Tálas Péter[1]: A következő 9/11 – Milyen stratégiai meglepetésre nem készülünk 2026-ban?

Vezetői összefoglaló. *A 2001. szeptember 11-i terrortámadások huszonötödik évfordulóján nem elsősorban annak van jelentősége, hogy megismétlődhet-e egy, az akkorival azonos támadás, hanem annak, hogy a biztonsági rendszerek képesek-e időben felismerni az új típusú fenyegetéseket. A 9/11 Bizottság (9/11 Commission) a 2001 előtti kudarcot négy területen – imagination, policy, capabilities, management – azonosította, s ezek közül különösen a „failure of imagination", vagyis a stratégiai képzelőerő hiányát emelte ki.[2] A 2001 óta kiépített terrorellenes rendszer ma lényegesen megnehezíti a hosszú előkészítést, több elkövető összehangolt tevékenységét és a jelentős szervezeti infrastruktúrát igénylő támadások végrehajtását, s ez a terrorista szereplők alkalmazkodása az egyszerűbb eszközök, kisebb csoportok és magányos elkövetők felé tolta el a terrorcselekmények alkalmazását az európai fenyegetés esetében.*

A következő stratégiai jelentőségű terrortámadás ezért nem feltétlenül valamely teljesen új technológiára épülhet, hanem inkább már ismert eszközök – például fizikai támadás, drónok, kiberművelet és információs manipuláció – összehangolt alkalmazására. A kereskedelmi drónok, a mesterséges intelligencia és más új technológiák valóban csökkenthetik bizonyos képességek hozzáférési küszöbét, de fontos különbséget tenni a technikailag lehetséges, a terroristák által ténylegesen alkalmazható és a stratégiai hatás kiváltására valóban alkalmas képességek között. Európa és Magyarország számára ezért a legfontosabb feladat nem feltétlenül új terrorelhárító struktúrák létrehozása, hanem a meglévő rendvédelmi, nemzetbiztonsági, honvédelmi, kibervédelmi és kritikusinfrastruktúra-védelmi rendszerek együttműködésének erősítése, valamint a fenyegetésekre vonatkozó alapfeltevések rendszeres felülvizsgálata.

Bevezetés

A 2001. szeptember 11-i amerikai terrortámadások huszonötödik évfordulója több szempontból is alkalmat kínál a nemzetközi terrorfenyegetettség változásának áttekintésére. Nem csupán azért, mert a New Yorkban, Washingtonban és Pennsylvaniában végrehajtott támadások közel háromezer ember életét követelték, hanem mindenekelőtt azért, mert következményeik messze meghaladták maguknak a merényleteknek a közvetlen fizikai hatását. A támadások nyomán ugyanis az Egyesült Államok meghirdette a terrorizmus elleni globális háborút, megindult az afganisztáni katonai művelet, majd az iraki háború, jelentősen átalakult az amerikai és az európai terrorellenes politika és az intézményrendszer is, a NATO pedig történetében első alkalommal alkalmazta a Washingtoni Szerződés kollektív védelemről szóló 5. cikkét.

Szeptember 11. ugyanakkor a terrorizmus társadalmi percepciójára is rendkívül erős hatást gyakorolt. Korábbi elemzéseinkben többször is felhívtuk arra a figyelmet, hogy a terrorizmus sajátos politikai erőszakforma, mivel az elkövetők egyik legfontosabb célja a közvetlen fizikai pusztításon túl a félelemkeltés, vagyis a társadalom biztonságérzetének befolyásolása. Éppen ezért a terrorfenyegetettség értékelésekor különösen fontos az események médiamegjelenítése és a társadalmi félelem mellett az objektívebb mutatók – a támadások, az áldozatok, az elkövetési módszerek és az elkövetői kör – figyelembevétele.[3]

A jelen elemzés azonban nem a nemzetközi terrorizmus elmúlt huszonöt évének általános mérlegét kívánja megvonni. Csupán arra keresi a választ, hogy szeptember 11. egyik legfontosabb szakmai tanulsága, a stratégiai meglepetés/stratégiai sokk problémája mennyiben

---

[1] Tálas Péter (talas.peter@svsd.hu), az SV/SD Consulting biztonságpolitikai elemzője.
[2] The 9/11 Commission Report. (2004) *9-11commission.gov*, 339-348. o.
[3] Tálas Péter (2009) Széljegyzet a biztonság szubjektív percepciójának veszélyeiről II. *Nemzet és Biztonság,* 2009. október, 31-34. p.; Kaiser Ferenc – Tálas Péter (2012): Politikai erőszakformák. *Nemzet és Biztonság*, 2012/5-6. 146-148. o.; Tálas Péter: Az Európai Unió terrorfenyegetettsége 2000 és 2019 között, a számok tükrében. SVKI Elemzések 2021/11.

tekinthető ma is aktuálisnak? Másként fogalmazva: *vajon ugyanazokkal a problémákkal szembesülhetnek-e a biztonsági intézmények 2026-ban, mint amelyek 2001 előtt megnehezítették az al-Káida terveinek felismerését, még akkor is, ha maga a fenyegetés teljesen más formát ölt?*

Ennek vizsgálatakor ugyanakkor fontos óvatosságra intenünk. Egy alacsony valószínűségű, de potenciálisan nagy következményű esemény lehetőségének felvetése nem jelenti annak valószínűsítését is. A terrorizmussal kapcsolatos politikai és médiadiskurzus egyik visszatérő problémája éppen az, hogy a lehetséges és a valószínű fenyegetések sokszor összemosódnak. Jelen elemzés ezért nem azt kívánja „megjósolni", hogyan néz majd ki a következő 9/11, hanem azokat a területeket tekinti át, amelyek a stratégiai meglepetés/sokk szempontjából 2026-ban különös figyelmet érdemelhetnek.

A „failure of imagination" helyi értékéről

A 9/11 Bizottság az amerikai állam szeptember 11. előtti felkészületlenségét négy területen azonosította: *imagination, policy, capabilities, management*, vagyis a stratégiai képzelőerő, a szakpolitika, a rendelkezésre álló képességek és az irányítás hiányosságaiban. A jelentésben különösen nagy hangsúlyt kapott az úgynevezett *failure of imagination,* vagyis a stratégiai képzelőerő hiánya.[4]

E megállapítást azonban véleményünk szerint érdemes pontosan értelmezni. Nem arról volt szó, hogy 2001 előtt senki sem tudta volna elképzelni repülőgépek terroristák általi fegyverként történő alkalmazását. Már csak azért sem, mert repülőgép-eltérítések korábban is történtek, az öngyilkos merényletek ugyancsak ismertek voltak, és a repülőgépek épületekbe vezetésével kapcsolatos terrorista elképzelések is megjelentek már korábban. Mi több George W. Bush elnök a szeptember 11-i események előtt csupán néhány héttel kapott egy tájékoztatást, amelyben szó esett egy Bin Laden által elkövetett repülőgép-eltérítés lehetőségéről.[5] A meglepetést tehát sokkal inkább *az ismert elemek összekapcsolásának módja* jelentette.

Az amerikai biztonsági szervek ráadásul több olyan részleges információval is rendelkeztek, amely utólag a készülő támadás indikátorának bizonyult (például ismert al-Káida terroristák belföldi jelenlétéről, gyanús közel-keleti férfiak amerikai repülőiskolai képzéséről), de az információk nem álltak össze megfelelő időben olyan fenyegetésképpé, amely a szeptember 11-i művelet felismeréséhez vezetett volna. A stratégiai meglepetés/sokk tehát részben információs, részben szervezeti és részben értelmezési probléma volt.[6]

Ezzel összefüggésben azonban érdemes *Scott Atran* és *Sankaran Kalyanaraman* figyelmeztetését is komolyan venni, akik arra mutattak rá, hogy a képzelőerő hiánya mellett annak „túlburjánzása" is problémákat okozhat.[7] Ha egy biztonsági rendszer minden elméletileg elképzelhető veszélyt magas prioritású fenyegetésként kezel, vagy túl termékeny képzeleterővel értékeli, olyan mértékben növekedhet a téves riasztások száma, hogy végül éppen a releváns indikátorokat nem tudja megfelelően azonosítani.

