MAGYAR KÜLÜGYI INTÉZET

Az iráni háború és a gazdaságbiztonság új fejezete

GORECZKY PÉTER

MKI Nézőpont
A Magyar Külügyi Intézet rendszeres kiadványa.

Kiadó:

Szerző(k):
Goreczky Péter

Lektorálta:
Vass Ágnes

Korábbi kiadványainkat megtekintheti az Intézet weboldalán.

Borítókép forrás: Shutterstock

2026. május 04.

Goreczky Péter, vezető kutató, MKI

AZ IRÁNI HÁBORÚ ÉS A GAZDASÁGBIZTONSÁG ÚJ FEJEZETE

Az iráni háború miatt átalakul a gazdasági sebezhetőség fogalma, amely az egymással összekapcsolt energetikai, pénzügyi, logisztikai és technológiai rendszerek rugalmasságának a függvénye. A védelmi stratégiákban új fejezetet kaphat az adatközpontok és technológiai nagyvállalatok védelme, amelyek most először váltak katonai támadások, illetve fenyegetések célpontjává. A szuverenitás egyre inkább az adathálózatok, az infrastruktúra és a technológiai ökoszisztémák feletti rendelkezést is jelenti, ami egyre nagyobb mértékben fogja meghatározni a 21. században a gazdasági és geopolitikai hatalmat.

A COVID-19 világjárvány óta a gazdaságbiztonság világszerte a kormányzati politikák fókuszába került, tükrözve azt a felismerést, hogy a gazdaságok összekapcsolódása a kétségtelen előnyök mellett a sebezhetőséget is növeli. A kereskedelem és a beruházások globális áramlása lehetővé teszi az egyes országok számára, hogy a hatékonyság mentén szakosodjanak, ugyanakkor a beszállítók, a piac és a technológia terén meglévő szűk keresztmetszetek kockázatot jelentenek, ha a kapcsolati háló geopolitikai konfliktusok vagy ellátási sokkok miatt megszakad. Az iráni háború pedig ebben a tekintetben új megfontolásokat hozott felszínre, elsősorban az ellátási láncok, a kritikus infrastruktúra és a technológia terén.

A konfliktus leglátványosabb, gazdaságbiztonságot érintő következménye az ellátási láncok legújabb zavara, ezúttal elsősorban az energiahordozók és egyéb nyersanyagok kereskedelme terén. Irán lépései megmutatták, hogy egy globális jelentőségű szállítmányozási útvonal megbénítása révén sokkal hatékonyabban lehet nyomás alá helyezni egy nagyhatalmat, mint katonai akciókkal. A háború okozta energiaválság részleteit itt nem érintve annyit érdemes kiemelni, hogy a közel-keleti konfliktus nem egyszerűen a sokkhatások iránti kitettségre irányítja a figyelmet, hanem a képességre, hogy az egyes gazdaságok mennyire tudják ezeket a sokkokat elviselni. A gazdasági sebezhetőség fogalma így át-

alakul, és már nem csupán a szűk értelemben vett függőséget jelenti, hanem az egymással összekapcsolt energetikai, pénzügyi, logisztikai és technológiai rendszerek rugalmasságát. Ebből pedig az következik, hogy egy fegyveres konfliktus sikeres megvívásának esélyeit az adott állam gazdasági ellenállóképessége és katonai ereje együttesen fogja meghatározni.

A tanulságok alapján a legtöbb kormány a beszállítók diverzifikálásában, a stratégiai tartalékok növelésében, illetve a near shoring és reshoring célú beruházásokban látja hosszabb távon a kockázatok csökkentésének útját. Ami a folyamat geopolitikai hatásait illeti, a magasabb olajár többletbevételt jelent Oroszország számára, amelyből az Ukrajna elleni háborút finanszírozhatja, az alternatív beszállítók jelentőségének növekedése pedig egyértelműen javítja Moszkva alkupozícióját a partnereivel szemben. Az EU-ban az energiaválság újra megnyithatja az energia megfizethetőségről és a beszerzéssel kapcsolatos mentességekről szóló politikai vitákat, csökkentve ezzel az Oroszországgal szembeni egységes uniós fellépés esélyeit.

Az energiahálózatok, a távközlési rendszerek, a pénzügyi infrastruktúra és az adathálózatok mind olyan tényezők, amelyektől egyre nagyobb mértékben függ világszerte a gazdasági tevékenység. A kritikus infrastruktúra védelme nem újdonság, amelynek geopolitikai aspektusai az elmúlt években egyre meghatározóbbá váltak a vonatkozó kormányzati stratégiákban. Ezen a téren a közel-keleti konfliktus azonban új fejezetet nyitott azzal, hogy Irán március elején az Amazon vállalat két térségbeli adatközpontját támadta drónokkal.[1] Április első napjaiban pedig további amerikai cégek érdekeltségébe tartozó adatközpontokat támadott az iráni haderő Bahreinben és Dubaiban. Irán a saját bőrén is megtapasztalta ezt az újfajta kitettséget, amikor amerikai vagy izraeli rakéta találta el egy iráni állami bank adatközpontját Teheránban. Az adatközpontok már eddig is a kémtevékenység és kibertámadások célkeresztjébe kerültek, ám a közel-keleti konfliktus során látott akciók fizikai támadások voltak, ami egészen új gazdaságbiztonsági kérdéseket vet fel. Az amerikai haderő az Irán elleni támadások során bevallottan alkalmaz mesterséges intelligenciát adatfeldolgozási és döntéstámogatási feladatokra.[2] Márpedig a mesterséges intelligencia infrastruktúrájának fontos elemét képezik az adatközpontok, az iráni vezetés ezért indokolhatta azzal a drón-

1 Annie Palmer, „Amazon says drone strikes damaged 3 facilities in UAE and Bahrain", *CNBC*, 2026. március 2. https://www.cnbc.com/2026/03/02/amazon-says-drone-strikes-damaged-3-facilities-in-uae-and-bahrain.html.

