre legalább 10 millió euróig, illetve a világszintű éves forgalom 2%-áig (a kettő közül a magasabb összegig) terjedő bírság kiszabását teszi lehetővé. A Btk. ezzel szemben ex post, a tényállást megvalósító, felróható magatartáshoz kapcsol büntetőjogi következményt – a közérdekű üzem működésének megzavarása esetén akár 10 évig terjedő szabadságvesztést. A büntetőjogi felelősség elsősorban természetes személyhez kötődik, a jogi személlyel szemben A jogi személlyel szemben alkalmazható büntetőjogi intézkedésekről szóló 2001. évi CIV. törvény szerinti intézkedések alkalmazhatók. A két szabályozás tehát nem zárja ki egymást, a Kibertv. szerinti kötelezettségek teljesítése vagy elmulasztása a gondatlanság megítélésénél

[52] (EU) 2022/2555 irányelv. 20–21. cikk. Btk. 8. §.
[53] Btk. 79. §. (EU) 2022/2555 irányelv. 20–21. cikk.

értékelhető körülmény, önmagában azonban nem alapoz meg büntetőjogi felelősséget.

Emellett a gondatlanság kapcsán kiemelendő, hogy ha egy megújulóenergia-szolgáltatót kibertámadás ér, és emiatt környezeti kár keletkezik, a büntetőbíróság a szolgáltató vezetőinek felelősségét az egyéni kötelezettség, annak megszegése, az okozati összefüggés, a gondatlanság és a tényállási eredmény vizsgálata alapján állapíthatja meg, ennek során a kiberbiztonsági előírásoknak jelentőségük lehet és annak, hogy a gazdasági társaság eleget tett-e a kiberbiztonsági törvényben és a NIS 2-ben előírt kötelezettségeknek. A kötelezettség megszegése önmagában nem elegendő, hiszen a Btk. 323.§ (5) szerinti közérdekű üzem megzavarása gondatlan alakzata csak valamennyi törvényi feltétel fennállásakor állapítható meg.[54]

Az elkövetők azonosítása terén pedig a NIS 2 által kötelezővé tett, a jelentős incidensről való tudomásszerzéstől számított 24 órán belüli korai előrejelzés, majd 72 órán belüli incidensbejelentés és naplózás biztosítja a digitális bizonyítékok azonnali rögzítését [55], amely bizonyítékok nélkül a nyomozó hatóságok lényegesen nehezebben tudnák a Btk. 423.§-a szerinti bűncselekményeket felderíteni a külföldi kiberbűnözői csoportokkal szemben.[56]

4. Nemzetközi bűnügyi együttműködés és korlátai

A közelmúltbeli összehasonlító jogi kutatások – így különösen a Journal of Legal Studies and Domestic Affairs elemzései – egyértelműen rámutattak arra, hogy a nem-technikai jellegű megelőzés, mint például a lakosság digitális tudatosságra nevelése, önmagában hatástalan a szervezett kiberbűnözéssel szemben. A bűnmegelőzés ezen formája kizárólag akkor bizonyulhat eredményesnek, ha a büntetőpolitika ezzel párhuzamosan differenciált elrettentő szankciókat alkalmaz a speciális célpontok, így a klímavédelmi és energetikai létfontosságú rendszerek védelmére. Az elemzések kiemelik, hogy a kiberbűnözés elleni fellépés legfőbb akadályai a joghatósági összeütközések, az elkövetők azonosításának nehézsége és az ok-okozati összefüggés bizonyítása.[57]

A területi elv alkalmazásának összetettségét és a joghatóság megállapíthatóságának nehézségeit mutatja, amikor az elkövető az „A” országban tartózkodik, a szerver a „B” országban található, a kár (pl. egy energiahálózat leállása miatt) pedig a „C” országban jelentkezik [58], az elkövető azonosítása esetében pedig a technikai anonimitás miatt teljesíthetők nehezen a büntetőjogi bizonyítási standardok, mivel a digitális nyomok könnyen manipulálhatók vagy megsemmisíthetők.