Vagyis a 9/11 tanulsága nem egyszerűen az, hogy „több képzelőerőre" van szükség. Hanem az, hogy olyan *fegyelmezett stratégiai képzelőerőre* van szükség, amely képes alternatív lehetőségeket megvizsgálni, ugyanakkor empirikus adatokkal és tényleges képességekkel is ellenőrzi azokat. Ennek lényege, hogy az elemző ne csak azt kérdezze meg, mi történhet, hanem azt is, hogy az adott forgatókönyv megvalósításához milyen képességekre, erőforrásokra és előkészületekre lenne szükség, s ezeknek vannak-e megfigyelhető jelei. Így egyszerre

---

[4] The 9/11 Commission Report (2004). *9-11commission.gov*, 339-360. o.
[5] Thomas S. Blanton (2004): The President's Daily Brief. *nsarchive2.gwu.edu*, 2004.04.12.
[6] Alex Martin – Peter Wilson (2008): The Value of Non-Governmental Intelligence: Widening the Field. *Intelligence and National Security*, 2008, 23(6), 774–775.;
[7] Scott Atran (2006): A Failure of Imagination (Intelligence, WMDs, and "Virtual Jihad"). *Studies in Conflict & Terrorism*, Volume 29, 2006 - Issue 3. 293-295. o.; Sankaran Kalyanaraman (2005): Travails of Intelligence Assessment: From Failed to Fertile Imagination. *Strategic Analysis*, Vol. 29, No. 1, Jan-Mar 2005. 44-57. o.

csökkenthető annak veszélye, hogy a megszokott fenyegetésképen kívül eső lehetőségeket figyelmen kívül hagyjuk, illetve annak, hogy a pusztán technikailag elképzelhető, de valójában kevéssé valószínű forgatókönyveket túlértékeljünk.[8]

A *fegyelmezett stratégiai képzelőerő* tehát nem a lehetőségek korlátlan bővítését jelenti, hanem az egyes forgatókönyvek megvalósíthatóságának és korai figyelmeztető jeleinek szisztematikus vizsgálatát, hogy az elemzés egyszerre maradjon nyitott és bizonyítékokon alapuló. Vagyis a terrortámadási forgatókönyv megvalósíthatóságát annak alapján érdemes vizsgálni, hogy az elkövető rendelkezik-e a szükséges szándékkal, technikai és szervezeti képességekkel, erőforrásokkal és hozzáféréssel, illetve ezek megszerzése milyen előkészületeket igényelhet. Ebből olyan megfigyelhető indikátorok vezethetők le – például szokatlan beszerzések, célpontfelderítés, technikai kísérletezés, kommunikációs vagy szervezeti változások –, amelyek együttes megjelenése növelheti a forgatókönyv valószínűségét.[9] Az elemzés akkor marad nyitott, de bizonyítékokon alapuló, ha az indikátorokat nem önmagukban tekinti bizonyítéknak, hanem több alternatív magyarázattal összevetve, előre meghatározott szempontok szerint értékeli.[10]

Megváltozott-e a terrorista innováció természete?

A terrorizmus története jól mutatja, hogy az elkövetők folyamatosan alkalmazkodnak a terrorellenes intézkedésekhez. Ha valamely támadási mód nehezebbé válik, általában más módszereket vagy kevésbé védett célpontokat keresnek. Például, miután az 1970-es évek elejétől a fémdetektorok megnehezítették a gépeltérítéseket, a terroristák a védtelen közterületek felé fordultak, és a fegyverek helyett testre rögzített öngyilkos robbanóöveket kezdtek használni. Amikor pedig 2006 után a repülőgépek felrobbantása szinte lehetetlenné vált, a merénylők bombák helyett a könnyen beszerezhető, mindennapi eszközökre váltottak, ami a késes támadások és teherautós gázolások hullámához vezetett.

Az innovációnak alapvetően három formáját szokták megkülönböztetni: a stratégiait, a szervezetit, és a taktikait. *Martha Crenshaw* szerint ez fennáll a terrorista innovációra is.[11] A terrorista csoportok általában taktikai innovációt hajtanak végre. Valamilyen más technológiai terület által alkalmazott stratégiai és szervezeti innovációt adaptálnak a saját terepen történő működésükre nézve. *Adam Dolnik* terrorista innovációval foglalkozó munkája[12] és a *Ranstorp–Normark* szerzőpáros szervezeti tanulást vizsgáló kötete[13] szintén arra hívják fel a figyelmet, hogy a terrorista innováció szinte soha nem jelenti valóban új technológia feltalálását. Ez érthető is, hiszen a terrorszervezetek állandó nyomás alatt állnak, illegálisan és korlátozott erőforrásokkal működnek, így nem engedhetik meg maguknak a bizonytalan kimenetelű, drága kutatás-fejlesztést.[14] Az a gyakoribb, hogy már rendelkezésre álló technológiát alkalmaznak új módon, új célpont ellen vagy más módszerrel kombinálva.

Szeptember 11. maga is ilyen innováció volt. A 19 elkövető nem fejlesztett új fegyvert, hanem egy létező civil technológiai rendszert, a kereskedelmi légi közlekedést alakította át

[8] Bart Schuurman – Quirine Eijkman (2015): Indicators of terrorist intent and capability: Tools for threat assessment. *Dynamics of Asymmetric Conflict*, 2015. 8(3), 215–231.; Richards J. Heuer Jr. (1999): Psychology of Intelligence Analysis. *Center for the Study of Intelligence*, 1999. 65-81. o.

[9] Bart Schuurman – Quirine Eijkman (2015): Indicators of terrorist intent and capability: Tools for threat assessment. *Dynamics of Asymmetric Conflict*, 2015. 8(3), 215–231.

[10] Richards J. Heuer Jr. (1999): Psychology of Intelligence Analysis. *Center for the Study of Intelligence*, 1999. 95-110. o.

[11] Ruben Duss (2026): Understanding Terrorist Innovation: A Case Study in Drone Adoption. *gnet-research.org*, 2026.03.20.

[12] Adam Dolnik (2007): Understanding Terrorist Innovation: Technology, Tactics and Global Trends. Routledge, 146-172. o.

[13] Magnus Ranstorp – Magnus Normark (eds.) (2015): Understanding Terrorism Innovation and Learning: Al-Qaeda and Beyond. Routledge.

[14] Daniel Bymen- V.S. Subrahmanian (2026): Artificial Intelligence and the Future of Terrorism. *csis.org*, 2026.07.10.

fegyverré. Az innováció nem a technológiában, hanem annak *felhasználási módjában és a művelet megszervezésében* rejlett.

A 2001 óta eltelt időszak ugyanakkor fontos változást hozott. A nyugati terrorelhárító rendszerek egyre hatékonyabban képesek felismerni a hosszú előkészítést, jelentős logisztikai infrastruktúrát és több elkövető nemzetközi mozgását igénylő támadásokat. Ennek egyik következménye, hogy Európában az elmúlt másfél évtizedben megnövekedett az egyszerűbb módszerekkel végrehajtott támadások jelentősége.

Korábbi elemzéseink a gépjárműves gázolásos (ramming) merényletek kapcsán már felhívták a figyelmet arra, hogy ezek gyorsan, olcsón és viszonylag kevés előkészítéssel végrehajthatók.[15] A magányos elkövetők és kis sejtek által alkalmazott egyszerű eszközök ugyanakkor nem feltétlenül a terroristák erősödését jelzik. A 2017-es londoni támadás után például éppen arra hívtuk fel a figyelmet, hogy a nagyobb logisztikai előkészületeket nem igénylő merényletek terjedése részben a dzsihádista szervezetek műveleti képességeinek gyengülésére is utalhat.[16]

Ez a 2026-os helyzet értékelésekor is fontos szempont. A technológiai fejlődés ugyanis egyidejűleg két, látszólag ellentétes folyamatot erősít. Egyrészt nehezebb nagy terrorista szervezeteket és összetett műveleteket titokban tartani. Másrészt viszont egyes technológiák a korábban csak jelentős szervezeti kapacitással hozzáférhető képességeket tehetnek kisebb csoportok vagy akár egyének számára is elérhetővé.

A kereskedelmi drónok jelentette fenyegetésről

A pilóta nélküli légi rendszerek elterjedése az elmúlt évtized egyik leglátványosabb katonai-technológiai változása volt. Az ukrajnai háború, valamint a közel-keleti konfliktusok azt is megmutatták, hogy ezek a viszonylag olcsó kereskedelmi eszközök felderítési, célazonosítási és támadó feladatokra is átalakíthatók.