2 „US military confirms use of 'advanced AI tools' in war against Iran", *Al Jazeera*, 2026. március 11., https://www.aljazeera.com/news/2026/3/11/us-military-confirms-use-of-advanced-ai-tools-in-war-against-iran.

támadást, hogy a létesítmények támogatják az országuk elleni amerikai katonai akciókat. Függetlenül attól, hogy ez így volt-e, az Egyesült Arab Emírségekben az adatközpont megrongálása komoly zavart okozott a helyi bankrendszer működésében is, ami jól mutatja, hogy a katonai vonatkozások mellett egy ilyen akció károkat okoz a kritikus szolgáltatások, a digitális kormányzási rendszerek és az egész nemzetgazdaság működésében is. Ráadásul egy adatközpont viszonylag sebezhető célpontnak számít, könnyebben lehet sikerként elkönyvelhető támadást intézni ellene, mint egy katonai bázis ellen. Az iráni háború egyik fő következménye tehát a gazdaságbiztonság terén, hogy az adatközpontok védelme többé már nem csupán kiberbiztonsági kérdésnek minősül. Az infrastrukturális beruházásokért felelős döntéshozóknak ezért a helyszín kiválasztásakor mostantól figyelembe kell venniük a geopolitikai stabilitást és a regionális konfliktusok kockázatát. Ugyanakkor az adatközpontok geopolitikai szempontból stabilabb régiókba telepítése nem olyan magától értetődő, mivel számos országban adatlokalizációs jogszabályok vannak érvényben, az adat-hozzáférés terén pedig technikai korlátok merülhetnek fel. Arra azonban mindenképpen számítani kell, hogy a kormányok egyre inkább az erőművekhez, repülőterekhez és távközlési csomópontokhoz hasonlóan fogják kezelni az adatközpontokat, beemelve őket a védelmi stratégiáikba. A feltörekvő hatalmak számára a következmények még összetettebbek. A háború ugyanis megerősíti azt a felismerést, miszerint a kritikus technológiai infrastruktúra nem csupán a fejlődés, hanem a szuverenitás eszköze is. A technológiai szuverenitás egyre népszerűbbé váló koncepciója ezzel további híveket szerezhet magának.

Az adatközpontok elleni fizikai támadások és a mesterséges intelligencia használata az Irán elleni katonai akció során további következményekkel fog járni a gazdaságbiztonsági stratégiák technológiai fejezeteire nézve. Az elmúlt hetek tanulságai alapján annyit biztosan ki lehet jelenteni, hogy a most zajló háborúnak minden korábbi katonai konfliktusnál nagyobb a digitális árnyéka. Mindezt jól mutatja, hogy Irán nem csupán az USA és Izrael haderejét, hanem az amerikai Big Tech régióban levő érdekeltségeit is legitim célpontként jelölte meg.[3] Az adatközpontok elleni fizikai támadásokhoz hasonlóan ez a fejlemény is egy olyan jövőt vetít előre, amelyben egy adott ország technológiai szolgáltató és innovációs bázisa kerülhet célkeresztbe a geopolitikai konfliktusok során.

3 Miranda Jeyaretnam, „Iran Threatens to Target U.S. Tech Firms if War Continues to Escalate”, *Time Magazine*, 2026. április 2., https://time.com/article/2026/04/01/iran-revolutionary-guard-corps-tech-apple-google-meta-microsoft-nvidia/.

Az Egyesült Államok már eddig is nyilvánvalóvá tette, hogy számára a technológiai fölény egyenlő a nemzetbiztonsággal. A közel-keleti konfliktus nyomán Washington várhatóan még nagyobb hangsúlyt fog fektetni a fejlett technológiákhoz való hozzáférés korlátozására, valamint a szövetséges hálózatok kritikus infrastruktúrájának védelmére. Peking számára pedig az lehet a történet tanulsága, hogy tovább kell fokoznia a technológiai önellátást és a rendszerszintű ellenőrzést célzó törekvéseit. Ez a gyakorlatban elsősorban a hazai félvezetőgyártási kapacitás, a szuverén felhőalapú infrastruktúra és a szigorúan szabályozott digitális hálózatok további fejlesztését jelenti.

Az eddig leírt folyamatok valójában mind abba az irányba mutatnak, hogy átalakulóban van a szuverenitás fogalma. A területi alapú ellenőrzés és hatalomgyakorlás mellett a szuverenitás egyre inkább az olyan rendszerek feletti rendelkezés képességét is jelenti, mint az adatok, a hálózatok, az infrastruktúra és a technológiai ökoszisztémák, amelyek a 21. században meghatározzák a gazdasági és geopolitikai hatalmat. Az iráni háború újra felszínre hozta az utóbbi években lassan megszokottá vált kérdést, hogy hogyan egyeztethető össze a gazdasági globalizáció a technológiai szuverenitással és az ellátás biztonsággal. A minden szempontból megfelelő választ eddig egyetlen állam sem találta meg. A szemünk előtt zajló útkeresésekből minden esetre egy töredezettebb világgazdaság képe bontakozik ki, amelyet egymással versengő szabványok, párhuzamos rendszerek és stratégiai bizalmatlanság jellemez.

MAGYAR
KÜLÜGYI
INTÉZET