[54] Btk. 8. §; 323. § (1), (5) bekezdés. 2024. évi LXIX. törvény.
[55] (EU) 2022/2555 irányelv. 23. cikk (4) bekezdés a)–b) pont.
[56] UNODC (2013): *i.m.* a digitális bizonyítékokról szóló fejezet.
[57] Sorbán (2024): *i.m.* 7–26.
[58] Btk. 3. §. Budapesti Egyezmény. 22. cikk. Sorbán (2024): *i.m.* 7–26.

Mivel globális konszenzus hiányában nem létezik egységes nemzetközi kiberbíróság, a bűnüldöző hatóságok kénytelenek a transznacionális büntetőjog hagyományos eszközeire és az államok közötti két- vagy többoldalú jogsegélyegyezményekre (Mutual Legal Assistance Treaties – MLAT) támaszkodni.[59]

A Budapesti Egyezmény (2001) a kiberbűnözés elleni fellépés egyik legjelentősebb nemzetközi eszköze, amely a részes államokat kötelezi a kiberbűncselekmények anyagi jogi tényállásainak megalkotására és a gyorsított adatmegőrzés bevezetésére. Magyarország az Egyezményt a 2004. évi LXXIX. törvénnyel hirdette ki, a 2022-es Második Kiegészítő Jegyzőkönyv a határokon átnyúló elektronikus bizonyítékok szolgáltatóktól való közvetlen beszerzését könnyíti meg.

A nemzetközi bűnügyi együttműködés hatékonyságát jelentősen korlátozza a kettős kriminalizáció elvéből fakadó dogmatikai problematika. A transznacionális jogsegélynyújtás alapvető előfeltétele ugyanis, hogy a megkeresés alapjául szolgáló cselekmény mind a megkereső, mind a megkeresett állam anyagi büntetőjoga szerint bűncselekménynek minősüljön. Ez eljárási akadályt gördít a hatóságok elé abban az esetben, ha a zöld átállást célzó, új típusú kiber-csalások – így különösen a fiktív karbonkredit-kereskedelem vagy a zöld alapokat érintő online visszaélések – a megkeresett állam büntetőkódexében még nincsenek önálló törvényi tényállásként nevesítve. A jogalkotási aszimmetria következtében a határokon átnyúló nyomozások és a bizonyítékok beszerzése ellehetetlenülhet, ami a kiberbűnözők számára biztosíthat büntetlenséget.[60]

Ugyanakkor a legfrissebb külföldi tanulmányok és emberi jogi jelentések (pl. a Human Rights Watch 2026-os elemzései) arra is figyelmeztetnek, hogy a kiberbűnözés elleni túl szigorú büntetőjogi fellépés jogalkotási túlkapásokhoz vezethet.

Egyes autoriter államok a kiberbiztonság megelőzésére hivatkozva olyan büntetőjogi törvénytervezeteket nyújtanak be, amelyek a legitim digitális tevékenységeket, a zöld aktivizmust, sőt az etikus hackerek tevékenységét is kriminalizálják, ezzel korlátozva a szabad véleménynyilvánítást és a mozgásszabadságot.[61] A modern büntetőjog feladata tehát a külföldi doktrínák

[59] Sorbán (2024): *i.m.* 7–26. Az Európai Parlament és a Tanács 2014/41/EU irányelve (2014. április 3.) a büntetőügyekben kibocsátott európai nyomozási határozatról. HL L 130., 2014.5.1., 1–36. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32014L0041 (Letöltés dátuma: 2026. október 11.) Az Európai Parlament és a Tanács (EU) 2023/1543 rendelete (2023. július 12.) a büntetőeljárásban és a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából alkalmazott, elektronikus bizonyítékokra vonatkozó európai közlésre kötelező határozatokról és európai megőrzésre kötelező határozatokról. HL L 191., 2023.7.28., 118–138. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32023R1543 (letöltés dátuma: 2026. október 11.)

[60] Budapesti Egyezmény. 25. cikk (4) bekezdés; 29. cikk (3) bekezdés.