Mindez érthető módon felvetette terrorista alkalmazásuk lehetőségét is.[17] A drónok terrorista alkalmazása egyébként nem új jelenség: különböző nem állami fegyveres szervezetek már az 1990-es évektől kísérleteztek velük, az Iszlám Állam pedig 2016–2017-re képes volt kereskedelmi eszközökből, egyszerű alkatrészekből és saját fejlesztésekből viszonylag nagy intenzitással alkalmazott drónképességet létrehozni.[18] A drónok vonzerejét az alacsony beszerzési költségük, a könnyű hozzáférhetőség és módosíthatóságuk, valamint sokoldalúságuk adja: felderítésre, célpontok megfigyelésére, kinetikus támadásra és propagandaanyagok előállítására egyaránt használhatók. Az Iszlám Állam esete különösen jól mutatja, hogy ugyanaz az eszköz egyszerre szolgálhatta a célpontfelderítést, a támadás végrehajtását és annak propagandacélú bemutatását.[19] A kereskedelmi technológia fejlődése ráadásul folyamatosan növeli az elérhető eszközök sebességét, hatótávolságát és repülési idejét, miközben csökken elérhetőségi küszöbük is (egyre olcsóbbak lesznek); a legújabb kutatások pedig több drón összehangolt, illetve rajszerű alkalmazását tekintik az egyik legfontosabb jövőbeni kockázatnak.[20]

---

[15] Tálas Péter (2017): A 2017 márciusi londoni terrormerényletről: gyengülő dzsihadisták? *Nemzet és Biztonság,* 2017/4. szám. 23–33. o.; Tálas Péter – Szente Varga Mónika (2017): A 2017. augusztusi spanyolországi terrortámadásokról. *Nemzet és Biztonság*, 2017/5. szám. 70–78. o.;

[16] Tálas Péter (2017): A 2017 márciusi londoni terrormerényletről: gyengülő dzsihadisták? *Nemzet és Biztonság,* 2017/4. szám. 23–33. o.

[17] Mateusz Osiecki et al. (2022): Drone as a Target of Terrorist Attack and a Weapon Against Terrorism – Analysis in the Light of International Law. *2022 International Conference on Unmanned Aircraft Systems (ICUAS),* Dubrovnik, Croatia, 2022, 1056-1065. o.; Ruben Duss (2026): Understanding Terrorist Innovation: A Case Study in Drone Adoption. *gnet-research.org*, 2026.03.20.

[18] Bálint Márton (2023): Drónok használata terrorista szervezetek által. *Bánki Közlemények*, V. évfolyam 1. szám, 55-62. o.; Report on the emerging patterns of misuse of technology by terrorist actors. *rm.coe.int*, 2025.

[19] Bálint Márton (2023): Drónok használata terrorista szervezetek által. *Bánki Közlemények*, V. évfolyam 1. szám, 55.; 61. o.

[20] Jake Dulligen et al (2025): The Rising Threat of Non-State Actor Commercial Drone Use: Emerging Capabilities and Threats*. CTCSentinel*, March 2025, Volume 18, Issue 3. 41. o.

Mindez azonban nem jelenti azt, hogy ez a technológiai lehetőség automatikusan terrorista támadóképességgé válik: az Európa Tanács 2025-ös jelentése szerint a drónok növekvő hozzáférhetősége és a korábbi fenyegetések ellenére Európában a terrorista szereplők egyelőre nem adaptálták érdemben ezt a támadási formát, ami arra utal, hogy a technológiai hozzáférés mellett a szervezeti struktúra, a szakértelem, az erőforrások, a kockázatvállalás és a terrorelhárítás ellenintézkedései is meghatározzák az innovációt.[21]

Fontos azonban jeleznünk, hogy a „drónfenyegetés" önmagában rendkívül tág kategória. Jelentős különbség van egy egyszerű kereskedelmi quadkopter, egy nagyobb hatótávolságú FPV-eszköz, egy programozott autonóm rendszer és egy katonai kategóriájú pilóta nélküli repülőeszköz között. Ugyancsak különbséget kell tennünk egyetlen drón alkalmazása és több tucat eszköz összehangolt használata között.

A terroristák számára a drónok jelentősége elsősorban abból fakadhat, hogy lehetővé teszik bizonyos hagyományos biztonsági intézkedések megkerülését. Egy tömegrendezvény, repülőtér vagy energetikai létesítmény védelmét korábban elsősorban a földi behatolás és bizonyos esetekben hagyományos légi fenyegetések ellen alakították ki. Egy kis méretű, alacsonyan repülő kereskedelmi eszköz más típusú védekezést igényel.

A stratégiai probléma azonban nem feltétlenül az egyes drónok alkalmazásából, hanem *több olcsó eszköz egyidejű használatából* adódhat. A katonai tapasztalatok ugyanis azt mutatják, hogy a támadó eszközök darabszámának növekedésével aránytalanul növekedhet a védelem terhelése. A Húszi lázadók vörös-tengeri hajók elleni akciói,[22] a szaúdi olajfinomítót megbénító 2019-es csapás,[23] valamint az ukrajnai háborúban alkalmazott Shahed-drónrajok[24] egyaránt azt bizonyítják, hogy az olcsó, kisméretű támadóeszközök tömeges indítása képes kijátszani vagy gazdaságilag és logisztikailag teljesen kimeríteni a méregdrága, hagyományos légvédelmi rendszereket.

Ezt ugyanakkor nem célszerű automatikusan terroristák által is reprodukálható képességnek tekinteni. Több tucat eszköz koordinálása, célba juttatása, elektronikai módosítása, illetve a művelet titokban tartása a szakértők szerint továbbra is komoly technikai és szervezeti kapacitást igényel.[25]

A fenyegetés ezért jelenleg *reális, de korlátozott*. A biztonsági szolgálatok számára elsősorban azok az indikátorok lehetnek figyelemre méltók, amelyek szélsőséges csoportok tartós érdeklődésére utalnak a dróntechnológia, az autonóm navigáció, az elektronikai módosítás vagy a kritikus infrastruktúrák technikai sérülékenységével kapcsolatban. Például kiemelt vészjelzésnek számíthat, ha radikális csoportok tagjai tömegesen vásárolnak civil drónokat azok 3D-nyomtatott fegyverré alakításához, vagy a GPS-zavarást kijátszó autonóm navigációs szoftverek szereznek be, miközben gyanús online adatgyűjtést vagy felderítő berepüléseket végeznek kritikus infrastruktúrák fizikai védelmi rendszerei körül. Ezek a technikai és felderítési nyomok együttesen azt jelezhetik, hogy a terroristák a meglévő technológiák kreatív átalakításával egy komplexebb, összehangolt csapásra készülnek.

---

[21] Report on the emerging patterns of misuse of technology by terrorist actors. *rm.coe.int*, 2025. 16. o.
[22] Gabriel Colodro (2025): Houthi drones drain billions from West as Red Sea chaos escalates, experts say. *jpost.com*, 2025.05.04.
[23] Sébastien Roblin (2019): Why U.S. Patriot missiles failed to stop drones and cruise missiles attacking Saudi oil sites. *nbcnews.com*, 2019.09.23.
[24] Defence Ukraine Team (2026): Draining the Magazine: Ukraine's Deep-Strike vs Russian Air Defence. *defenceukraine.com*, 2026.07.07.
[25] Kerry Chávez - Ori Swed (2020): The proliferation of drones to violent nonstate actors. *Defence Studies*, 2020. 21(1):1-24. o.; Don Rassler – Yannick Veilleux-Lepage (2025): On the Horizon: The Ukraine War and the Evolving Threat of Drone Terrorism. *CTCSentinel*, March 2025. 20. o.; Dennis G Barten (2022): A Counter-Terrorism Medicine Analysis of Drone Attacks. *Prehospital and disaster medicine*, 2022, 37(2),192-196 o.

A mesterséges intelligencia: új fegyver vagy képességsokszorozó?

Hasonló óvatosság indokolt a mesterséges intelligencia (AI) terrorista felhasználásának megítélésekor.

