A következő 9/11 nem olyan lesz, mint az előző

9/11 valódi tanulsága. A 2001. szeptember 11-i terrortámadások huszonötödik évfordulóján nem elsősorban azt érdemes vizsgálni, megismétlődhet-e az akkori támadás, hanem azt, hogy a biztonsági rendszerek képesek lennének-e időben felismerni egy más formában jelentkező stratégiai meglepetést. A 9/11 Bizottság az amerikai rendszer kudarcát négy területen – imagination, policy, capabilities, management – azonosította, s különösen a stratégiai képzelőerő hiányát emelte ki. Ez azonban nem jelenti azt, hogy minden technikailag elképzelhető fenyegetést valószínűnek kell tekinteni. A tanulság inkább a fegyelmezett stratégiai képzelőerő szükségessége: alternatív forgatókönyveket kell vizsgálni, majd azokat az elkövetői szándék, a tényleges képességek, a szükséges erőforrások és a megfigyelhető előkészületek alapján tesztelni.

A terrorizmus alkalmazkodott. A 2001 óta kiépített terrorellenes rendszer jelentősen megnehezítette a hosszú előkészítést, kiterjedt logisztikát és több elkövető összehangolt tevékenységét igénylő támadásokat. A terroristák ehhez alkalmazkodtak: Európában felértékelődtek az egyszerű eszközökkel, kis csoportok vagy magányos elkövetők által végrehajtott akciók. Innovációjuk nem új technológia feltalálása, inkább a már létezők új módon, új célpont ellen vagy egymással kombinálva történő alkalmazása. Maga 9/11 is ilyen innováció volt: az elkövetők a kereskedelmi légi közlekedést alakították fegyverré.

A technológia önmagában nem fordulat. A 2026-os technológiai környezetben elsősorban a kereskedelmi drónok, a mesterséges intelligencia, a kiberműveletek és az információs manipuláció kínálhat új lehetőségeket. A drónok olcsók, hozzáférhetők és módosíthatók, de a technológiai hozzáférés nem azonos az operatív képességgel. Az Iszlám Állam 2016–2017-ben jelentős drónképességet épített ki, Európában azonban a terroristák egyelőre nem adaptálták érdemben ezt a támadási formát. Hasonló óvatosság indokolt a mesterséges intelligencia esetében is: ma még csak képességsokszorozó, amely olcsóbbá és gyorsabbá teheti a propagandát, információgyűjtést, célpontfelderítést vagy adatfeldolgozást.

A veszély a kombinációban rejlik. Nagyobb stratégiai jelentősége lehet a különböző támadási módok összekapcsolásának. Egy fizikai akció kibertámadással, drónokkal és információs manipulációval kombinálva nagyobb működési és pszichológiai hatást válthat ki, mint az egyes elemek külön-külön. Felértékelődhetnek azok a kritikus infrastruktúrák is, amelyek kiesése más rendszerek működésére továbbgyűrűző zavarokat okozhat. A célpont stratégiai jelentőségét ezért nemcsak fizikai vagy szimbolikus értéke, hanem a tőle függő rendszerek száma és kiesésének rendszerhatása is meghatározhatja.

A fenyegetésértékelést az állami és nem állami szereplők közötti kapcsolatok összetettsége is nehezíti. A proxytevékenység, az államilag támogatott terrorizmus és a hibrid művelet nem azonos kategóriák. Egy konkrét robbantás, kibertámadás vagy szabotázsakció esetében azonban kezdetben nehéz lehet megállapítani, hogy terrorizmusról, szervezett bűnözésről, államilag támogatott szabotázsról, proxytevékenységről vagy közvetlen állami műveletről van-e szó. A felelős azonosításának bizonytalansága ezért önmagában is stratégiai hatású lehet, mert késleltetheti annak eldöntését, mely intézménynek, milyen jogi keretben és milyen eszközökkel kell reagálnia.

A „következő 9/11” tehát nem feltétlenül egy új fegyverhez, eszközhöz kötődik. A stratégiai meglepetés inkább abból fakadhat, hogy egy támadó több ismert képességet – fizikai támadást, drónt, kiberműveletet és információs manipulációt – egyetlen összetett műveletben kapcsol össze. Ez kockázati forgatókönyv, nem előrejelzés. A stratégiai hatást pedig már nemcsak az áldozatok száma és a félelemkeltés, hanem rendszerszintű működési zavar is meghatározhatja.

Mire kell felkészülnünk? Magyarország továbbra is egy viszonylag alacsony terrorfenyegetettségű régió része, de ez nem jelent sérthetetlenséget. Három feladat különösen fontos: a rendvédelmi, nemzetbiztonsági, honvédelmi, kibervédelmi és kritikusinfrastruktúra-védelmi szervezetek együttműködésének erősítése; a létfontosságú rendszerek közötti függőségek és egy esetleges kiesés dominóhatásainak vizsgálata; valamint a kis valószínűségű, de nagy következményű forgatókönyvek rendszeres tesztelése.

9/11 legfontosabb figyelmeztetése huszonöt év után ezért nem az, hogy egy korábbi támadás elhárítására kell még jobban felkészülnünk, hanem az, hogy időben ismerjük fel, ha valaki az ismert technológiákat, módszereket és sérülékenységeket olyan módon kapcsolja össze, amelyre a biztonsági rendszer még nem készült fel.

2026. szeptember 10.