[61] Human Rights Watch (2026): *China: Cybercrime bill entrenches censorship, surveillance.* 2026. március 17. https://www.hrw.org/news/2026/03/17/china-cybercrime-bill-entrenches-censorship-surveillance (letöltés dátuma: 2026. október 11.)

szerint az elrettentés és az alapvető emberi jogok közötti kényes egyensúly fenntartása is.[62]

4.1. Határokon átnyúló elektronikus bizonyítás és az Europol Kiberbűnözés Elleni Központjának szerepe

A gyakorlati bűnüldözés szintjén a nemzetközi fellépés két pillérre támaszkodik, amelyek közül az első a határokon átnyúló elektronikus bizonyítás (E-evidence) megújult rendszere. Az új nemzetközi és európai uniós szabályozás – kiemelten az uniós E-evidence rendelet, valamint a Budapesti Egyezmény kiegészítő jegyzőkönyvei – jelentős újítást vezetett be a nyomozó hatóságok számára a közvetlen adatkérés intézményével.[63]

Ez a jogi konstrukció lehetővé teszi, hogy a nyomozást lefolytató szervek a hagyományos, gyakran hónapokig elhúzódó kölcsönös jogsegélyeljárási utat megkerülve, közvetlenül a külföldi illetékességű tech-szolgáltatóktól igényeljék a digitális bizonyítékokat, így az IP-címeket és a szervernaplókat. Ennek a megoldásnak a kulcsfontosságú előnye az időfaktor optimalizálása, ami kritikus jelentőséggel bír a kiberbűnözés kontextusában, hiszen megakadályozza, hogy az elkövetők idő előtt törölhessék vagy manipulálhassák az eljárás sikerét megalapozó digitális nyomokat.[64]

A transznacionális fellépés másik operatív pillérét az Europol Kiberbűnözés Elleni Központjának (EC3) speciális módszertana alkotja. Az EC3 a közös nyomozócsoportokban (Joint Investigation Teams – JITs) elemző és operatív támogatást nyújt a több állam joghatóságát érintő hálózatok felszámolásához, a csoportok létrehozása a tagállami hatóságok feladata Eurojust támogatásával. A központ hatékonyan összehangolja a rajtütéseket, foganatosítja az érintett szerverek nemzetközi lefoglalását, másfelől kiemelt hangsúlyt fektet a proaktív prevencióra is, így különösan az operatív állomány folyamatosan monitorozza a dark web fórumait, mélyrehatóan elemzi a zsarolóprogramok kriminológiai trendjeit, és korai figyelmeztető jelzéseket (Early Warning) bocsát ki a tagállamok nemzeti hatóságai felé a kritikus infrastruktúrákat fenyegető legújabb kiberveszélyekről.[65]

Megállapítható, hogy a határokon átnyúló elektronikus bizonyítási eljárások hatékonysága nagyban függ az Europol által biztosított operatív támogatástól. Ugyanakkor a normatív szabályozási törekvések és az operatív-technikai támogatási mechanizmusok sem képesek maradéktalanul áthidalni a fennálló strukturális hiányosságokat. A felelősségi keretek érvényesíthetőségét a bűncselekmények transznacionális és deterritorializált jellege számottevően

[62] Human Rights Watch (2026): *i.m.*
[63] (EU) 2023/1543 rendelet. 3–6. és 34. cikk. Második Kiegészítő Jegyzőkönyv (CETS 224). 6–8. cikk.
[64] (EU) 2023/1543 rendelet. 4–5., 7–10., 12. és 16. cikk. Második Kiegészítő Jegyzőkönyv (CETS 224). 6–8., 13–14. cikk.
[65] Europol: *Joint investigation teams.* https://www.europol.europa.eu/partners-collaboration/joint-investigation-teams (letöltés dátuma: 2026. október 11.), Europol (2025): *i.m.*

korlátozza, amely jelenség a globális kiberbűnözéssel szembeni fellépés egyik legjelentősebb strukturális aszimmetriájaként azonosítható.