Az utóbbi években igen gyorsan növekedett azoknak a tanulmányoknak és szakpolitikai dokumentumoknak a száma, amelyek az AI terroristák általi felhasználását lehetséges új biztonsági fenyegetésként tárgyalják.[26] A szakirodalomban ugyanakkor egyelőre több potenciális alkalmazási lehetőséget találunk, mint tényleges, dokumentált stratégiai felhasználást. Az ezekben tárgyalt egyik legfőbb kockázat a *személyre szabott online radikalizáció* és a *deepfake technológia*, amelyek révén a terrorcsoportok interaktív csevegőbotokkal közvetlenül toborozhatnak tagokat, illetve politikai vezetők hamisított videóival azonnali pánikot és társadalmi konfliktusokat robbanthatnak ki.[27] Komoly fenyegetést jelent továbbá a nyílt forráskódú, tudományos célú modellek manipulálása, amelyeket a merénylők *vegyi, biológiai vagy radiológiai (CBRN) fegyverek* és veszélyes mérgek hatékonyabb laboratóriumi előállítására próbálhatnak meg felhasználni.[28] Végezetül az AI-alapú adatelemző rendszerek a *komplex műveleti logisztika optimalizálására* is alkalmasak, mivel segítségükkel a terrorsejtek pontosabban feltérképezhetik a kritikus infrastruktúrák gyenge pontjait, és összehangolhatják a szimultán támadások menetrendjét a legkisebb lebukási kockázat mellett.[29]

A szakirodalom alapján ugyanakkor a technológia jelentősége elsősorban abban állhat, hogy *csökkenti egyes tevékenységek tudás-, idő- és munkaerőigényét.* A generatív AI-rendszerek például alkalmasak nagy mennyiségű információ feldolgozására, többnyelvű szövegek előállítására, nyílt forrású adatok elemzésére, képek és videók létrehozására vagy az automatizált online kommunikáció támogatására. Ezek a képességek önmagukban nem újak, hiszen propagandát, toborzást, célpontfelderítést és információgyűjtést a terrorista szervezetek korábban is folytattak. A mesterséges intelligencia tehát nem feltétlenül hoz létre új terrorista tevékenységtípust, egyelőre inkább csak *hatékonyabbá és olcsóbbá tehet már létező tevékenységeket.*[30] Ebből a szempontból az AI jelentőségét talán pontosabb képességsokszorozóként meghatározni, amikor például egy szervezet korábban több ember munkáját igénylő propaganda-, fordítási vagy adatfeldolgozó tevékenységét kevesebb személy bevonásával végezheti el.[31] Például az Iszlám Állam (ISIS) és szövetségesei által indított *„News Harvest"* projektben alkalmazott AI-híradós avatarok, valamint a terrorszervezetek által használt automatizált fordítószoftverek és hangklónozó technológiák pontosan bizonyítják, hogy a mesterséges intelligencia hatékony képességsokszorozóként működik a gyakorlatban is. Ezen eszközök segítségével egyetlen operátor is képes korábban egész stúdiókat, anyanyelvi fordítókat vagy technikai szakértőket

---

[26] Tyler Houser – Beidi Dong (2025): The Convergence of Artificial Intelligence and Terrorism: A Systematic Review of the Literature. *Studies in Conflict & Terrorism,* 1–24. https://doi.org/10.1080/1057610X.2025.2527608

[27] Gabriel Weimann et al. (2025): Generating Terror: The Risks of Generative AI Exploitation. *CTCSentinel*, January 2024, Volume 17, Issue 1. 17-24. o.; Nasir Ahmad Ganaie (2026): The role of artificial intelligence in radicalization, recruitment and terrorist propaganda: deconstructing violent extremism and reimagining counterterrorism in contemporary digital ecosystems. *frontiersin.org*, 2026.01.06.

[28] Nicolò Miotto (2024): The potential terrorist use of large language models for chemical and biological terrorism. *europeanleadershipnetwork.org*, 2024.04.05.; Congress Takes One Step Closer to Challenging ISIS' AI Revolution. *pfluger.house.gov*, 2025.11.20.

[29] Singapore Terrorism Threat Assessment Report 2025. *isd.gov.sg*, 2025.07.29.; Daniel Bymen- V.S. Subrahmanian (2026): Artificial Intelligence and the Future of Terrorism. *csis.org*, 2026.07.10.

[30] Manuel R. Torres Soriano (2025): The transformative impact of Artificial Intelligence on terrorism: Horizon 2035. *IEEE.ES Framework Paper* 01/2026. 1-18. o. *ieee.es*, 2026.01.28.; Gabi Siboni - Simon Tsipsis (2025): The Use of Artificial Intelligence and Advanced Technologies by Terrorist Organizations. *jiss.org.il*, October 2025.; Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes. *unicri.org*, 2021.06. 1-34. o.

[31] Terrorist Use of Generative AI. *techagainstterrorism.org*, 2023.; Miron Lakomy (2023): Artificial Intelligence as a Terrorism Enabler? Understanding the Potential Impact of Chatbots and Image Generators on Online Terrorist Activities. *gnet-research.org*, 2023.12.15.

igénylő, professzionális minőségű globális propagandát és kibertámadási segédleteket előállítani, radikálisan csökkentve a sejtek humánerőforrás- és időigényét.[32]

Ugyanakkor az sem hagyható figyelmen kívül, hogy a terrorizmusellenes szervek ugyanezeket a technológiákat szintén alkalmazhatják. Az AI tehát nem kizárólag a támadó oldal képességeit növeli, hanem a fenyegetések felismerését, az adatelemzést és bizonyos monitoringfeladatokat is segítheti.[33] A terrorizmus ellen fellépő szervek már ma is sikeresen alkalmazzák a mesterséges intelligenciát a határvédelmi kamerák és drónok adatainak valós idejű elemzésére a gyanús mozgások kiszűrésére,[34] valamint olyan gépi tanulásos algoritmusok futtatására, melyek több millió banki tranzakcióból képesek azonnal feltérképezni a rejtett terrorfinanszírozási hálózatokat.[35] Emellett a hatóságok és a tech-vállalatok ma már fejlett nyelvi modellekkel, automatizáltan azonosítják és törlik a radikális online propagandát, mielőtt az elterjedhetne a közösségi médiában, hatékonyan ellensúlyozva a támadói oldal technológiai előnyét.[36]

Vagyis a mesterséges intelligencia terrorista csoportok és terrorellenes erők közötti stratégiai egyensúlyra gyakorolt tényleges hatása egyelőre kétesélyes. Jelenleg a technológiai és erőforrásbeli fölény, valamint a speciális informatikai szakértelem miatt a védelmi és elhárító szervek hatékonyabban profitálnak az AI-alkalmazásokból, mint a terrorista szervezetek. Ez a képességbeli szakadék *(capabilities gap)* ugyanakkor a technológia demokratizálódásával és a nyílt forráskódú modellek terjedésével szűkülhet, ami a jövőben felerősítheti az MI-alapú vagy MI-vel támogatott támadások kockázatát.

A fizikai és kibertámadások összekapcsolásáról

A modern társadalmak működése egyre inkább egymással összekapcsolt fizikai és digitális infrastruktúrákon alapul. Az energiaellátás, a közlekedés, a kommunikáció, a vízellátás, az egészségügy és a pénzügyi szolgáltatások jelentős része informatikai rendszerektől függ. Ez értelemszerűen növeli egy kombinált fizikai–kiber, illetve kiber-fizikai támadás lehetséges hatását.[37] A valódi kérdés az, hogy mekkora mértékben és hogyan?

A kibertér terroristák általi felhasználásával foglalkozó szakirodalom már több mint két évtizede hajlamos arra, hogy a technikailag lehetséges forgatókönyveket ténylegesen várható fenyegetésekkel azonosítsa, így nem egyszer vetítette előre atomerőművek és gátak digitális megsemmisítését.[38] A valóságban azonban a nagy fizikai pusztítást vagy jelentős emberi áldozatokat okozó kiberterrorista támadások száma továbbra is rendkívül alacsony, mivel az ilyen komplex és bonyolult kiberfegyverek kifejlesztésére (mint például az iráni nukleáris programot megbénító Stuxnet vírus volt) kizárólag a rendkívül komoly erőforrásokkal rendelkező nemzetállamok képesek. A terrorszervezetek kibertevékenysége technikai és anyagi korlátjaik miatt eddig kimerült az alacsony hatásfokú weboldal-rongálásokban, adathalászatban vagy túlterheléses támadásokban. Ráadásul a monitorokon megjelenő hálózati rendszerhibák nem nyújtanak olyan sokkoló vizuális médiatartalmat, mint a hagyományos robbantások, így a

[32] These ISIS News Anchors Are AI Fakes. Their Propaganda is Real. hstoday.us, 2024.05.21.; Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment Efforts. *thesoufancenter.org*, 2024.10.03.
[33] Boaz Ganor (2021): Artificial or Human: A New Era of Counterterrorism Intelligence? *Studies in Conflict & Terrorism*, 2021. 44(7), 605–624. o.
[34] Erman Akilli (2024): Artificial Intelligence in Counterterrorism. Navigating The Intersection of Security, Ethics, and Privacy. *SETA Perspetive*, Number 72. April 2024.
[35] AI and Counterterrorism: Potential, Pitfalls, and the Path Forward. *captechu.edu*, 2024.01.31.
[36] Ioannis Syllaidopoulos (2025): A Comprehensive Survey on AI in Counter-Terrorism and Cybersecurity: Challenges and Ethical Dimensions. *ieeexplore.ieee.org*, 2025.06.02.
[37] Sophia Backhaus et al. (2020): A Cyberterrorism Effect? Emotional Reactions to Lethal Attacks on Critical Infrastructure. *Cyberpsychology, Behavior, and Social Networking*, 2020, 23(9), 1-9. o.
[38] Robert K. Knake (2010): Cyberterrorism Hype v. Fact. *cfr.org*, 2010.02.12.; Jerry Brito - Tate Watkins (2012): Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy. 39-84. o. *mercatus.org*, 2012.04.10.; Takács Gergely (2020): Kiberterrorizmus, kiberbűnözés, kiberhadviselés és kritikus infrastruktúrák. rtk.uni-nke.hu, 2020.

kiberterrorizmus képtelen kiszolgálni a félelemkeltésre épülő terrorista propaganda elsődleges, látványos céljait. Éppen ezért nem a „kiber-9/11” típusú forgatókönyveket tartjuk a legfontosabbnak.

