A technológiai függőség stratégiai kockázatai – A Starlink-korlátozások európai tanulságai

Az ukrajnai Starlink-szolgáltatások 2026. október 14-én bevezetett újabb korlátozása ismét rámutatott a modern hadviselés egyik alapvető stratégiai sérülékenységére: a katonai képességek működése egyre nagyobb mértékben függ olyan külföldi technológiáktól, amelyek alkalmazási feltételeit, hozzáférhetőségét és korlátozását nem feltétlenül a felhasználó állam ellenőrzi. A probléma nem kizárólag amerikai, és nem is az Egyesült Államokkal fennálló szövetségi viszony megkérdőjelezéséről szól. Általánosabb kérdés, hogy egy állam mennyire képes önállóan működtetni létfontosságú katonai és biztonsági rendszereit válság vagy politikai nézeteltérés esetén.

Az ukrajnai eset tanulságai. Október 14-én ukrán tisztviselők arról számoltak be, hogy a SpaceX korlátozta a Starshield katonai műholdas kommunikációs szolgáltatás mozgás közbeni használatát. A sebességkorlátozás több drónműveletet megzavart, egyes bevetéseket törölni kellett. Az ukrán fél szerint a változtatás előzetes figyelmeztetés nélkül történt. A korlátozás pontos oka és döntési háttere egyelőre nem tisztázott. Elon Musk szerint a Starshield használati feltételeiről az amerikai katonai vezetés dönt, míg a kereskedelmi Starlink eltérő szabályozás alatt működik. Bár a történtekből nem következik bizonyítottan, az elemzők szerint Washington politikai nyomásgyakorlás céljából rendelte el a korlátozást.

A katonai következmény mindenesetre egyértelmű: egy külső szolgáltató által végrehajtott műszaki vagy hozzáférési változtatás azonnal befolyásolhatja a felderítés, a csapásmérés, a drónirányítás és a légvédelem működését. A függőség tehát nem pusztán beszerzési vagy informatikai kérdés, hanem a katonai műveletek végrehajthatóságát érintő stratégiai kockázat.

A függőség több, mint technológiai lemaradás. A modern hadseregek nemcsak fegyverrendszereket vásárolnak külföldről, hanem egyre gyakrabban azok működtetéséhez nélkülözhetetlen szolgáltatásokat is: műholdas kommunikációt, felderítési adatokat, szoftverfrissítéseket, titkosítási megoldásokat, felhőkapacitást és mesterséges intelligencia-alapú elemzési rendszereket. Ezek esetében a tulajdonjog nem feltétlenül jelent tényleges rendelkezési jogot. Egy megvásárolt eszköz használhatósága függhet a szolgáltató szerződéses feltételeitől, a gyártó által ellenőrzött szoftvertől, külföldi exportengedélyektől vagy egy másik állam politikai döntéseitől. A függőség három formája különösen veszélyes: ha a szolgáltatás távolról korlátozható; ha a működéshez szükséges adatok és frissítések kizárólag külföldről érkeznek; illetve, ha nincs gyorsan alkalmazható helyettesítő megoldás. Ilyenkor a technológiai fölény előnye egyben stratégiai sérülékenységgé válhat.

Európa sajátos problémája. Az európai NATO-tagállamok számára az amerikai technológiai együttműködés nélkülözhetetlen biztonsági előnyt jelent. Az Egyesült Államok olyan műholdas felderítési, rakétaindítás-előrejelzési és kommunikációs képességekkel rendelkezik, amelyeket Európa jelenleg nem tud teljes egészében helyettesíteni. Különösen az űralapú rakétaindítás-észlelés és a nagy teljesítményű, alacsony pályás műholdas kommunikáció területén jelentős a függőség.

A kérdés persze nem az amerikai technológia elutasítása, hanem az egyoldalú függőség csökkentése. A szövetségesi bizalom és a technológiai önállóság nem egymást kizáró célok. Ellenkezőleg: a saját képességekkel rendelkező európai államok megbízhatóbb és nagyobb teherviselésre képes NATO-szövetségesek lehetnek. Az Európai Unió már tett lépéseket ebbe az irányba. A GOVSATCOM 2026 januárjában megkezdte működését, az IRIS² európai műholdrendszer első indításait pedig 2029-re tervezik.

A stratégiai autonómia valódi tartalma. Az európai technológiai önállóság nem jelenthet teljes önellátást. Ez gazdaságilag irreális, katonailag pedig szükségtelen volna. A stratégiai autonómia végső soron nem azt jelenti, hogy mindent magunk állítunk elő, hanem azt, hogy létfontosságú döntéseink végrehajtása nem függhet kizárólag mások hozzájárulásától. A cél annak biztosítása, hogy egyetlen külső szolgáltató vagy állam se válhasson valamely létfontosságú képesség kizárólagos működtetőjévé. Ehhez a kritikus rendszerek esetében több szolgáltató alkalmazására, átjárható műszaki megoldásokra, saját adatfeldolgozási és szoftveres képességekre, valamint előre kidolgozott tartalékmegoldásokra van szükség. A beszerzéseknél nemcsak az ár és a teljesítmény, hanem a hozzáférés garantálhatósága, a korlátozhatóság és a válsághelyzeti működőképesség is stratégiai szempont kell, hogy legyen.

2026. október 16.