***

A klímaválság és a kiberbűnözés nem egymástól független jelenségek, hanem egymást kölcsönösen erősítő, rendszerszintű kockázatok. A kiberbiztonsági prioritásokat nélkülöző, erőltetett ütemű zöld átállás a kritikus infrastruktúrák rendszerszintű sebezhetőségét megfelelő védelem hiányában növelheti: ez a folyamat teremti meg a tiszta energia paradoxonát, amelyben az ökológiai fenntarthatóságot célzó technológiai modernizáció egyúttal új kiberbiztonsági kockázatokat generál.[66]

A szabályozási környezetben azonosított diszfunkciók mérséklése céljából szakpolitikai és jogalkotási lépések megtétele válhat szükségszerűvé, így különösen a létfontosságú rendszerek, kritikus infrastruktúra fogalmának kiterjesztése, a hazai jogalkotásnak az uniós NIS 2 irányelven túlmutatóan kötelező biztonsági és tanúsítási szabályok előírása a lakossági és üzleti célú napelemes inverterek, okosmérők és helyi mikrohálózatok gyártói számára. Kulcsfontosságú lenne annak biztosítása is, hogy a magánszemélyek által használt okoseszközök ne szolgálhassanak könnyű belépési pontként a hackerek számára az országos energiahálózat irányába.[67]

Indokolt lehet a kombinált kockázatértékelési standardok bevezetése, így például a környezetvédelmi engedélyezési eljárások során a nagyobb zöld beruházásoknál (szél- és naperőműveknél) a klíma- és kiberkockázatok együttes hatásvizsgálatának kötelezővé tétele.

A zöld pénzügyi piacok kiberfókuszú szabályozása során a szén-dioxid-kvótákkal kereskedő oldalakat és a zöld beruházási alapokat terhelő ügyfél-átvilágítási, valamint pénzmosás elleni szabályokat szükséges lenne összehangolni a nemzetközi kiberbűnözés elleni egyezményekkel. Ezáltal hatékonyabban elejét lehetne venni annak, hogy a klímavédelmi pénzügyi források a digitális csalásokon keresztül a szervezett bűnözés finanszírozási forrásává váljanak.[68]

A nemzetközi jogi felelősség fogalmi meghatározásának pontosításával - akár a Tallinni Kézikönyv következő átdolgozott kiadásaiban vagy ENSZ-határozatokban - javasolt lenne egyértelműen rögzíteni, hogy a természeti katasztrófák idején elkövetett, kritikus infrastruktúrát célzó kibertámadások

[66] Gruber–Pytlak (2025): *i.m.*; Ibraheem–Bello-Ahmed (2025): *i.m.*
[67] (EU) 2024/2847 rendelet. 13–14. és 71. cikk. Andriani, Astri Dwi–Kaewnaknaew, Chirapat (2026): Green Governance Transition Policies and Cybersecurity for Sustainable Digital Infrastructures. *Advance Knowledge for Executives*, Vol. 5., No. 1., Article 66. https://www.researchgate.net/publication/406996468_Green_Governance_Transition_Policies_and_Cybersecurity_for_Sustainable_Digital_Infrastructures (letöltés dátuma: 2026. október 11.) 4.4. rész.
[68] (EU) 2022/2555 irányelv. 21. cikk. INTERPOL (2013): *i.m.*

büntetőjogi szempontból súlyosabban, humanitárius veszélyhelyzet okozása esetén pedig nemzetközi bűncselekményként minősüljenek.[69]

A kiberbűnözés környezeti hatásai nem csupán elméleti dilemmák, hanem a jelen valóságának monumentális kihívásai. A törékeny egyensúlyon alapuló, rendkívül töredezett nemzetközi politikai és társadalmi rendszerek, valamint a joghatósági akadályok jelenleg szinte lehetetlenné teszik a hatásos és egységes globális szintű fellépést.

Látható, hogy miközben a szén-dioxid-kibocsátás csökkentése érdekében rohamléptékben történik a kritikus infrastruktúrák digitalizációja, a jogi szabályozás tehetetlensége miatt a megújuló energiaforrások sebezhetőségéből fakadó kettősség közvetlen biztonsági kockázattá válik.