Nagyobb figyelmet érdemelhet az a lehetőség, hogy egy hagyományos fizikai támadás hatását kiberművelet segítségével növeljék meg – amikor például a fizikai csapással párhuzamosan megzavarják egy objektum vagy térség kommunikációját, irányítási rendszerét, közlekedését és információszolgáltatását –, vagy fordítva, egy kiberművelet következtében létrejövő működési zavart használjanak ki egy fizikai akció végrehajtására. Az ilyen jellegű hibrid műveletekre a legkomolyabb példákat eddig kizárólag a magas technológiai hátterű nemzetállamok szolgáltatták, mint amikor a 2022-es ukrajnai invázió kezdetén a katonai offenzívával párhuzamosan indított kibertámadással bénították meg az ukrán védelmi kommunikációt,[39] vagy amikor a szíriai reaktor elleni 2007-es légicsapás során a radarrendszerek digitális manipulációjával maszkírozták a fizikai bombázást.[40] Bár a bonyolult koordináció, az elektronikai módosítások és a műveleti titoktartás miatt ez a képesség jelenleg meghaladja a független terrorszervezetek önálló kapacitásait, a biztonságpolitikai szakértők figyelmeztetnek, hogy az aszimmetrikus hadviselés fejlődésével és a kettős felhasználású technológiák elterjedésével a terrorcsoportok a jövőben képessé válhatnak e módszerek lemásolására.[41] Ennek megfelelően komoly jövőbeli fenyegetést jelent, hogy a terrorsejtek egy fizikai merénylet hatássokszorozásaként digitálisan lekapcsolhatják a mentőszolgálatok hálózatait, illetve egy kiberzavar okozta tömegpánikot kihasználva hajthatnak végre hagyományos robbantásos akciókat.

A lényeg tehát nem feltétlenül az egyes támadási módok önálló hatékonysága, hanem a *kombinációjukból létrejövő rendszerhatás.* Ezt azért is fontos hangsúlyozni, mert egy összetett infrastruktúrában egyetlen helyi meghibásodás vagy támadás következménye más rendszerekre is átterjedhet. Egy energetikai zavar például kommunikációs, egészségügyi és közlekedési következményekkel járhat. A terroristák számára ezért egyes esetekben nem maga az objektum lehet a stratégiai célpont, hanem az általa fenntartott rendszer működésének megzavarása.

A komplex infrastruktúrák egymásra utaltságát és a támadásokból eredő dominóhatást kiválóan szemlélteti a 2019-es venezuelai áramhálózati blackout, ahol egy energetikai kiesés azonnal magával rántotta a távközlést, leállította a tömegközlekedést, és a kórházi rendszerek megbénításával közvetlen egészségügyi katasztrófát okozott.[42] Hasonlóan súlyos láncreakciót idézett elő a 2021-es dél-afrikai vasúti szabotázshullám, amely során a jelzőrendszerek kábeleinek lokális rongálása az országos logisztika összeomlásához, a szénszállítmányok elakadása miatt pedig hetekig tartó lakossági áramkorlátozásokhoz vezetett,[43] míg az amerikai Colonial Pipeline olajvezeték elleni kiberakció során a hackerek a fizikai infrastruktúra érintetlenül hagyásával, pusztán az adminisztratív IT-rendszer lezárásával sodorták üzemanyagkrízisbe szinte a teljes keleti partot.[44] Ezek a példák egyértelműen igazolják, hogy a támadók számára a stratégiai célpontot sokszor nem egy konkrét objektum fizikai megsemmisítése jelenti, hanem az a rendszerszintű hatás, amellyel egyetlen ponton előidézett helyi zavar a teljes társadalmi és ellátási hálózat működését képes megbénítani.

---

[39] Case Study – Viasat. *cyberconflicts.protect.ngo*, 2022.06.

[40] David A. Fulghum – Douglas Barrie (2007): Israel used electronic attack in air strike against Syrian mystery target. *abcnews.com*, 2007.10.08.

[41] Hibrid fenyegetések. *consilium.europa.eu*, é.n.

[42] Shaylim Valderrama (2019): Venezuela blames 'attack' as another crippling blackout hits. reuters.com, 2019.03.25.; Francisco Morandi - Luisa Palacios (2026): Venezuela’s Overwhelming Electricity Crisis. *americasquarterly.org*, 2026.08.19.

[43] Economic impact of the recent unrest: National Treasury and PBO briefing. *pmg.org.za*, 2021.08.24. PRASA on plans to deal with damage caused by vandalism and theft of its infrastructure. *pmg.org.za*, 2021.10.21.

[44] Colonial Pipeline Cyber Incident. *energy.gov*, 2026.08.14.

A fizikai támadás és az információs sokk lehetősége

A 2001. szeptember 11-i merényletek egyik fontos sajátossága volt, hogy az események jelentős részét a világ közvéleménye lényegében valós időben követte. A World Trade Center második tornyába becsapódó repülőgépet, majd a tornyok összeomlását televíziókon keresztül a globális közönség is látta. A terrorizmus félelemkeltő hatása szempontjából ez önmagában is igen jelentős sokk volt. Nem véletlen, hogy az ikertornyok összeomlásának felvételei mindmáig a sebezhetőség és a biztonság elvesztésének univerzális szimbólumai.

A mai információs környezet alapvetően különbözik a huszonöt évvel ezelőtti, 2001. szeptember 11-i helyzettől, mivel a hagyományos, szerkesztett média egykori információs kapuőri szerepét mára átvették a decentralizált közösségi platformok (X, TikTok, Telegram), amelyeken keresztül a szemtanúk beszámolói szűretlenül és másodpercek alatt terjednek el globálisan. Egy zajló krízishelyzet kaotikus óráiban a generatív mesterséges intelligencia és a deepfake technológia által tömegesen előállított, manipulált tartalmak miatt egyre nehezebbé válik a hiteles információk kiszűrése, ami teljesen erodálhatja a hatóságokba vetett társadalmi bizalmat. Ez a radikálisan felgyorsult és dezinformációval terhelt digitális ökoszisztéma közvetlenül megfosztja a biztonsági szerveket a higgadt helyzetértékeléshez szükséges időablaktól, miközben a félelmet felerősítő algoritmusok révén akaratlanul is a terroristák legfőbb lélektani hatássokszorozójává válik.[45]

A fizikai és a digitális hadviselés szimultán alkalmazása merőben új lehetőségeket teremt a támadások pszichológiai hatásának maximalizálására, amit kiválóan jelzett a 2024-es moszkvai Crocus City Hall elleni merénylet, amelynek kaotikus óráiban egy AI-generált deepfake videóval hamisan próbálták az ukrán vezetést bűnbaknak beállítani.[46] Ehhez hasonlóan a 2023-as gázai konfliktus során is megfigyelhető volt a mesterséges intelligencia káros hatása, amikor a lakosság legmélyebb félelmeit megcélozva, gyanús WhatsApp-csoportokban terjesztettek szintetikus, klónozott hangfelvételeket a túszul ejtett áldozatokról a hátországi tömegpánik és a teljes bizonytalanság gerjesztése érdekében.[47] A nemzetközi védelmi elemzések arra is figyelmeztetnek, hogy egy fizikai csapást követően a támadók a jövőben a helyi hatóságok kommunikációs csatornáit feltörve hamis evakuációs utasításokat adhatnak ki, amelyekkel a menekülő civileket szándékosan egy második aktív robbantási zónába vagy a mentőcsapatok útvonalára terelhetik, teljesen megbénítva a válságkezelést.[48] Az ilyen információs művelet célja nem feltétlenül újabb áldozatok okozása lenne. Sokkal inkább annak elérése, hogy *az érintett társadalom és a döntéshozók egy ideig ne legyenek biztosak abban, mi történik valójában*.