A klímavédelmi célok megvalósítása ezért nem járhat a kritikus rendszerek digitális kiszolgáltatottságával, a nemzeti és nemzetközi szintű szabályozásnak is olyan kereteket kell teremtenie, amelyben a környezeti fenntarthatóság és a technológiai biztonság egymást erősíti.

Források jegyzéke:

- Aguirre, B. E.–Lane, David (2019): Fraud in disaster: Rethinking the phases. I*nternational Journal of Disaster Risk Reduction,* Vol. 39., Article 101232. https://doi.org/10.1016/j.ijdrr.2019.101232
- Andriani, Astri Dwi–Kaewnaknaew, Chirapat (2026): Green Governance Transition Policies and Cybersecurity for Sustainable Digital Infrastructures. *Advance Knowledge for Executives*, Vol. 5., No. 1., Article 66. https://www.researchgate.net/publication/406996468_Green_Governance_Transition_Policies_and_Cybersecurity_for_Sustainable_Digital_Infrastructures (letöltés dátuma: 2026. október 11.)
- Australian Competition and Consumer Commission / Scamwatch (2011): Continue to beware of scam solar offers. 2011. szeptember 21. https://www.scamwatch.gov.au/about-us/news-and-alerts/continue-to-beware-of-scam-solar-offers (letöltés dátuma: 2026. október 11.)
- Check Point Software Technologies (2025): *The State of Cyber Security 2025*. 13th Annual Edition. https://www.checkpoint.com/resources/items/report-cyber-security-report-2025 (letöltés dátuma: 2026. október 11.)
- Citizens Advice (2021): 19 million targeted by a green scam – here are five top tips on staying safe when making your home more energy efficient. 2021. december 6. https://www.citizensadvice.org.uk/about-us/media-centre/press-releases/19-million-targeted-by-a-green-scam-here-are-five-top-tips-on-staying-safe-when-making-your-home-more-energy-efficient/ (letöltés dátuma: 2026. október 11.)

[69] Schmitt (2017): *i.m.;* ENSZ Alapokmány. International Law Commission (2001): *i.m.*

- Council of Europe (2022): Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. CETS No. 224. Strasbourg, 2022. május 12. https://rm.coe.int/1680a49dab (letöltés dátuma: 2026. október 11.)
- Dragos (2026): Dragos OT Cybersecurity Report: Adversaries Increase Real-World Impact, Map Control Loops Across Industrial Infrastructure. 2026. február 17. https://www.dragos.com/resources/press-release/dragos-2026-year-in-review-new-ot-threats-ransomware (letöltés dátuma: 2026. október 11.)
- Egyesült Nemzetek Szervezete (1945): Az Egyesült Nemzetek Alapokmánya.
- Electric Reliability Council of Texas (2021): Notice of Electric Reliability Council of Texas, Inc. Regarding Corporate Governance Status and Expected Vacancy of Chief Executive Officer Position. Public Utility Commission of Texas, Project No. 51878, 2021. március 10. https://www.ercot.com/files/docs/2021/03/10/51878_Notice_ERCOT_Corporate_Governance_Status_Expected_CEO_Vacancy.pdf (letöltés dátuma: 2026. október 11.)
- European Commission (2011): Update on transitional measure for EU ETS registries: Austria and Poland to resume operations on 7 March. 2011. március 4. https://climate.ec.europa.eu/news-other-reads/news/update-transitional-measure-eu-ets-registries-austria-and-poland-resume-operations-7-march-2011-03-04_en (letöltés dátuma: 2026. október 11.)
- Europol (2009): Carbon Credit fraud causes more than 5 billion euros damage for European Taxpayer. 2009. december 9. https://www.europol.europa.eu/media-press/newsroom/news/carbon-credit-fraud-causes-more-5-billion-euros-damage-for-european-taxpayer (letöltés dátuma: 2026. október 11.)
- Europol (2025): *Steal, deal and repeat: How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment (IOCTA) 2025*. Luxembourg, Publications Office of the European Union. DOI: 10.2813/4926508. https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data (Letöltés dátuma: 2026. október 11.)
- Europol (é. n.): Joint investigation teams. https://www.europol.europa.eu/partners-collaboration/joint-investigation-teams (letöltés dátuma: 2026. október 11.)
- Farooq, A.–Shahid, K.–Olsen, R. L. (2024): Securing the green grid: A data anomaly detection method for mitigating cyberattacks on smart meter measurements. *International Journal of Critical Infrastructure*