Az említettek a terrorizmus klasszikus félelemkeltő logikájának technológiailag korszerűbb változatai lehetnek. Fontos azonban jeleznünk, hogy egyelőre elsősorban potenciális alkalmazási lehetőségről beszélünk, mivel kevés olyan terrorista műveletet ismerünk, amelyben a generatív AI-ra épülő információs manipuláció és a fizikai támadás tudatosan összehangolt, patikamérlegen kiszámított stratégiai műveletként jelent volna meg. Ennek ellenére az olyan közelmúltbeli hibrid kampányok, mint a 2023–2024-es gázai konfliktust kísérő tömeges deepfake- és botakciók,[49] vagy a 2024-es brit zavargásokat kirobbantó, mesterséges intelligenciával generált álhírhullámok[50] már egyértelműen mutatják a fejlődés irányát. Ezeknek az összetett, a

---

[45] Tyler Houser – Beidi Dong (2025): The Convergence of Artificial Intelligence and Terrorism: A Systematic Review of the Literature. *Studies in Conflict & Terrorism,* 1–24. https://doi.org/10.1080/1057610X.2025.2527608; Miron Lakomy (2023): Artificial Intelligence as a Terrorism Enabler? Understanding the Potential Impact of Chatbots and Image Generators on Online Terrorist Activities. *gnet-research.org*, 2023.12.15.

[46] Olga Robinson – Shayan Sardarizadeh – Paul Brown (2024): Moscow attack: Debunking the false claims. *bbc.com*, 2024.03.26.; Fact Check: Old Budanov comments falsely linked to March 2024 Russia concert attack. *reuters.com*, 2024.03.29.

[47] Yael Ram – Liran Antebi (2023): Deep Fake in Swords of Iron: A Battle for Public Opinion. *inss.org.il*, 2023.11.05.

[48] Emma de Mos (2025): The impact of mis- and disinformation during CBRN incidents. 9-14. o. *jcbrncoe.org*, 2025.

[49] Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment Efforts. *thesoufancenter.org*, 2024.10.03.

[50] Sam Stockwell - Ardi Janjeva - Broderick McDonald (2026): Adding Fuel to the Fire: AI Information Threats and Crisis Events. *cetas.turing.ac.uk*, 2026.02.11.

fizikai és a digitális teret egyszerre uraló folyamatoknak az igazi veszélye és biztonságpolitikai kihívása éppen abban rejlik, hogy a kifinomult technikai álcázás miatt a kaotikus első órákban szinte lehetetlen azonnal és pontosan kideríteni, hogy egy független terrorista sejt magánakciójáról vagy egy idegen nemzetállam által vezérelt hibrid támadásról van-e szó.[51]

A puha célpontoktól a rendszerhatásig

A terrorista célpontválasztással foglalkozó szakirodalom régóta felhívja a figyelmet arra, hogy az elkövetők nem feltétlenül a katonailag vagy politikailag legfontosabb objektumokat választják célpontnak. Gyakran sokkal fontosabb számukra, hogy a célpont könnyen megközelíthető, nehezen védhető és jelentős médiafigyelmet biztosító helyszín legyen.[52] A terrorizmuskutatás által *„puha célpontoknak" (soft targets)* nevezett helyszínek kiválasztása pontosan azt a racionális kalkulációt tükrözi, amely a minimális katonai védelmet maximális lélektani és médiahatással kombinálja. A terroristák azért részesítik előnyben a könnyen megközelíthető közlekedési csomópontokat – mint a madridi vonatokat és a londoni metrókat, vagy a brüsszeli repülőteret –, a kulturális és szórakozóhelyeket – mint a párizsi Bataclan koncerttermet, a Manchester Arenát vagy a moszkvai Crocus City Hallt –, valamint a zsúfolt turisztikai zónákat és sportesemányeket – mint a nizzai és barcelonai sétányokat, illetve a Boston Marathont –, mert ezeken a helyszíneken a védtelen civil tömegek jelenléte garantálja a magas áldozatszámot és az azonnali, globális élő médiavisszhangot. Ezen aszimmetrikus akciók elsődleges célja nem a kemény katonai infrastruktúra rombolása, hanem a társadalmi pánik maximalizálása annak az üzenetnek a terjesztésével, hogy a mindennapi élet tágas, nyitott tereiben bárki, bármikor áldozattá válhat.

A puha célpontok ebből a szempontból tartós kihívást jelentenek. Minden bevásárlóközpontot, vasútállomást, vallási helyszínt, szórakozóhelyet vagy tömegrendezvényt ugyanolyan intenzitással megvédeni ugyanis sem gazdasági, sem társadalmi szempontból nem lehetséges.

2026-ban az infrastruktúra-hálózatok komplexitása a célpontválasztás egy további, fontos szempontját indokolhatja: a modern, hálózatvezérelt társadalmakban a terroristák és szabotőrök számára egy-egy objektum jelentőségét már nemcsak annak szimbolikus értéke vagy a helyszínen potenciálisan elérhető áldozatszám határozza meg, hanem az is, hogy milyen más rendszerek működése függ tőle. Ebből következően egy viszonylag kevéssé látványos, elszigetelt, fizikailag kisméretű és nehezen védhető elem stratégiai súlya jóval nagyobb lehet, mint amit fizikai mérete vagy ismertsége alapján feltételeznénk.[53]

Vagyis a rendszerfüggőségek növekedése új lehetőséget teremthet a szándékosan aránytalan rendszerhatást kereső támadások számára. Különösen sérülékenyek lehetnek az energia-, közlekedési és kommunikációs infrastruktúrák olyan szűk keresztmetszetei, amelyek kiesése az interdependenciák miatt más rendszerek működésére is átterjedhet. Vasúti biztosítóberendezések, tranzitvezetékek egyes csomópontjai, tenger alatti adatkábelek vagy kritikus digitális szolgáltatásokat kiszolgáló infrastruktúrák ebből a szempontból nem feltétlenül látványos, de potenciálisan nagy rendszerhatású célpontok lehetnek. Fontos azonban hangsúlyozni, hogy e sérülékenységek megléte önmagában nem bizonyítja a terroristák növekvő érdeklődését vagy képességét ilyen támadások végrehajtására; csupán azt jelzi, hogy egy sikeres támadás

---

[51] Hibrid fenyegetések. *consilium.europa.eu*, é.n.

[52] Victor Asal et al. (2009): The Softest of Targets: A Study on Terrorist Target Selection. *Journal of Applied Security Research*, 4(3), 258–278.; Tomáš Zeman (2020): Soft Targets: Definition and Identification. *Academic and Applied Research in Military and Public Management Science*, 19(1), 109–119.; Sydney L. Reichin et al. (2025): Recommendations for Assessing Vulnerabilities in Soft Targets and Crowded Places. *Studies in Conflict & Terrorism*. 1–29. https://doi.org/10.1080/1057610X.2025.2488285

[53] David Riedman (2017): The Cold War on Terrorism: Reevaluating Critical Infrastructure Facilities as Targets for Terrorist Attacks. *Homeland Security Affairs*, Volume XIII. June 2017.; Mahmut Cengiz (2026): Targeting the Backbone: Terrorist Threats to Critical Infrastructure. *hstoday.us*, 2026.04.16.

következményei a hálózati függőségek miatt a közvetlen fizikai károknál jóval szélesebb körűek lehetnek.

A stratégiai célpontelemzés (strategic target analysis) ezért egyre kevésbé korlátozható kizárólag az egyes objektumok elszigetelt fizikai védelmére, például kerítések építésére vagy fegyveres őrség felállítására. A modern terrorelhárítási és kockázatkezelési doktrínák szerint az ellátási láncok, a rendszerszintű függőségek, a beépített strukturális tartalékok (redundanciák) és az egyes kritikus ágazatok közötti keresztbefonódások és oda-vissza hatások dinamikus feltérképezése ugyanolyan fontossá vált, mint maga a fizikai objektumvédelem. Ha a védelmi szervek nem hálózati kontextusban elemzik a kockázatokat, képtelenek lesznek azonosítani azokat a rejtett sebezhetőségeket, amelyeket a támadók a rendszerszintű megbénítás érdekében kiaknázhatnak.[54]

Az állami és nem állami fenyegetések közötti határ elmosódása

Szeptember 11. után az Egyesült Államok számára viszonylag gyorsan egyértelművé vált, hogy a támadásokat az al-Káida hajtotta végre. Az elkövető azonosítása és egy állam közötti viszony meghatározása természetesen akkor sem volt problémamentes, de a fenyegetés alapvetően transznacionális terrorista szervezetként volt értelmezhető.