Protection, Vol. 46., Article 100694. https://doi.org/10.1016/j.ijcip.2024.100694

- Federal Energy Regulatory Commission–North American Electric Reliability Corporation–Regional Entities (2021): The February 2021 Cold Weather Outages in Texas and the South Central United States. 2021. november. https://ferc.gov/sites/default/files/2021-11/cold%20weather%20report_%20november%202021.pdf (letöltés dátuma: 2026. október 11.)
- Gruber, Carolyn–Pytlak, Allison (2025): *Cyber and climate threats: Shared risks, resilience, and response strategies.* Stimson Center, 2025. március 4. https://www.stimson.org/2025/cyber-and-climate-threats-shared-risks-resilience-and-response-strategies/ (Letöltés dátuma: 2026. október 11.)
- Guy Carpenter (2025): Climate change x cyber: An intertwining risk.
- https://gcstage65.www.guycarp.net/insights/2025/09/climate-change-x-cyber-an-intertwining-risk.html (letöltés dátuma: 2026. október 11.)
- https://njt.jog.gov.hu/jogszabaly/2024-69-00-00 (Letöltés dátuma: 2026. október 11.)
- https://www.un.org/en/about-us/un-charter/full-text (Letöltés dátuma: 2026. október 11.)
- https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/ (letöltés dátuma: 2026. október 11.)
- Human Rights Watch (2026): China: Cybercrime bill entrenches censorship, surveillance. 2026. március 17. https://www.hrw.org/news/2026/03/17/china-cybercrime-bill-entrenches-censorship-surveillance (letöltés dátuma: 2026. október 11.)
- Ibraheem, Idris Olanrewaju – Bello-Ahmed, Lateefat (2025): Green tech, safe networks: The role of cybersecurity in combating climate change. *Discover Internet of Things*, Vol. 5., Article 58. https://doi.org/10.1007/s43926-025-00125-5
- International Criminal Court, Office of the Prosecutor (2025): Policy on Cyber-Enabled Crimes under the Rome Statute. 2025. december 3. https://www.icc-cpi.int/news/policy-cyber-enabled-crimes-under-rome-statute (Letöltés dátuma: 2026. október 11.)
- International Energy Agency (2024): Electricity 2024: Analysis and forecast to 2026. Paris, IEA. https://iea.blob.core.windows.net/assets/6b2fd954-2017-408e-bf08-952fdd62118a/Electricity2024-Analysisandforecastto2026.pdf (letöltés dátuma: 2026. október 11.)
- International Energy Agency (2025): Energy and AI. AI and energy security. Paris, IEA. https://www.iea.org/reports/energy-and-ai/ai-and-energy-security (letöltés dátuma: 2026. október 11.)

- International Law Commission (2001): Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. Yearbook of the International Law Commission, 2001, Vol. II., Part Two. https://legal.un.org/ilc/texts/instruments/English/commentaries/9_6_2001.pdf (letöltés dátuma: 2026. október 11.)
- INTERPOL (2013): Guide to Carbon Trading Crime. Lyon, INTERPOL, 2013. június. https://www.interpol.int/content/download/5172/file/Guide%20to%20Carbon%20Trading%20Crime.pdf (letöltés dátuma: 2026. október 11.)
- Johansmeyer, Tom (2025): Bad decisions have consequences: How cyber security could fall victim to climate change. *British Actuarial Journal*, Vol. 30., Article e15. https://doi.org/10.1017/S1357321725000091
- Macbeath, Alastair (2025): A climate of criminality: The organized crime–climate change nexus. Global Initiative Against Transnational Organized Crime, 2025. november 14. https://globalinitiative.net/analysis/a-climate-of-criminality/ (letöltés dátuma: 2026. október 11.)
- Mezei Kitti (2020): A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre. *Állam- és Jogtudomány,* 61. évf., 4. sz., 65–81. https://jog.tk.elte.hu/uploads/files/2020-04-teljes.pdf (letöltés dátuma: 2026. október 11.)
- Modat (2026): Modat research shows more than 8,500 exposed systems in Europe's wind and solar parks. 2026. október 6. https://modat.io/blog/modat-research-exposed-systems-wind-and-solar/ (letöltés dátuma: 2026. október 11.)
- One Solutions (2026): A biztonság illúziója. https://www.one.hu/static/documents/kozep-nagyvallalatok/One-Solutions_A_biztonsag_illuzioja_ebook.pdf (letöltés dátuma: 2026. október 11.)
- Reuters (2019): Chinese group swindles $18.5 million from Indian arm of Italian company – Economic Times. 2019. január 10. https://uk.marketscreener.com/quote/stock/MAIRE-S-P-A-13369769/news/Maire-Tecnimont-Chinese-group-swindles-18-5-million-from-Indian-arm-of-Italian-company-Economic-27846733/ (letöltés dátuma: 2026. október 11.)
- Ribeiro, Anna (2026): Why industrial cybersecurity must evolve as climate disruption and digitalization reshape critical infrastructure. Industrial Cyber, 2026. március 15. https://industrialcyber.co/features/why-industrial-cybersecurity-must-evolve-as-climate-disruption-and-digitalization-reshape-critical-infrastructure/ (letöltés dátuma: 2026. október 11.)

- Schmitt, Michael N. (szerk.) (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge*, Cambridge University Press. https://ccdcoe.org/research/tallinn-manual/ (letöltés dátuma: 2026. október 11.)
- Shanghai Metals Market (2026): [SMM PV Flash] Nearly 8,000 European Solar Systems Found Exposed Online, Raising Cybersecurity Concerns. 2026. október 8. https://news.metal.com/newscontent/104145195-smm-pv-flash-nearly-8000-european-solar-systems-found-exposed-online-raising-cybersecurity-concerns (letöltés dátuma: 2026. október 11.)
- Sheahan, Maria–Steitz, Christoph–Rinke, Andreas (2022): Satellite outage knocks out thousands of Enercon's wind turbines. Reuters, 2022. február 28. https://finance.yahoo.com/news/1-satellite-outage-knocks-control-152923545.html (Letöltés dátuma: 2026. október 11.)
- Sorbán Kinga (2024): A jogellenes tartalomközléssel megvalósított kiberbűncselekmények elleni fellépés eljárásjogi dilemmái a nemzetközi együttműködésben. Belügyi Szemle, 72. évf., 1. sz., 7–26. https://doi.org/10.38146/BSZ.2024.1.1
- Supreme Court of Texas (2023): CPS Energy v. Electric Reliability Council of Texas, No. 22-0056; Electric Reliability Council of Texas, Inc. v. Panda Power Generation Infrastructure Fund, LLC et al., No. 22-0196. 2023. június 23. https://www.txcourts.gov/media/1456698/220056_220196.pdf (letöltés dátuma: 2026. október 11.)
- Texas Department of State Health Services (2021): February 2021 Winter Storm-Related Deaths – Texas. 2021. december 31. https://www.dshs.texas.gov/sites/default/files/commprep/disasterepi/surveillance/SMOC_FebWinterStorm_MortalitySurvReport_12-30-21.pdf (Letöltés dátuma: 2026. október 11.)
- The Irregular Warfare Initiative (2025): Cybersecurity's Climate Crisis. 2025. május 22. https://www.irregularwarfare.org/cybersecuritys-climate-crisis/ (letöltés dátuma: 2026. október 11.)
- The Perryman Group (2021): Preliminary Estimates of Economic Costs of the February 2021 *Texas Winter Storm.* 2021. február 25. https://www.perrymangroup.com/media/uploads/brief/perryman-preliminary-estimates-of-economic-costs-of-the-february-2021-texas-winter-storm-02-25-21.pdf (Letöltés dátuma: 2026. október 11.)
- Tressler, Judah (2025): The Clean Energy Paradox: Unmasking Hidden Cyber Threats in Our Green Transition. LinkedIn Pulse, 2025. május 19. https://www.linkedin.com/pulse/clean-energy-paradox-unmasking-hidden-cyber-threats-our-tressler-92ojc (Letöltés dátuma: 2026. október 11.)