A mai biztonsági környezet ennél összetettebb. Az államok stratégiai céljaik eléréséhez a közvetlen fellépés mellett különböző közvetítő szereplőket, fedett és nehezen azonosítható eszközöket is alkalmazhatnak. Fontos azonban különbséget tenni az állami proxytevékenység, az államilag támogatott terrorizmus és a hibrid műveletek között. A proxy olyan nem állami szereplő, amelyet valamely állam saját stratégiai céljai érdekében támogat, de nem szükségszerűen alkalmaz terrorista módszereket, és saját érdekekkel, illetve bizonyos fokú autonómiával is rendelkezhet. Az államilag támogatott terrorizmus ennél szűkebb kategória, amelyben az állami támogatást élvező szereplő terrorista módszereket alkalmaz. A hibrid művelet viszont tágabb fogalom: katonai és nem katonai, nyílt és fedett eszközök – például kiberműveletek, dezinformáció, gazdasági nyomás, szabotázs vagy proxyk – összehangolt alkalmazását jelentheti.

A jelenlegi biztonsági környezet mindhárom jelenségre, illetve az állami fellépés más, nehezen azonosítható formáira is kínál példákat. A kiberműveletek terén a kínai államhoz köthető *Volt Typhoon* csoport[55] kritikus infrastruktúrákba történő behatolása az állami kiberműveletek és a felelősazonosítás problémáját mutatja, míg az iráni *CyberAv3ngers*[56] esete arra jó példa, hogy állami kötődésű kiberszereplők hacktivista identitást is felhasználhatnak tevékenységük elfedésére. Az információs térben a *Storm-1516*-hoz hasonló, Oroszországhoz kötött hálózatok[57] dezinformációs műveletei azt mutatják, hogy a befolyásolási műveletek végrehajtói és tényleges támogatói közötti kapcsolatot ugyancsak nehezen lehet gyorsan azonosítani. A Hezbollah és Irán kapcsolata pedig arra jó példa, hogy az állami támogatás és a nem állami szereplő saját cselekvési autonómiája egyidejűleg is jelen lehet. Ezek a példák tehát nem ugyanannak a jelenségnek a változatai: nem minden proxy terrorista, nem minden államilag támogatott szereplő proxy, és nem minden hibrid művelet tartalmaz terrorista elemet.

A probléma ezért nem az, hogy eltűnnének a klasszikus terrorizmus, a szabotázs, a proxytevékenység és az állami hibrid műveletek közötti fogalmi határok, hanem az, hogy egy konkrét

---

[54] Kiss Adrienn (2023): Létfontosságú rendszerelemek vizsgálata 1. – Hálózatosságvizsgálat. *Hadmérnök*, 18. évfolyam (2023) 2. szám. 123–137. o.; Zachary Kallenborn - Henry H Willis (2025): Globally Critical Infrastructure: The Unique Risks and Challenges. *pmc.ncbi.nlm.nih.gov*, 2025.11.11.

[55] PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. *cisa.gov*, 2024.02.07.

[56] Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure. *cisa.gov*, 2026.07.22.

[57] Clint Watts (2024): Russian election interference efforts focus on the Harris-Walz campaign. *blogs.microsoft.com*, 2024.09.17.

esemény esetében kezdetben nehéz lehet megállapítani, melyik kategóriával állunk szemben. Egy kritikus infrastruktúra elleni robbantás vagy kibertámadás esetében így nem feltétlenül az lesz az első kérdés, hogy melyik terrorszervezet hajtotta végre, hanem hogy *terrorizmusról, szervezett bűnözésről, államilag támogatott szabotázsról, proxytevékenységről, közvetlen állami műveletről vagy ezek valamely kombinációjáról van-e szó*. Ebben a környezetben a felelősazonosítás bizonytalansága önmagában is stratégiai jelentőségűvé válhat. Minél tovább tart ugyanis az elkövető, az esetleges támogató vagy megrendelő, valamint a művelet természetének azonosítása, annál nehezebb meghatározni, hogy mely intézménynek, milyen jogi keretben és milyen eszközökkel kell reagálnia.

Ez Európa számára különösen fontos probléma, mivel a terrorelhárítás, a rendvédelem, a nemzetbiztonság, a kibervédelem és a katonai védelem eltérő intézményi és jogi keretek között működik. Egy összetett vagy nehezen azonosítható támadás ezért nemcsak fizikai vagy működési károkat okozhat, hanem azzal is stratégiai hatást érhet el, hogy bizonytalanságot teremt a támadás természetét, az elkövető kilétét és így a megfelelő válasz módját illetően.

Milyen lehet a „következő 9/11”?

A fentiek alapján nem tartjuk szakmailag indokoltnak, hogy egyetlen konkrét forgatókönyvet nevezzünk meg a következő stratégiai terrortámadás lehetséges formájaként. Ez ugyanis éppen azt a problémát idézné elő, amelyet el kívánunk kerülni: egyetlen támadási modell túlzott kiemelésével más, ugyanilyen veszélyes lehetőségeket szorítanánk háttérbe. Annyi azonban megállapíthatónak látszik, hogy egy potenciálisan stratégiai jelentőségű jövőbeni támadásnak nem feltétlenül egyetlen új, futurisztikus fegyver vagy technológia adná a különlegességét. Sokkal inkább az, ha a támadók több, már ma is meglévő és ismert képességet egyidejűleg, egymás hatását felerősítve alkalmaznának.

Egy ilyen modern, többdimenziós műveletre jó példa egy olyan *összetett támadási láncolat*, amelyben az alábbi elemek egymásra épülve bénítják meg a védekezést:

1. *A kiber-előkészítés.* A támadók egy összehangolt *kiberművelettel* első lépésként megbénítják a célország segélyhívó központjait, a rendőrségi kommunikációs csatornákat vagy a közlekedési jelzőrendszereket, ezzel mesterséges vakságot és működésképtelenséget idézve elő a hatóságoknál.
2. *A kinetikai csapás.* A digitális bénultságot kihasználva egyidejűleg végrehajtanak egy *fizikai támadást* egy kritikus csomópont (például egy transzformátorállomás vagy egy forgalmas pályaudvar) ellen, miközben a levegőből *pilóta nélküli eszközökkel (drónokkal)* akadályozzák meg a mentőegységek helyszínre jutását, vagy mérnek csapást a környező megerősített pontokra.
3. *Az információs káosz.* A fizikai és digitális pusztítással párhuzamosan elindul az *információs manipuláció:* a közösségi médiát elárasztják a mesterséges intelligenciával generált álhírek és manipulált videók (deepfake), amelyek hamis kormányzati utasításokat terjesztenek, vagy teljesen más helyszínekre irányítják a lakosság figyelmét.

Ez a kombináció azért bír stratégiai veszéllyel, mert a különböző típusú támadások nem egyszerűen összeadódnak, hanem *szinergiát alkotnak*: a kibertámadás megvakítja a hatóságokat, a drónok megbénítják a helyszíni reagálást, az álhírek pedig pánikba sodorják a társadalmat. A védekező állam így nem egyetlen válsággal áll szemben, hanem egy olyan komplex rendszerösszeomlással, amelyben a különböző intézmények (hadsereg, rendőrség, IT-védelem) képtelenek koordinálni a válaszlépéseiket. Az ilyen támadás stratégiai jelentőségét nem feltétlenül a közvetlen áldozatok vagy a fizikai károk nagysága adná. Fontosabb lehetne, hogy egyszerre okoz működési zavart, társadalmi bizonytalanságot, információs káoszt és politikai nyomást.

Ez egyben visszavezet bennünket a stratégiai terrortámadás fogalmához. Korábbi elemzésünkben stratégiai terrortámadásnak azokat a támadásokat neveztük, amelyek nagy áldozatszámukkal, médiahatásukkal és félelemkeltő erejükkel jelentősen befolyásolják a társadalom

biztonságpercepcióját és terrorizmusképét, jóllehet nem feltétlenül okoznak stratégiai léptékű fizikai károkat.[58] E meghatározást 2026-ban talán annyiban érdemes kiegészíteni, hogy a stratégiai jellegű terrorcselekmény *rendszerszintű működési zavart* is kiválthat.