- U.S. Department of Justice, U.S. Attorney's Office, Southern District of New York (2024): U.S. Attorney Announces Criminal Charges in Multi-Year Fraud Scheme in the Market for Carbon Credits. 2024. október 2. https://www.justice.gov/usao-sdny/pr/us-attorney-announces-criminal-charges-multi-year-fraud-scheme-market-carbon-credits (Letöltés dátuma: 2026. október 11.)
- U.S. Securities and Exchange Commission (2024): In the Matter of CQC Impact Investors LLC. Order Instituting Cease-and-Desist Proceedings, Making Findings, and Imposing a Cease-and-Desist Order. Securities Act Release No. 11315; Exchange Act Release No. 101232; Administrative Proceeding File No. 3-22224, 2024. október 2. https://www.sec.gov/files/litigation/admin/2024/33-11315.pdf (Letöltés dátuma: 2026. október 11.)
- United Nations Office on Drugs and Crime (2013): Comprehensive Study on Cybercrime. Draft, 2013. február. Vienna, United Nations. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (Letöltés dátuma: 2026. október 11.)
- Van den Berg, Stephanie–Sterling, Toby (2026): Thousands of European wind and solar power systems exposed online, Dutch researchers say. Reuters, 2026. október 6. https://www.reuters.com/technology/thousands-european-wind-solar-power-systems-exposed-online-dutch-researchers-say-2026-10-06/ (Letöltés dátuma: 2026. október 11.)
- Viasat (2022): KA-SAT Network cyber attack overview. 2022. március 30.
- Zephyr Energy plc (2026): Cybersecurity incident. RNS Number: 7163Z, 2026. április 9. https://data.fca.org.uk/artefacts/NSM/RNS/7a1bddd4-4ebc-40c3-9d32-841ebf646163.html (letöltés dátuma: 2026. október 11.)

- 2001. évi CIV. törvény a jogi személlyel szemben alkalmazható büntetőjogi intézkedésekről.
- 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt, Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.
- 2012. évi C. törvény a Büntető Törvénykönyvről.
- 2013. évi V. törvény a Polgári Törvénykönyvről.
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról.
- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148

irányelv hatályon kívül helyezéséről (NIS 2 irányelv). HL L 333., 2022.12.27., 80–152.

- Az Európai Parlament és a Tanács (EU) 2023/1543 rendelete (2023. július 12.) a büntetőeljárásban és a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából alkalmazott, elektronikus bizonyítékokra vonatkozó európai közlésre kötelező határozatokról és európai megőrzésre kötelező határozatokról. HL L 191., 2023.7.28., 118–138.
- Az Európai Parlament és a Tanács (EU) 2024/1760 irányelve (2024. június 13.) a fenntarthatósággal kapcsolatos vállalati átvilágításról, valamint az (EU) 2019/1937 irányelv és az (EU) 2023/2859 rendelet módosításáról. HL L, 2024/1760, 2024.7.5.
- Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, továbbá az (EU) 2020/1828 irányelv módosításáról (kiberrezilienciáról szóló rendelet). HL L, 2024/2847, 2024.11.20.
- Az Európai Parlament és a Tanács 2014/41/EU irányelve (2014. április 3.) a büntetőügyekben kibocsátott európai nyomozási határozatról. HL L 130., 2014.5.1., 1–36.