Mit jelent mindez Kelet-Közép-Európa és Magyarország számára?

Az elmúlt huszonöt évben Európa terrorellenes képességei jelentősen fejlődtek. Megerősödött a hírszerzési és rendvédelmi információcsere, a terrorfinanszírozás elleni fellépés, az utasadatok felhasználása, a határbiztonság és a kritikus infrastruktúrák védelme.

Ezzel párhuzamosan azonban a fenyegetettségi környezet is összetettebbé vált. A hagyományos terrorizmus mellett az európai államoknak állami és nem állami kibertámadásokkal, szabotázsműveletekkel, dezinformációval és hibrid fenyegetésekkel is számolniuk kell. E fenyegetések között ráadásul nem mindig húzható egyértelmű határ.

Magyarország szempontjából különösen fontos jeleznünk, hogy Kelet-Közép-Európa hosszabb távon a világ egyik kevésbé terrorfenyegetett térsége volt. Korábbi adataink alapján az Európai Unió kelet-közép-európai térségét 2000–2019 között kifejezetten alacsony terrorfenyegetettség jellemezte.[59] Az olyan terrorizmussal foglalkozó intézmények jelentései, mint a Sydney-i központú *Institute for Economics & Peace (IEP)* által kiadott *Global Terrorism Index (GTI)*, vagy az Európai Unió bűnüldözési ügynöksége, az *Europol* által évente publikált *EU Terrorism Situation & Trend Report (TE-SAT)*, mind azt mutatják, hogy ez a trend a 2020 és 2026 közötti időszakban is stabilnak bizonyult.

Jóllehet Kelet-Közép-Európa fizikailag továbbra is védettebb a klasszikus, tömeges áldozatokkal járó terrorakcióktól, a globális világrend átalakulása egyértelműen felértékeli a régió stratégiai szerepét. A nagyhatalmi érdekek törésvonalán fekvő térségben a modern, nehezen elhatárolható fenyegetések miatt nem hagyhatók figyelmen kívül a technológiai és módszertani változások. A kiber-fizikai rendszerek összefonódása, valamint a nyílt konfliktusokat felváltó, államilag támogatott szabotázsakciók és hibrid műveletek ugyanis már itt is közvetlen, határokon átnyúló kockázatot jelentenek.

Ráadásul egy álcázott állami proxycsoport által végrehajtott digitális szabotázs vagy egy MI-alapú információs kampány nem igényel fizikai jelenlétet a célországban. Mivel ezek az akciók egyszerre hordozzák a köztörvényes bűnözés, a politikai terrorizmus és a burkolt állami hadviselés jegyeit, a hagyományos terrorakcióktól leginkább védett országok sem vonhatják ki magukat a hatásaik alól; nemzeti biztonsági és védelmi stratégiáik folyamatos igazítása ezért a relatív biztonság megőrzésének alapvető feltétele.

Véleményünk szerint Magyarország számára elsősorban három stratégiai következtetés adódik a fentiekből.

Egyrészt, nem feltétlenül új, különálló terrorellenes intézmények létrehozása a legfontosabb feladat, hanem annak biztosítása, hogy a meglévő rendőrségi, nemzetbiztonsági, honvédelmi, kibervédelmi, katasztrófavédelmi és kritikusinfrastruktúra-védelmi szervezetek a hibrid és összetett fenyegetéseket integráltan, hatékony ágazatközi együttműködésben legyenek képesek kezelni.

Másrészt, a pontszerű objektumvédelem mellett egyre nagyobb figyelmet érdemel a létfontosságú rendszerek közötti ágazatközi függőségek és átnyúló kapcsolatok folyamatos vizsgálata. Nem csupán azt a kérdést kell feltenni, hogy egy adott létesítmény fizikai védelme menynyire biztosított, hanem azt is, milyen dominóhatású következményekkel járna működésének rövid vagy hosszú távú kiesése a tőle függő egyéb kritikus rendszerekre.

---

[58] Tálas Péter (2017): A londoni merénylet azt is üzeni, hogy gyengülnek a dzsihadisták. *SVKI Elemzések* 2017/8. 1. o.
[59] Tálas Péter (2021): Az Európai Unió terrorfenyegetettsége 2000 és 2019 között, a számok tükrében. *SVKI Elemzések* 2021/11.

Harmadrészt, elengedhetetlennek látszik a kis valószínűségű, de katasztrofális következményű (úgynevezett *High-Impact Low-Probability*) forgatókönyvek rendszeres és szimulációs vizsgálata. Nem azért, mert ezek bekövetkezése a mindennapokban feltétlenül valószínű, hanem azért, mert az ilyen jellegű stratégiai gyakorlatok alkalmasak a megszokott, rutinszerű intézményi alapfeltevések tesztelésére és a rejtett sebezhetőségek felszínre hozására.

Következtetések – a 9/11-teszt 2026-ban

Huszonöt évvel a szeptember 11-i támadások után viszonylag nagy bizonyossággal állítható, hogy az akkori módszerek azonos formában történő megismétlése ma már lényegesen nehezebb feladat elé állítaná az elkövetőket. A repülésbiztonság szigorítása, a nemzetközi hírszerzési együttműködés elmélyülése, a terrorfinanszírozás elleni szisztematikus fellépés, valamint az utasmozgások és gyanús személyek ellenőrzésének digitalizációja mind jelentős fejlődésen mentek keresztül. Ebből a sikeres adaptációból azonban korántsem következik, hogy a stratégiai meglepetés lehetősége végleg megszűnt volna. Sőt, bizonyos értelemben éppen a terrorellenes intézkedések hatékonysága kényszeríti ki annak vizsgálatát, hogy az elkövetők miként változtatják meg módszereiket a jól védett területek és a már ismert támadási formák elkerülése érdekében.

A modern „9/11-teszt" lényege ezért véleményünk szerint nem abban a kérdésben rejlik, hogy képesek lennénk-e ma megakadályozni a 2001-es eseményeket – erre a válasz ugyanis nagy valószínűséggel igen. A szakmailag sokkal relevánsabb kérdés úgy hangzik: *időben felismernénk-e egy olyan új támadási forma kialakulását, amelynek egyes technológiai és szervezeti elemeit külön-külön ugyan már ismerjük, de amelyeket jelenleg még nem tekintünk egyetlen összefüggő, komplex fenyegetés részeinek?* Erre a felvetésre a válasz már lényegesen kevésbé egyértelmű.

A 9/11 Bizottság által egykor megfogalmazott stratégiai *„képzelőerő kudarca" (failure of imagination)* mint alapvető rendszerszintű hiányosság, így huszonöt év elteltével sem veszítette el a jelentőségét. Érdemes azonban pontosítanunk ezt a koncepciót: a cél nem az, hogy a biztonsági szolgálatok minden elképzelhető támadási formát tévedhetetlenül előre jelezzenek, hiszen ez sem szakmailag, sem az erőforrások korlátozottsága miatt nem lehetséges. A valódi feladat annak biztosítása, hogy a védelmi architektúra képes legyen rendszeresen megkérdőjelezni saját rutinszerű alapfeltevéseit, időben azonosítani az új technológiai és szervezeti lehetőségeket, valamint határozott különbséget tenni az elméletileg elképzelhető és a gyakorlatban ténylegesen valószínű fenyegetések között.

Ennek a rendszerszintű rugalmasságnak az eléréséhez nyújtanak nélkülözhetetlen segítséget a strukturált elemzési módszerek, mint az alapfelvetések ellenőrzése (*Key Assumptions Check*), az alternatív hipotézisek vizsgálata, a kritikus szemléletű *Red Teaming*, a korai figyelmeztető indikátorrendszerek (*warning systems*), vagy éppen az alternatív jövőképek (*Alternative Futures*) modellezése. Ezeknek a módszereknek elsődleges célja ugyanis nem a következő 9/11 hajszálpontos megjóslása. Sokkal inkább az, hogy radikálisan csökkentsék annak a forgatókönyvnek a valószínűségét, amely szerint egy jövőbeni katasztrófa után ismételten arra a keserű következtetésre kellene jutnunk, hogy az információk valójában rendelkezésre álltak, a technológia és a sebezhetőségek is ismertek voltak – csupán az intézményi képzelőerő hiányzott ahhoz, hogy végig gondoljuk: mindezeket valaki képes lehet egyetlen pusztító láncreakcióvá összekapcsolni.

2026. szeptember 8.